ALGÈBRE ET GÉOMÉTRIE

François COMBES

Ancien élève de l'École Normale Supérieure de Saint-Cloud
Professeur de Mathématiques à l'Université d'Orléans

AVANT PROPOS

Cet ouvrage a été conçu à partir du cours enseigné par l'auteur ces dernières années en Licence de Mathématiques. Le contenu de cet enseignement découlait lui-même des exigences des programmes des Concours du CAPES et de l'Agrégation de Mathématique auxquels la grande majorité des étudiants de ce cursus se destinaient.

C'est donc un livre qui se veut pratique, très proche des programmes des concours que nous avons mentionnés, incluant de nombreux exemples et exercices d'application. Il introduit les notions algébriques de groupe (partie I) et d'anneau (partie III). Il les utilise d'une part dans le cadre de la géométrie affine et de la géométrie euclidienne (partie II), et d'autre part en théorie des nombres (partie IV), chapitres importants dans la formation des futurs enseignants.

Les fondements de la géométrie affine ne sont plus enseignés dans les Premiers Cycles Universitaires où il a fallu faire place à de nouvelles disciplines. C'est dans le cours d'algèbre de Licence que ce chapitre trouve une place naturelle. En effet, la notion de groupe est partout sous-jacente en géométrie. Elle y trouve d'innombrables illustrations et applications. Depuis F. Klein et H. Poincaré, les géométries, euclidiennes ou non, sont perçues dans le contexte d'un ensemble de points sur lequel un groupe opère. En géométrie plane euclidienne, apparaissent divers groupes classiques : groupe des homothéties et translations, groupe des isométries, groupe des déplacements, groupe des similitudes,... dont la structure doit être connue.

Par ailleurs, la nécessité de découper les cursus en Unités d'enseignement séparées, crée artificiellement une division des mathématiques en disciplines que l'on a tendance à considérer comme des domaines disjoints. Or, dans la réalité, et historiquement, la pensée est un tout où les grands chapitres se rencontrent, s'interpénètrent. Par exemple, c'est le développement de l'analyse qui a provoqué la naissance de la géométrie analytique au 17^{e} siècle et de la géométrie riemannienne au milieu du 19^{e} siècle, de la théorie analytique des nombres dans la deuxième moitié du 19^{e} siècle. C'est la puissance de l'algèbre moderne qui explique le développement de la géométrie algébrique au 20^{e} siècle. Dans cet ouvrage, nous avons voulu mettre en valeur cette présence de l'algèbre au sein de la géométrie, de la géométrie en théorie des nombres, chaque discipline apportant ses outils à l'autre : preuve géométrique de l'existence de solutions pour des équations diophantiennes en arithmétique, démonstration algébrique de l'impossibilité d'effectuer certaines constructions géométriques à la règle et au compas (quadrature du cercle, contruction des polygones réguliers,...), etc.

Comme nous l'indiquions, afin de privilégier le caractère pratique et utile de cet ouvrage, nous avons volontairement limité le contenu aux notions figurant explicitement dans les programmes des Concours de recrutement des enseignants du Second Degré : groupes cycliques et abéliens, groupe symétrique, groupes de transformations géométriques classiques, anneau des polynômes, applications classiques à l'arithmétique, à la théorie des nombres...

Les parties de ce livre qui ne sont pas explicitement au programme du CAPES de Mathématique, et qui concernent plutôt la préparation à l'Agrégation, apparaissent à la fin des parties I et IV. Il s'agit des théorèmes de Sylow et de l'étude des anneaux factoriels.

Je tiens à remercier, très chaleureusement, mes collègues J. M. CHEVALLIER , C. POP , J. F. HAVET , J. P. SCHREIBER qui m'ont accordé beaucoup de temps pour m'aider à surmonter les difficultés pratiques liées à l'utilisation des logiciels, et qui m'ont fait le cadeau le plus précieux pour un mathématicien : des exemples intéressants, des remarques originales, qui ont enrichi cet ouvrage.

Je remercie également les Editions BREAL, qui ont accepté de publier ce livre, et qui m'ont donné des conseils très utiles pour sa conception.

Table des matières

I GROUPES **9**

1 La catégorie des groupes **11**
1.1 Factorisation d'une application 11
1.2 Loi de composition interne sur un ensemble 13
1.3 Notion de groupe 15
1.4 Homomorphismes de groupes 16
1.5 Sous-groupes 18
1.6 Noyau et image d'un homomorphisme 20
1.7 Indice d'un sous-groupe, théorème de Lagrange 21
1.8 Groupe quotient 23
1.9 Factorisation des homomorphismes 24
1.10 Produit direct de groupes 25
1.11 Caractérisation du produit direct 26
1.12 Procédé de symétrisation 27
1.13 Sous-groupes de $\mathbb{Z}$ et de $\mathbb{R}$ 28
1.14 Sous-groupe engendré par un élément 30
1.15 Exercices du chapitre 1 31

2 Actions de groupes **39**
2.1 Groupe agissant sur un ensemble 39
2.2 Orbite, stabilisateur d'un point 41
2.3 Action d'un groupe fini sur un ensemble fini 43
2.4 Théorème de Cauchy 45
2.5 Théorème d'isomorphisme de Noether 45
2.6 Produits semi-directs 47
2.7 Caractérisation des produits semi-directs 48
2.8 Exercices du chapitre 2 50

3 Groupes abéliens finis **59**
3.1 Groupes cycliques, générateurs 59
3.2 Homomorphismes entre groupes cycliques 60
3.3 Sous-groupes d'un groupe cyclique 62
3.4 Produit de deux groupes cycliques 63
3.5 Groupes d'ordre premier 64
3.6 Décomposition cyclique d'un groupe abélien fini 65
3.7 Groupes résolubles 69
3.8 Exercices du chapitre 3 71

4 Le groupe symétrique **79**
4.1 Décomposition d'une permutation en cycles . . . 79
4.2 Cycles conjugués . . . 80
4.3 Générateurs du groupe symétrique . . . 81
4.4 Signature d'une permutation . . . 81
4.5 Non résolubilité du groupe des permutations . . . 83
4.6 Exercices du chapitre 4 . . . 84

5 Sous-groupes de Sylow **91**
5.1 Théorèmes de Sylow . . . 91
5.2 Structure de quelques groupes finis . . . 94
5.3 Groupes d'ordre 8 . . . 96
5.4 Exercices du chapitre 5 . . . 97

II GEOMETRIE **103**

6 Géométrie affine **105**
6.1 Espace affine associé à un espace vectoriel . . . 105
6.2 Repères cartésiens . . . 107
6.3 Applications affines . . . 109
6.4 Existence d'applications affines . . . 111
6.5 Isomorphismes affines . . . 112
6.6 Sous-espaces affines . . . 114
6.7 Sous-espaces affines en dimension finie . . . 115
6.8 Sous-espaces affines et applications affines . . . 117
6.9 Groupe affine . . . 118
6.10 Groupe des homothéties et translations . . . 120
6.11 Orientation d'un espace affine réel . . . 121
6.12 Exercices du chapitre 6 . . . 123

7 Barycentres en géométrie affine **133**
7.1 Barycentres . . . 133
7.2 Applications affines et barycentres . . . 135
7.3 Sous-espaces affines et barycentres . . . 136
7.4 Repères affines . . . 137
7.5 Espace affine hyperplan d'un espace vectoriel . . . 139
7.6 Parties convexes d'un espace affine réel . . . 141
7.7 Enveloppe convexe d'une partie . . . 143
7.8 Points extrémaux d'une partie convexe . . . 143
7.9 Sommets des polygones et polyèdres convexes . . . 145
7.10 Les polyèdres convexes réguliers . . . 146
7.11 Exercices du chapitre 7 . . . 148

8 Géométrie affine euclidienne **153**
8.1 Espaces affines euclidiens . . . 153
8.2 Rappels sur le groupe orthogonal . . . 154
8.3 Isométries affines . . . 156
8.4 Symétries orthogonales . . . 157
8.5 Symétries glissées . . . 159
8.6 Isométries produits de symétries hyperplanes . . . 160

8.7 Groupe des isométries de $\mathcal{E}_n$ 162
8.8 Décomposition canonique d'une isométrie 163
8.9 Classification des isométries du plan 164
8.10 Classification des isométries de l'espace 166
8.11 Groupe des similitudes 170
8.12 Sous-groupes finis du groupe des déplacements 171
8.13 Exercices du chapitre 8 174

III ANNEAUX **187**

9 Généralités sur les anneaux **189**
9.1 Les objets de cette catégorie mathématique 189
9.2 Les morphismes dans cette catégorie mathématique 192
9.3 Les sous-anneaux 194
9.4 Sous-anneau engendré par une partie non vide 195
9.5 Idéaux d'un anneau 195
9.6 Intersection et somme d'idéaux 196
9.7 Quotient d'un anneau par un idéal bilatère 198
9.8 Idéaux maximaux 199
9.9 Corps 200
9.10 Corps des fractions d'un anneau intègre 202
9.11 Quotient par un idéal maximal 204
9.12 Sous-corps premier d'un corps 205
9.13 Exercices du chapitre 9 206

10 Anneaux de polynômes **213**
10.1 Polynômes à coefficients dans un anneau 213
10.2 Division euclidienne 215
10.3 Fonction polynomiale et racines d'un polynôme 216
10.4 Dérivée formelle d'un polynôme, formule de Taylor 217
10.5 Multiplicité d'une racine 218
10.6 Un exemple: les polynômes cyclotomiques 219
10.7 Groupe K_* lorsque K est un corps commutatif 221
10.8 Le polynôme d'interpolation de Lagrange 224
10.9 Résolution des équations du troisième degré 224
10.10 Exercices du chapitre 10 226

11 Anneaux principaux **237**
11.1 Idéaux principaux, anneaux principaux 237
11.2 Exemples classiques: les anneaux euclidiens 238
11.3 Entiers d'un corps quadratique 240
11.4 Divisibilité dans un anneau principal 241
11.5 Décomposition en facteurs irréductibles 244
11.6 Anneau des entiers de Gauss 246
11.7 Théorème chinois 249
11.8 Quotients dans les anneaux principaux 250
11.9 Exercices du chapitre 11 252

IV Théorie des nombres **261**

12 Arithmétique **263**
12.1 Congruences, anneau $\mathbb{Z}/n\mathbb{Z}$ . . . 263
12.2 Théorèmes de Fermat-Euler et de Wilson . . . 264
12.3 Résidus quadratiques . . . 267
12.4 Nombres premiers . . . 269
12.5 Nombres de Mersenne, nombres de Fermat . . . 270
12.6 Un pas vers le théorème de Dirichlet . . . 272
12.7 Equations diophantiennes . . . 273
12.8 Exercices du chapitre 12 . . . 277

13 Nombres algébriques **289**
13.1 Eléments algébriques d'une algèbre . . . 289
13.2 Une application à l'algèbre linéaire . . . 290
13.3 Nombres transcendants . . . 292
13.4 Le corps des nombres algébriques . . . 294
13.5 Constructions à la règle et au compas . . . 296
13.6 Quelques constructions à la règle et au compas . . . 298
13.7 Exercices du chapitre 13 . . . 301

14 Anneaux factoriels **307**
14.1 Une généralisation des anneaux principaux . . . 307
14.2 Polynômes primitifs . . . 310
14.3 Irréductibilité des polynômes . . . 311
14.4 Anneau des polynômes sur un anneau factoriel . . . 312
14.5 Critère d'irréductibilité d'Eisenstein . . . 314
14.6 Irréductibilité des polynômes cyclotomiques . . . 317

INDEX **319**

Première partie

GROUPES

Chapitre 1

La catégorie des groupes

1.1 Factorisation d'une application

Définition.

On appelle relation d'équivalence sur un ensemble non vide E, une relation binaire R sur E vérifiant les conditions suivantes :
a) $\forall\, x \in E \quad xRx$ *(réflexivité),*
b) $\forall\, x \in E \quad \forall\, y \in E \quad xRy \quad \Leftrightarrow \quad yRx$ *(symétrie),*
c) $\forall\, x \in E \quad \forall\, y \in E \quad \forall\, z \in E \quad (\, xRy \quad et \quad yRz\,) \quad \Rightarrow \quad xRz$ *(transitivité).*

La partie $C_x = \{y \in E \mid xRy\}$ de E est appelée la *classe d'équivalence* modulo R de $x \in E$. Elle contient x d'après a). Considérons $y \in C_x$. Pour tout $z \in C_y$ on a $z \in C_x$ (d'après c)), ce qui prouve que $C_y \subset C_x$. Comme les conditions $x \in C_y$ et $y \in C_x$ sont équivalentes, d'après b), on a de même $C_x \subset C_y$ et donc $C_x = C_y$. Il en résulte que tout $x \in E$ appartient à l'une des parties de la famille $(C_x)_{x\in E}$ et à une seule. Les classes d'équivalence constituent une partition de E.

Notons $\mathcal{P}(E)$ l'ensemble des parties de E. La famille $(C_x)_{x\in E}$ constitue un sous-ensemble de $\mathcal{P}(E)$ appelé l'*ensemble quotient de E par R*. On le note E/R. Dans la suite, la classe de $x \in E$ sera vue essentiellement comme élément de ce nouvel ensemble E/R et sera notée $\overline{x}$. L'*application canonique* $j : x \mapsto \overline{x}$ est surjective de E sur E/R.

Considérons une application f de E dans un ensemble F. Soit $(x, y) \in E \times E$. Posons $x\, R_f\, y$ si et seulement si $f(x) = f(y)$. On définit ainsi une relation d'équivalence R_f sur E. Elle partage E en classes d'éléments ayant la même image par f.

Pour la surjection canonique $j : E \to E/R$ considérée précédemment, on a $R_j = R$.

Proposition.

Considérons une relation d'équivalence R sur l'ensemble E, une application f de E dans un autre ensemble F constante sur toute classe d'équivalence $\overline{x}$. Il existe alors une application $\overline{f}$ de E/R dans F, unique, telle que $\overline{f} \circ j = f$. On a $Im\,(f) = Im\left(\overline{f}\right)$. L'application $\overline{f}$ est injective si et seulement si $R = R_f$.

Démonstration. La condition $\overline{f} \circ j = f$ impose la valeur $\overline{f}(\overline{x}) = f(x)$ pour tout élément $\overline{x}$ de E/R, d'où l'unicité de $\overline{f}$.

L'existence tient au fait que f est constante sur toute classe $\overline{x}$. La valeur $f(x)$ ne dépend que de $\overline{x} \in E/R$ et non du représentant particulier x de la classe $\overline{x}$. Il existe

donc une application $\overline{f}$ bien définie de E/R dans F telle que $\overline{f}(\overline{x}) = f(x)$, c'est-à-dire telle que $\overline{f} \circ j = f$. On a évidemment $\text{Im}\,(f) = \text{Im}\left(\overline{f}\right)$.

Enfin, $\overline{f}$ est injective si les conditions $\overline{f}(\overline{x}) = \overline{f}(\overline{y})$ et $\overline{x} = \overline{y}$ sont équivalentes. Or

$$\overline{x} = \overline{y} \quad \Leftrightarrow \quad xRy \qquad \text{et} \qquad \overline{f}(\overline{x}) = \overline{f}(\overline{y}) \quad \Leftrightarrow \quad f(x) = f(y) \quad \Leftrightarrow \quad xR_f y\,.$$

Donc $\overline{f}$ est injective si et seulement si $R = R_f$. ∎

Définition.

On dit que $\overline{f}$ se déduit de f par factorisation, ou par passage au quotient.

Corollaire.

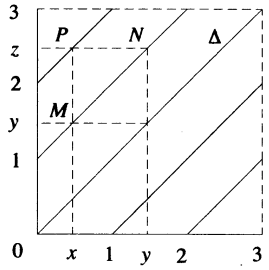
Soit $f : E \to F$ une application. Elle admet la décomposition canonique $f = i \circ \overline{f} \circ j$ où $j : E \to E/R_f$ désigne la surjection canonique, où $\overline{f} : E/R_f \to f(E)$ est bijective et où $i : x \mapsto x$ est l'injection naturelle de $f(E)$ dans F.

Exercice 1. Soit R une relation binaire sur un ensemble E. On appelle graphe de R, la partie $G_R = \{(x,y) \in E \times E \mid xRy\}$ de $E \times E$.
Quelles propriétés de G_R traduisent le fait que R est une relation d'équivalence ? Que dire d'une relation d'équivalence qui est aussi une relation d'ordre ?
Si $E = [0,3[$, dessiner le graphe de la relation binaire $x \equiv y \pmod 1$.

Solution. La réflexivité ($\forall x \in E \quad xRx$) signifie que G_R contient la diagonale $\Delta = \{(x,x)\,;\ x \in E\}$.

La symétrie est traduite par l'invariance de G_R dans la symétrie $(x,y) \mapsto (y,x)$ par rapport à la diagonale Δ.

La transitivité de la relation R signifie que si deux points $M = (x,y)$ et $N = (y,z)$ du graphe, sont tels que "l'ordonnée" y de M et "l'abscisse" de N sont égales, alors $P = (x,z)$ est lui aussi élément de G_R.



La relation d'équivalence R ne peut être une relation d'ordre que si $G_R = \Delta$, c'est-à-dire si les classes d'équivalence sont toutes ponctuelles. (R est l'égalité.)

Exercice 2. Soient $f : X \to Y$ et $g : X \to Z$ des applications surjectives. Montrer que $R_f = R_g$ si et seulement s'il existe une bijection u de Y sur Z telle que $g = u \circ f$.

Solution. S'il existe $u : Y \to Z$ injective telle que $g = u \circ f$, pour tout $x \in X$ et tout $y \in X$ on a

$$x\,R_g\,y \;\Leftrightarrow\; g(x) = g(y) \;\Leftrightarrow\; u(f(x)) = u(f(y)) \;\Leftrightarrow\; f(x) = f(y) \;\Leftrightarrow\; x\,R_f\,y$$

Donc $R_f = R_g$. Réciproquement, supposons que $R_f = R_g$. Désignons par j la surjection canonique de X sur $X/R_f = X/R_g$. Les décompositions canoniques de f et g donnent des bijections $\overline{f} : X/R_f \to Y$ et $\overline{g} : X/R_g \to Z$ telles que $f = \overline{f} \circ j$ et $g = \overline{g} \circ j$. Alors $u = \overline{g} \circ \overline{f}^{-1}$ est une bijection de Y sur Z telle que $u \circ f = (\overline{g} \circ \overline{f}^{-1}) \circ (\overline{f} \circ j) = \overline{g} \circ j = g$.

1.2 Loi de composition interne sur un ensemble

Définition.

On appelle loi de composition interne, ou opération, sur un ensemble E, une application $(x,y) \mapsto x*y$ de $E \times E$ dans E.

Cette opération est dite *commutative* si $x*y = y*z$ pour tout $x \in E$ et tout $y \in E$.

Elle est dite *associative* si $(x*y)*z = x*(y*z)$ pour tous $x \in E$, $y \in E$, $z \in E$.

S'il existe $e \in E$ tel que $e*x = x$ pour tout $x \in E$ on dit que e est *neutre à gauche*.

S'il existe $e' \in E$ tel que $x*e' = x$ pour tout $x \in E$ on dit que e' est *neutre à droite*.

On dit que $e \in E$ est *neutre* s'il est neutre à gauche et neutre à droite.

Si l'opération est notée additivement, l'élément neutre se note 0 et s'appelle le *zéro*.

On dit que $a \in E$ est *régulier* si pour tout $x \in E$ et pour tout $y \in E$,

$$(a*x = a*y) \;\Rightarrow\; (x = y) \qquad \text{et si} \qquad (x*a = y*a) \;\Rightarrow\; (x = y).$$

Si tout $a \in E$ est régulier, on dit que la loi de composition $*$ est régulière.

Dans la suite, une loi de composition interne sera le plus souvent notée $(x,y) \mapsto xy$ (notation multiplicative) ou $(x,y) \mapsto x+y$ (notation additive). La notation additive n'est employée que dans des cas où l'opération est commutative (mais pas toujours comme le montre l'exemple du produit dans $\mathbb{R}$ ou $\mathbb{C}$).

Si $e \in E$ est neutre à gauche et si $e' \in E$ est neutre à droite on a $e' = ee' = e$. Alors $e = e'$ est un élément neutre. S'il existe un élément neutre, il est donc unique.

Supposons que l'opération soit associative et qu'il existe un élément neutre e. Soit $n \in \mathbb{N}$. On note x^n (ou nx si l'opération est notée additivement), l'élément e si $n = 0$, l'élément $x \cdots x$ produit (ou somme) de x par lui-même n fois si $n > 0$.

Si $x \in E$ admet un *inverse à gauche* y (tel que $yx = e$) et un *inverse à droite* z (tel que $xz = e$), alors $y = z$ car

$$y = ye = y(xz) = (yx)z = ez = z.$$

Cet élément y de E vérifie donc les relations suivantes,

$$yx = xy = e,$$

et il est le seul à les vérifier. On l'appelle l'*inverse* de x et on le note x^{-1}. Si les notations sont additives, on l'appelle l'*opposé* de x et on le note $-x$. On a $(x^{-1})^{-1} = x$.

Si $x, y \in E$ sont inversibles, alors xy est inversible et $(xy)^{-1} = y^{-1}x^{-1}$. En effet,

$$(y^{-1}x^{-1})(xy) = y^{-1}(x^{-1}x)y = y^{-1}ey = y^{-1}y = e,$$

et on a de même $(xy)(y^{-1}x^{-1}) = e$.

En particulier, x^2 est inversible et a pour inverse $(x^{-1})^2$ que l'on note x^{-2}. Par récurrence sur $k \in \mathbb{N}$, on voit que x^k admet pour inverse l'élément $(x^{-1})^k$, que l'on note x^{-k} (ou $-kx$ en notation additive).

Définition.

On dit qu'une relation d'équivalence R sur l'ensemble E est compatible avec une loi de composition interne $(x,y) \mapsto x*y$ définie sur E si pour tous $x, y, x', y' \in E$,

(1) $$xRx' \quad \textit{et} \quad yRy' \quad \Rightarrow \quad (x*y)\,R\,(x'*y').$$

Proposition.

Si la relation d'équivalence R est compatible avec l'opération $*$ sur E, en posant $\overline{x}\cdot\overline{y} = \overline{x*y}$ on définit une opération sur E/R. Si $*$ est associative (resp. commutative, avec élément neutre), l'opération quotient $\cdot$ possède cette propriété sur E/R. Si $x \in E$ est inversible, $\overline{x}$ est inversible dans E/R. Son inverse est la classe de x^{-1}.

Démonstration. Soit $(a,b) \in (E/R)\times(E/R)$. Il existe $x \in E$ et $y \in E$ tels que $\overline{x} = a$ et $\overline{y} = b$. Si on considère d'autres représentants $x' \in E$ et $y' \in E$ des classes a et b, on a $x\,R\,x'$ et $y\,R\,y'$. La condition (1) montre que $\overline{x*y} = \overline{x'*y'}$. Ainsi, $\overline{x*y} \in E/R$ ne dépend que de a et de b et non des représentants x et y choisis. Il existe donc une application bien définie de $(E/R)\times(E/R)$ dans E/R telle que pour tout $x \in E$ et pour tout $y \in E$ l'image de $(\overline{x}\,,\,\overline{y})$ soit $\overline{x*y}$. Cela démontre la première assertion.

Si $*$ est associative sur E, il en est de même pour l'opération quotient car :

$$(\overline{x}\cdot\overline{y})\cdot\overline{z} \;=\; (\overline{x*y})\cdot\overline{z} \;=\; \overline{(x*y)*z} \;=\; \overline{x*(y*z)} \;=\; \overline{x}\cdot(\overline{y*z}) \;=\; \overline{x}\cdot(\overline{y}\cdot\overline{z})\,.$$

Si $*$ est commutative on a $\overline{x}\cdot\overline{y} = \overline{x*y} = \overline{y*x} = \overline{y}\cdot\overline{x}$ et $(E/R\,,.)$ est commutatif.

Si $e \in E$ est élément neutre pour $*$, pour tout $\overline{x} \in E/R$ on a $\overline{e}\cdot\overline{x} = \overline{e*x} = \overline{x}$ et de même $\overline{x}\cdot\overline{e} = \overline{x}$ donc $\overline{e}$ est neutre dans E/R.

Si $x \in E$ a un inverse y, de la relation $x*y = y*x = e$ on déduit $\overline{x}\cdot\overline{y} = \overline{y}\cdot\overline{x} = \overline{e}$ donc $\overline{x}$ a pour inverse $\overline{y}$ dans E/R. ∎

Exercice 1. Etudier l'opération $*$ définie sur $E = \mathbb{R}\setminus\{-1\}$ par $a*b = a+b+ab$.

Solution. Pour tout $a \in E$ et tout $b \in E$ on a $a*b \in E$. En effet, si on avait $a*b = -1$ soit $(1+a)(1+b) = 0$, on aurait $1+a = 0$ ou $1+b = 0$, ce qui est exclu. Donc $(a,b) \mapsto a*b$ est une loi de composition interne sur E. Elle est commutative car l'expression de $a*b$ est symétrique en a et b. Elle est associative. En effet, l'expression $(a*b)*c = a+b+c+ab+bc+ca+abc$ est invariante par permutation circulaire. En utilisant la commutativité, on en déduit $(a*b)*c = (b*c)*a = a*(b*c)$. Pour tout $a \in E$, on a $a*0 = a$ donc 0 est élément neutre. Tout $a \in E$ admet un inverse b car l'équation $a+b+ab = 0$ a une solution unique $b = \frac{-a}{1+a}$ puisque $a \neq -1$.

Exercice 2. Soit $f : x \mapsto \exp(2i\pi x)$ de $\mathbb{R}$ dans $\mathbb{C}$. Montrer que R_f est compatible avec l'addition de $\mathbb{R}$. Etudier l'opération quotient sur $\mathbb{R}/R_f$.

Solution. $x\,R_f\,x' \;\Leftrightarrow\; e^{2i\pi x} = e^{2i\pi x'} \;\Leftrightarrow\; e^{2i\pi(x-x')} = 1 \;\Leftrightarrow\; x-x' \in \mathbb{Z}$.

Soient x,y,x',y' tels que xR_fx' et yR_fy'. On a $x-x' \in \mathbb{Z}$, $y-y' \in \mathbb{Z}$ d'où

$$(x+y)-(x'+y') = (x-x')+(y-y') \in \mathbb{Z} \quad \text{et donc} \quad (x+y)R_f(x'+y')\,.$$

Ainsi, la relation d'équivalence R_f est compatible avec l'addition. La classe de $x \in \mathbb{R}$, modulo R_f, est $\overline{x} = \{x+k\,;\;\; k \in \mathbb{Z}\}$. Il existe un représentant de cette classe et un seul, dans $[0,1[$, qui est $x - E(x)$, où $E(x)$ est la partie entière de x. L'application associant à $\overline{x}$ ce représentant, est donc une bijection de E/R_f sur $[0,1[$ qui permet d'identifier E/R_f avec $[0,1[$. L'opération quotient est définie par $\overline{x}+\overline{y} = \overline{x+y}$. Dans cette identification, elle devient l'opération $(s,t) \mapsto s+t-E(s+t)$ sur $[0,1[$.

1.3 Notion de groupe

Définition.

On appelle groupe un ensemble G muni d'une loi de composition interne associative, admettant un élément neutre, telle que tout élément de G ait un inverse.

Si $xy = yx$ pour tout $x \in G$ et tout $y \in G$, on dit que G est *commutatif*, ou *abélien*.
Le cardinal de G s'appelle l'*ordre* du groupe G et sera noté $[G : 1]$.

Proposition.

Soit G un groupe.
(i) *Pour tout $a \in G$, la translation à gauche $l_a : x \mapsto ax$ et la translation à droite $r_a : x \mapsto xa$, sont bijectives, d'applications réciproques $l_{a^{-1}}$ et $r_{a^{-1}}$.*
(ii) *Pour tout $a \in G$ et tout $b \in G$ on a $\quad l_a \circ l_b = l_{ab} \quad$ et $\quad r_a \circ r_b = r_{ba}$.*
(iii) *La loi de composition est régulière.*
(iv) *L'élément neutre e est le seul idempotent de G.*

Démonstration. (i) et (ii) Les relations (ii) sont dues à l'associativité :
$\forall x \in G \quad l_a \circ l_b(x) = a(bx) = (ab)x = l_{ab}(x) \quad$ et $\quad r_a \circ r_b(x) = (xb)a = x(ba) = r_{ba}(x)$.
Avec $b = a^{-1}$, on obtient $l_a \circ l_{a^{-1}} = l_e = \mathrm{Id}_G$, puis $l_{a^{-1}} \circ l_a = \mathrm{Id}_G$ en remplaçant a par a^{-1}. Donc l_a est bijective et $(l_a)^{-1} = l_{a^{-1}}$. De même $(r_a)^{-1} = r_{a^{-1}}$.
(iii) et (iv) L'injectivité de l_a et celle de r_a donnent la régularité de l'opération :

$$(ax = ay) \quad \Rightarrow \quad (x = y) \qquad , \qquad (xa = ya) \quad \Rightarrow \quad (x = y)\,.$$

En particulier, pour tout $x \in G$,

$$x^2 = x \quad \Leftrightarrow \quad xx = xe \quad \Rightarrow \quad x = e\,. \qquad \blacksquare$$

Exercice. En étudiant sa table de multiplication, montrer qu'un groupe G d'ordre 2 ou 3 ne peut avoir qu'une seule structure.

Solution. Soient e, a, ou e, a, b, les éléments de G, où e est neutre. Dans la table de multiplication de G, la ligne et la colonne de e sont imposées car e est neutre :

	e	a
e	e	a
a	a	.

	e	a	b
e	e	a	b
a	a	.	.
b	b	.	.

L'opération étant régulière, la ligne de a, image de $l_a : x \mapsto ax$, est une permutation des éléments de G (prop. 1-3). Il en est de même pour toute ligne et toute colonne. Il existe une seule façon de compléter chacun des tableaux ci-dessus, chaque élément de G apparaissant une fois et une seule dans chaque ligne et dans chaque colonne :

	e	a
e	e	a
a	a	e

	e	a	b
e	e	a	b
a	a	b	e
b	b	e	a

S'il existe une loi de groupe sur G, elle est donc unique et elle ne peut avoir que la table de multiplication ci-dessus. Cette table définit effectivement une loi de groupe car on retrouve la table d'un groupe connu, par exemple de $\mathbb{Z}/2\mathbb{Z}$ (resp. $\mathbb{Z}/3\mathbb{Z}$).

1.4 Homomorphismes de groupes

Définition.

Soient G, G' deux groupes, d'éléments neutres e et e'. On appelle homomorphisme (ou morphisme) de G dans G', une application f de G dans G' telle que

(1) $$\forall\, x \in G \quad \forall\, y \in G \quad f(xy) = f(x)f(y)\,.$$

Le sous-ensemble $\mathrm{Ker}\,(f) = \{\, x \in G \mid f(x) = e' \,\}$ de G est appelé le *noyau* de f.

On note $\mathrm{Hom}\,(G, G')$ l'ensemble des homomorphismes de G dans G'. Il existe au moins un homomorphisme de G dans G' : l'homorphisme trivial $f_0 : x \mapsto e'$.

Un homomorphisme de G dans G est appelé un *endomorphisme* de G. On note $\mathrm{End}\,(G)$ l'ensemble des endomorphismes de G.

On dit que $f \in \mathrm{Hom}\,(G, G')$ est un *isomorphisme*, s'il existe $g \in \mathrm{Hom}\,(G', G)$ tel que $g \circ f = \mathrm{Id}_G$ et $f \circ g = \mathrm{Id}_{G'}$. Il suffit pour cela que l'homomorphisme f soit bijectif. En effet, en appliquant f^{-1} aux deux membres de la relation (1), on voit que $f^{-1} \in \mathrm{Hom}\,(G', G)$. S'il existe un isomorphisme de G sur G' on dit que les groupes G et G' sont isomorphes. Nous écrirons $G \simeq G'$ pour traduire cela.

On appelle *automorphisme* de G, un isomorphisme de G sur G. On note $\mathrm{Aut}\,(G)$ l'ensemble des automorphismes de G.

Pour tout $x \in G$, l'application $\mathrm{Ad}_x : y \mapsto xyx^{-1}$ est bijective de G sur G, d'application réciproque $\mathrm{Ad}_{x^{-1}} : y \mapsto x^{-1}yx$. C'est un homomorphisme car

$$\forall\, y \in G \;\; \forall\, y' \in G \quad \mathrm{Ad}_x(yy') = xyy'x^{-1} = xyey'x^{-1} = xyx^{-1}xy'x^{-1} = \mathrm{Ad}_x(y)\ \mathrm{Ad}_x(y')\,.$$

Un tel automorphisme $\mathrm{Ad}_x : y \mapsto xyx^{-1}$ de G est appelé un *automorphisme intérieur*. On note $\mathrm{Int}\,(G)$ l'ensemble $\{\mathrm{Ad}_x\,;\ x \in G\}$ des automorphismes intérieurs de G.

Une bijection f d'un groupe G sur un ensemble X permet de *transporter la structure de G sur X* : on définit une loi de composition $*$ sur X en posant :

$$x * x' = f[f^{-1}(x)f^{-1}(x')]\,.$$

Muni de cette opération, X est un groupe et f est un isomorphisme de G sur X.

Soit $f \in \mathrm{Hom}\,(G, G')$. On a $f(e) = e'$. En effet $f(e)^2 = f(e^2) = f(e)$. Or d'après la 1-3, prop. (iv), e' est le seul idempotent de G' donc $f(e) = e'$.

Pour tout $x \in G$ on a $f(x^{-1}) = f(x)^{-1}$. En effet, $xx^{-1} = x^{-1}x = e$ donne $f(x)f(x^{-1}) = f(x^{-1})f(x) = e'$. Par récurrence, on montre que $f(x^k) = f(x)^k$ pour tout $k \in \mathbb{N}$, puis pour tout $k \in \mathbb{Z}$.

Proposition.

Soient G, G' et G'' des groupes. Pour tout $f \in \mathrm{Hom}\,(G, G')$ et tout $g \in \mathrm{Hom}\,(G', G'')$ la composée $g \circ f$ est un élément de $\mathrm{Hom}\,(G, G'')$.

Démonstration. Pour tout $x \in G$ et pour tout $y \in G$ on a :

$$(g \circ f)(xy) = g[f(xy)] = g[f(x)f(y)] = g[f(x)]g[f(y)]\,. \qquad \blacksquare$$

Corollaire.

Soit G un groupe. L'ensemble $\mathrm{Aut}\,(G)$ des automorphismes de G, muni de l'opération $(\alpha, \beta) \mapsto \alpha \circ \beta$ est un groupe d'élément neutre Id_G.

Démonstration. On sait que la composition des applications de G dans G est associative et admet Id_G comme élément neutre. D'après la proposition, compte tenu du fait que la composée de deux bijections est bijective, $(\alpha, \beta) \mapsto \alpha \circ \beta$ est une loi de composition interne sur $\mathrm{Aut}(G)$. Par définition de la notion d'isomorphisme, tout élément f de $\mathrm{Aut}(G)$ admet un inverse f^{-1} dans $\mathrm{Aut}(G)$. Ainsi, $\mathrm{Aut}(G)$ est un groupe. ∎

Exercice 1. On munit $E = \mathbb{R} \setminus \{-1\}$ de l'opération définie par $a * b = a + b + ab$. Montrer que E est un groupe isomorphe au groupe multiplicatif $\mathbb{R}^*$.

Solution. L'application $f : a \mapsto 1 + a$ est bijective de E sur $\mathbb{R}^*$. On a :

$$a * b = (1 + a)(1 + b) - 1 = f^{-1}[f(a)f(b)].$$

L'opération considérée sur E se déduit donc de la multiplication existant sur $\mathbb{R}^*$ par transport à l'aide de la bijection f, d'où le résultat. On retrouve ainsi les propriétés obtenues en 1-2, ex. 1 : le groupe est abélien, il a pour élément neutre $f^{-1}(1) = 0$, l'inverse de $a \in E$ est $f^{-1}(\frac{1}{f(a)}) = \frac{1}{1+a} - 1 = \frac{-a}{1+a}$.

Exercice 2. $\mathbb{R}$ est-il un groupe quand on le munit de l'opération définie par :

a) $x * y = \sqrt{x^2 + y^2}$? , **b)** $x * y = \sqrt[3]{x^3 + y^3}$?

Solution. a) $x * y = y \quad \Rightarrow \quad x^2 + y^2 = y^2 \quad \Leftrightarrow \quad x = 0$.
Seul 0 pourrait être élément neutre. Mais pour $y < 0$ on a $0 * y = \sqrt{y^2} = -y$. Donc $(\mathbb{R}, *)$ n'a pas d'élément neutre. Ce n'est pas un groupe. On peut vérifier que la loi de composition $*$ est commutative et associative.

b) $f : x \mapsto x^3$ est continue sur $\mathbb{R}$, strictement croissante, de limites $-\infty$ et $+\infty$ en $-\infty$ et $+\infty$. C'est une bijection de $\mathbb{R}$ sur $\mathbb{R}$, d'application réciproque $f^{-1} : x \mapsto \sqrt[3]{x}$ définie sur tout $\mathbb{R}$. On a $x * y = f^{-1}(f(x) + f(y))$ donc $(\mathbb{R}, *)$ est obtenu en transportant la structure de $(\mathbb{R}, +)$ à l'aide de f. C'est un groupe isomorphe à $(\mathbb{R}, +)$, d'élément neutre $f^{-1}(0) = 0$. L'inverse de x dans $(\mathbb{R}, *)$ est $f^{-1}(-f(x)) = -x$.

Exercice 3. Déterminer $\mathrm{End}(G)$ et $\mathrm{Aut}(G)$ lorsque G est le groupe $(\mathbb{Z}, +)$.

Solution. Soit $f \in \mathrm{End}(\mathbb{Z})$. Posons $k = f(1)$. Pour tout $n \in \mathbb{Z}$ on a $f(n) = kn$:

- pour $n \geqslant 0$, $\quad f(n) = f(1 + \cdots + 1) = f(1) + \cdots + f(1) = nf(1) = kn$.
- pour $n < 0$, $\quad f(n) = f(-|n|) = -f(|n|) = -k|n| = kn$.

Réciproquement, soit $k \in \mathbb{Z}$. Considérons $f_k : n \mapsto kn$. C'est un endomorphisme de $\mathbb{Z}$ car le produit distribue l'addition dans $\mathbb{Z}$. Ainsi $\mathrm{End}(\mathbb{Z}) = \{f_k ; \ k \in \mathbb{Z}\}$. Comme $f_k(1) = k$, on voit que $k \mapsto f_k$ est injective (et donc bijective) de $\mathbb{Z}$ sur $\mathrm{End}(\mathbb{Z})$. De plus, notons que l'on a :

$$\forall k \in \mathbb{Z} \quad \forall k' \in \mathbb{Z} \qquad f_{k+k'} = f_k + f_{k'} \quad \text{et} \quad f_{kk'} = f_k \circ f_{k'}.$$

Cela montre que $f : k \mapsto f_k$ est un isomorphisme du groupe $(\mathbb{Z}, +)$ sur le groupe $(\mathrm{End}(\mathbb{Z}), +)$. C'est même un isomorphisme d'anneaux de $\mathbb{Z}$ sur $\mathrm{End}(\mathbb{Z})$ (voir ch. 9).

L'endomorphisme f_k est surjectif si et seulement si $k\mathbb{Z} = \mathbb{Z}$, soit si $k = \pm 1$. Alors f_k est bijectif. Donc $\mathrm{Aut}(\mathbb{Z}) = \{\mathrm{Id}, -\mathrm{Id}\}$.

1.5 Sous-groupes

Définition.

On appelle sous-groupe du groupe G un sous-ensemble non vide H de G tel que :

(1) $\forall x \in G \ \forall y \in G \quad x, y \in H \ \Rightarrow \ xy \in H \quad , \quad \forall x \in G \quad x \in H \ \Rightarrow \ x^{-1} \in H$.

Si $\alpha(H) = H$ pour tout $\alpha \in Int(G)$ on dit que H est un sous-groupe distingué de G , ce que l'on écrit $H \lhd G$.

Si $\alpha(H) = H$ pour tout $\alpha \in Aut(G)$, on dit que H est un sous-groupe caractéristique de G . Un sous-groupe caractéristique est évidemment distingué.

On appelle centre de G , l'ensemble $Z(G) = \{ x \in G \mid \forall y \in G \quad xy = yx \}$.

Dans la définition précédente, la condition $H \neq \emptyset$ peut être remplacée par $e \in H$. En effet, il existe $x \in H$. On a alors $x^{-1} \in H$ et $e = xx^{-1} \in H$.

Le fait que H est un sous-groupe peut se traduire par les conditions suivantes :

$$H \neq \emptyset \qquad \text{et} \qquad \forall x \in G \ \forall y \in G \quad x, y \in H \quad \Rightarrow \quad x^{-1}y \in H .$$

Notons que $\{e\}$ et G sont deux sous-groupes (caractéristiques) particuliers de G .

Proposition.

Soient G un groupe et $(H_i)_{i \in I}$ une famille de sous-groupes (resp. de sous-groupes caractéristiques, de sous-groupes distingués) de G . Alors $H = \bigcap_{i \in I} H_i$ est un sous-groupe (resp. un sous-groupe caractéristique, un sous-groupe distingué) de G .

Démonstration. On a $e \in H = \bigcap_{i \in I} H_i$. Pour tout $x \in H$ et pour tout $y \in H$, on a $\forall i \in I \quad x, y \in H_i$ d'où $\forall i \in I \quad x^{-1}y \in H_i$ c'est-à-dire $x^{-1}y \in H$.

Donc H est un sous-groupe. Supposons H_i caractéristique pour tout $i \in I$. Alors

$$\forall \alpha \in \mathrm{Aut}(H) \qquad \alpha(H) = \alpha(\bigcap_{i \in I} H_i) = \bigcap_{i \in I} \alpha(H_i) = \bigcap_{i \in I} H_i = H .$$

Ainsi H est caractéristique. De même, si $H_i \lhd G$ pour tout $i \in I$, alors $H \lhd G$. ∎

Corollaire.

Soit A une partie non vide du groupe G .

(i) *Il existe un plus petit sous-groupe de G contenant A , à savoir l'intersection H des sous-groupes de G contenant A . Ce sous-groupe H est l'ensemble*

$$H = \{ x_1 \cdots x_k \, ; \ k \in \mathbb{N}^* \, , \ x_1 \in A \cup A^{-1} , \ldots , \ x_k \in A \cup A^{-1} \} .$$

(ii) *Soit $\alpha \in Aut(G)$. Si on a $\alpha(A) = A$ alors $\alpha(H) = H$.*

(iii) *Si les éléments de A commutent deux à deux, alors H est commutatif.*

Démonstration. (i) La famille $\mathcal{F}$ des sous-groupes de G contenant A est non vide car $G \in \mathcal{F}$. D'après la proposition, l'intersection H_0 de cette famille est un sous-groupe qui contient A . On a donc $H_0 \in \mathcal{F}$. Etant l'intersection de la famille, H_0 est le plus petit élément de $\mathcal{F}$. D'après (1), H_0 doit contenir $A^{-1} = \{x^{-1} \, ; \ x \in A\}$ et l'ensemble H de tous les mots $x_1 \cdots x_k$ formés avec les éléments de A ou A^{-1} . Le lecteur vérifiera que H est un sous-groupe de G contenant les éléments de A (mots de longueur $k = 1$). On a donc $H_0 \subset H$, car H_0 est le plus petit sous-groupe contenant A , et $H_0 = H$.

(ii) Si $\alpha(A) = A$, pour tout $a \in A$, on a $\alpha(a) \in A$ et donc $\alpha(a^{-1}) = \alpha(a)^{-1} \in A^{-1}$. Tout mot $m = x_1 \cdots x_k$ où $x_1, \ldots, x_k \in A \cup A^{-1}$ a pour image un autre mot $\alpha(m) = \alpha(x_1) \cdots \alpha(x_k)$ de H, ce qui prouve que $\alpha(H) \subset H$. On a aussi $A = \alpha^{-1}(A)$, d'où pareillement $\alpha^{-1}(H) \subset H$ et donc $H \subset \alpha(H)$. Finalement $\alpha(H) = H$.

(iii) Les éléments de $A \cup A^{-1}$ commutent deux à deux. En effet, pour tous $x, y \in A$,

$$x^{-1}y^{-1} = (yx)^{-1} = (xy)^{-1} = y^{-1}x^{-1} \quad \text{et} \quad xy^{-1} = y^{-1}yxy^{-1} = y^{-1}xyy^{-1} = y^{-1}x.$$

Ensuite, par récurrence sur les longueurs k et l des mots $m = x_1 \cdots x_k$ et $m' = x'_1 \cdots x'_l$ de H, où $x_1, \ldots, x_k, x'_1, \ldots, x'_l \in A \cup A^{-1}$, on vérifie que ces mots commutent. ∎

Définition 1.

Ce plus petit sous-groupe H de G contenant A est appelé le sous-groupe de G engendré par A. Nous le noterons $\langle A \rangle$.

Si $\langle A \rangle = G$, on dit que A est un système de générateurs de G.

Définition 2.

Si G est engendré par un élément $a \in G$, on dit que G est monogène.

On appelle ordre de $a \in G$ l'ordre $[\langle a \rangle : 1]$ du sous-groupe monogène de G engendré par a. Nous le noterons $o(a)$.

Exercice 1.

a) Donner un exemple de groupe et de sous-groupes dont la réunion n'est pas un sous-groupe.

b) Montrer que la réunion de deux sous-groupes H et K d'un groupe G est un sous-groupe, si et seulement si l'un des sous-groupes est contenu dans l'autre.

c) Montrer que la réunion H d'une famille totalement ordonnée $(H_i)_{i \in I}$ de sous-groupes de G est un sous-groupe de G.

Quelle est la réunion des sous-groupes $H_i = 10^{-i}\mathbb{Z}$, où $i \in \mathbb{N}$, de $(\mathbb{R}, +)$?

Solution. a) Dans $\mathbb{Z}$, la réunion des sous-groupes $2\mathbb{Z}$ et $3\mathbb{Z}$ n'est pas un sous-groupe. En effet, la somme $2 + 3 = 5$ de deux éléments n'est multiple ni de 2, ni de 3.

b) Si on a $H \subset K$ alors $H \cup K = K$ est un sous-groupe de G. De même si $K \subset H$.

Si on a $H \not\subset K$ et $K \not\subset H$, il existe $h \in H$ et $k \in K$ tels que $h \notin K$ et $k \notin H$. Si $H \cup K$ était un sous-groupe, on obtiendrait $hk \in H \cup K$, ce qui se traduirait par

$$(\exists\, h' \in H, \quad hk = h') \quad \text{ou} \quad (\exists\, k' \in K, \quad hk = k').$$

On obtiendrait $k = h^{-1}h' \in H$ ou $h = k'k^{-1} \in K$. C'est absurde.

c) $H \neq \emptyset$ car $H_i \neq \emptyset$. Soient $x, y \in H$. Il existe $i \in I$ et $j \in I$ tels que $x \in H_i$ et $y \in H_j$. La famille $(H_i)_{i \in I}$ étant totalement ordonnée, on a $H_i \subset H_j$ ou $H_j \subset H_i$. Si par exemple $H_i \subset H_j$, on voit que $x \in H_j$ et $y \in H_j$, d'où $x^{-1}y \in H_j \subset H$. On raisonne de même si $H_j \subset H_i$. Donc H est un sous-groupe de G.

La réunion des sous-groupes $H_i = 10^{-i}\mathbb{Z}$, de $(\mathbb{R}, +)$, est l'ensemble $\mathbb{D}$ des nombres décimaux (un nombre décimal est un rationnel admettant, parmi toutes les fractions qui le représentent, une expression de la forme $\frac{k}{10^m}$ avec $m \in \mathbb{N}$, $k \in \mathbb{Z}$.)

Exercice 2. Soit A une partie non vide du groupe G.

a) Montrer que $A' = \{ x \in G \mid \forall a \in A \quad xa = ax \}$ est un sous-groupe de G.

b) Soit α un automorphisme de G tel que $\alpha(A) = A$. Montrer que $\alpha(A') = A'$.

c) Montrer que le centre $Z(G)$ de G est un sous-groupe caractéristique de G.

Solution. a) On a $e \in A'$. Soient $x \in A'$ et $y \in A'$. Pour tout $a \in A$ on a

$$\begin{aligned}(x^{-1}y)a &= x^{-1}(ya) = x^{-1}(ay) = x^{-1}a(xx^{-1})y \\ &= x^{-1}(ax)x^{-1}y = x^{-1}(xa)x^{-1}y = (x^{-1}x)ax^{-1}y = a(x^{-1}y).\end{aligned}$$

Donc $x^{-1}y \in A'$ et A' est un sous-groupe de G.

b) De $\alpha(A) = A$, on déduit $A = \alpha^{-1}(A)$. Soit $x \in A'$. On a

$$\forall\, a \in A \qquad \alpha(x)a = \alpha[x\alpha^{-1}(a)] = \alpha[\alpha^{-1}(a)x] = a\alpha(x)$$

Cela prouve que $\alpha(x) \in A'$ et donc que $\alpha(A') \subset A'$. Puisque $A = \alpha^{-1}(A)$, ce résultat s'applique à α^{-1}. On obtient $\alpha^{-1}(A') \subset A'$, d'où $A' \subset \alpha(A')$ et donc $\alpha(A') = A'$.

c) Prenons $A = G$; alors $A' = Z(G)$. On applique b) pour tout $\alpha \in \mathrm{Aut}(G)$.

1.6 Noyau et image d'un homomorphisme

Lemme.

On considère deux groupes G, G', un homomorphisme $f : G \to G'$ et une partie non vide A de G. On a

$$\begin{aligned} f^{-1}(f(A)) &= A\,\mathrm{Ker}(f) = \mathrm{Ker}(f)\,A, && \textit{(en notation multiplicative)} \\ f^{-1}(f(A)) &= A + \mathrm{Ker}(f) = \mathrm{Ker}(f) + A && \textit{(en notation additive)}\end{aligned}$$

Démonstration. Montrons par exemple que $f^{-1}(f(A)) = A\,\mathrm{Ker}(f)$.

$$\begin{aligned} x \in f^{-1}(f(A)) &\Leftrightarrow f(x) \in f(A) \Leftrightarrow \exists a \in A \quad f(x) = f(a) \\ &\Leftrightarrow \exists a \in A \quad f(a^{-1}x) = e \Leftrightarrow \exists a \in A \quad a^{-1}x \in \mathrm{Ker}(f) \\ &\Leftrightarrow \exists a \in A \quad x \in a\,\mathrm{Ker}(f) \Leftrightarrow x \in A\mathrm{Ker}(f).\end{aligned}$$

∎

Proposition.

Soient G, G' deux groupes, d'éléments neutres e, e', et soit $f \in \mathrm{Hom}(G, G')$.

(i) *Si H est un sous-groupe de G alors $f(H)$ est un sous-groupe de G'.*
En particulier, l'image $\mathrm{Im}(f) = f(G)$ de f est un sous-groupe de G'.

(ii) *Si H' est un sous-groupe de G' alors $f^{-1}(H') = \{ x \in G \mid f(x) \in H' \}$ est un sous-groupe de G. Si H' est distingué, alors $f^{-1}(H')$ est distingué.*

(iii) *Le noyau $\mathrm{Ker}(f)$ de f est un sous-groupe distingué de G.*
Pour que f soit injectif, il faut et il suffit que $\mathrm{Ker}(f) = \{e\}$.

Démonstration. (i) D'abord $e' = f(e) \in f(H)$. Considérons $y \in f(H)$ et $y' \in f(H)$. Il existe $x \in H$ et $x' \in H$ tels que $f(x) = y$ et $f(x') = y'$. On a
$y^{-1}y' = f(x)^{-1}f(x') = f(x^{-1}x') \in f(H)$ car $x^{-1}x' \in H$.
Ainsi $f(H)$ est un sous-groupe de G'.

(ii) On a $e \in f^{-1}(H')$ car $f(e) = e' \in H'$. Considérons $x \in f^{-1}(H')$ et $x' \in f^{-1}(H')$. On a alors $f(x) \in H'$ et $f(x') \in H'$, d'où $f(x^{-1}x') = f(x)^{-1}f(x') \in H'$ et donc $x^{-1}x' \in f^{-1}(H')$. Cela prouve que $f^{-1}(H')$ est un sous-groupe de G.

Supposons $H' \lhd G'$. Pour tout $y \in G$ et pour tout $x \in f^{-1}(H')$, on a $yxy^{-1} \in f^{-1}(H')$ car $f(yxy^{-1}) = f(y)f(x)f(y)^{-1} \in H'$. Ainsi $f^{-1}(H')$ est distingué.
(iii) On a $\{e'\} \lhd G'$, d'où $\mathrm{Ker}\,(f) = f^{-1}(\{e'\}) \lhd G$, d'après (ii). D'après le lemme, on a $f^{-1}(f(\{a\})) = \{a\}$ pour tout $a \in G$, si et seulement si $\mathrm{Ker}\,(f) = \{e\}$. ∎

Exercice. On considère l'application $\mathrm{Ad} : x \mapsto \mathrm{Ad}_x$ du groupe G dans $\mathrm{Aut}\,(G)$.

a) Montrer que c'est un homomorphisme et préciser son noyau.

b) Montrer que son image $\mathrm{Int}\,(G)$ est distinguée dans le groupe $\mathrm{Aut}\,(G)$.

Solution.
a) $\forall\, x \in G \quad \forall\, x' \in G \quad \mathrm{Ad}_x \circ \mathrm{Ad}_{x'} = \mathrm{Ad}_{xx'}$. En effet,

$$\forall\, y \in G \quad (\mathrm{Ad}_x \circ \mathrm{Ad}_{x'})(y) = x(x'yx'^{-1})x^{-1} = (xx')y(xx')^{-1} = \mathrm{Ad}_{xx'}(y)\,.$$

Ainsi Ad est un homomorphisme. Il a pour noyau le centre $Z(G)$ de G car

$$\mathrm{Ad}_x = \mathrm{Id}_G \quad \Leftrightarrow \quad \forall y \in G\ xyx^{-1} = y \quad \Leftrightarrow \quad \forall y \in G\ xy = yx \quad \Leftrightarrow \quad x \in Z(G)\,.$$

b) $\mathrm{Int}\,(G) = \{\, \mathrm{Ad}_x\,;\ \ x \in G\,\}$ est l'image de l'homomorphisme Ad. C'est donc un sous-groupe de $\mathrm{Aut}\,(G)$. Soient $x \in G$ et $\alpha \in \mathrm{Aut}\,(G)$. Pour tout $y \in G$ on a :

$$(\alpha \circ \mathrm{Ad}_x \circ \alpha^{-1})(y) = \alpha(x\alpha^{-1}(y)x^{-1}) = \alpha(x)y\alpha(x)^{-1} = \mathrm{Ad}_{\alpha(x)}(y)\,.$$

Donc $\alpha \circ \mathrm{Ad}_x \circ \alpha^{-1} = \mathrm{Ad}_{\alpha(x)} \in \mathrm{Int}\,(G)$ et $\mathrm{Int}\,(G)$ est distingué dans $\mathrm{Aut}\,(G)$. La relation $\alpha \circ \mathrm{Ad}_x \circ \alpha^{-1} = \mathrm{Ad}_{\alpha(x)}$ montre que $Z(G) = \mathrm{Ker}\,(\mathrm{Ad})$ est caractéristique.

1.7 Indice d'un sous-groupe, théorème de Lagrange

Soient G un groupe et H un sous-groupe de G. Le lecteur vérifiera qu'en posant

$$xR_Hy \qquad \Leftrightarrow \qquad y^{-1}x \in H$$

on définit une relation d'équivalence sur G. La classe d'équivalence de $y \in G$ est

$$yH = \{yh\,;\ \ h \in H\,\}\,.$$

On définit de même une relation d'équivalence sur G en posant

$$xR'_Hy \qquad \Leftrightarrow \qquad xy^{-1} \in H\,.$$

La classe de $y \in G$ modulo R'_H est

$$Hy = \{hy\,;\ \ h \in H\,\}\,.$$

Si G est abélien, on a évidemment $R_H = R'_H$ et $xH = Hx$ pour tout $x \in G$. Par exemple, si $G = \mathbb{Z}$ et si $H = n\mathbb{Z}$, on retrouve la notion classique de *congruence* modulo n car $R_H = R'_H$, notée $\equiv$ et définie par

$$x \equiv y \qquad \Leftrightarrow \qquad x - y \in n\mathbb{Z}\,.$$

La classe de $y \in \mathbb{Z}$ est $y + H = y + n\mathbb{Z} = \{y + nk\,;\ \ k \in \mathbb{Z}\}$.

L'application $\varphi : x \mapsto x^{-1}$ est une bijection de G sur G. Elle vérifie $\varphi \circ \varphi = \mathrm{Id}_G$ et $\varphi(H) = H$. On a $\varphi(xH) = Hx^{-1}$ donc φ induit une bijection de l'ensemble G/R_H sur l'ensemble G/R'_H. Ces deux ensembles ont donc le même cardinal.

Définitions.

On appelle xH (resp. Hx) la classe à gauche (resp. à droite) de x modulo H.
L'ensemble G/R_H des classes à gauche modulo H se note G/H.
L'ensemble G/R'_H des classes à droite modulo H se note $G \setminus H$.
Le cardinal commun aux ensembles G/H et $G \setminus H$ s'appelle l'indice de H dans G.
Nous le noterons $[G : H]$. Si $H = \{e\}$, alors $[G : H]$ est l'ordre $[G : 1]$ de G.

Théorème. (de Lagrange)

Soient G un groupe fini et K, H deux sous-groupes de G tels que $K \subset H$. On a

$$[G : K] = [G : H]\,[H : K].$$

En particulier, pour tout sous-groupe H de G on a $[G : 1] = [G : H]\,[H : 1]$.

Démonstration. Dans H, l'équivalence modulo K (à gauche par exemple), crée une partition en classes, soit $H = \bigcup_{i\in I} h_i K$. L'équivalence modulo H partage de même G en classes $G = \bigcup_{j\in J} g_j H$. La translation $h \mapsto g_j h$ étant bijective de H sur $g_j H$, on a la partition $g_j H = \bigcup_{i\in I} g_j(h_i K)$ d'où la partition de G en classes modulo K :

$$G = \bigcup_{j\in J} g_j H = \bigcup_{j\in J}\bigcup_{i\in I} g_j(h_i K) = \bigcup_{(i,j)\in I\times J} g_j h_i K.$$

On peut supposer les indexations $i \mapsto h_i K$ et $j \mapsto g_j H$ bijectives. On a alors

$$\text{card}\,(I) = [H : K], \quad \text{card}\,(J) = [G : H], \quad \text{card}\,(I \times J) = [G : K],$$

d'où la formule de Lagrange. ∎

Corollaire.

Soit G un groupe fini. L'ordre $o(a)$ de tout élément a de G divise l'ordre $[G : 1]$.

Démonstration. Appliquer le th. de Lagrange au sous-groupe $H = \langle a \rangle$. ∎

Exercice. a) Soient G un groupe fini, K et M deux sous-groupes de G d'ordres k et m. Si k et m sont premiers entre eux, étudier l'intersection de K et M.

b) Pour $n \geqslant 1$, montrer que $\mathbb{U}_n = \{z \in \mathbb{C} \mid z^n = 1\}$ est un sous-groupe de $\mathbb{C}^*$.

c) Soient k, m des diviseurs de $n \geqslant 1$. Etudier $\mathbb{U}_k \cap \mathbb{U}_m$.

d) Dans l'anneau $\mathbb{C}[X]$, quel est le pgcd des polynômes $X^k - 1$ et $X^m - 1$?

e) Dans l'anneau $\mathbb{R}[X]$, quel est le pgcd des polynômes $X^k - 1$ et $X^m - 1$?

Solution.

a) $K \cap M$ est sous-groupe de K et de M. D'après le th. de Lagrange, son ordre divise k et m. On a donc $[K \cap M : 1] = 1$. On en déduit que $K \cap M = \{e\}$.

b) $f : z \mapsto z^n$ est un homomorphisme de $\mathbb{C}^*$ dans $\mathbb{C}^*$ car $(zz')^n = z^n z'^n$ pour tous $z \in \mathbb{C}^*$, $z' \in \mathbb{C}^*$. Son noyau $\mathbb{U}_n = \{z \in \mathbb{C} \mid z^n = 1\}$ est un sous-groupe de $\mathbb{C}^*$.

c) $z^k = 1 \quad \Rightarrow \quad z^n = (z^k)^{\frac{n}{k}} = 1$. On a donc $\mathbb{U}_k \subset \mathbb{U}_n$ et de même $\mathbb{U}_m \subset \mathbb{U}_n$. D'après le th. de Lagrange $[\mathbb{U}_k \cap \mathbb{U}_m : 1]$ divise $k = [\mathbb{U}_k : 1]$ et $m = [\mathbb{U}_m : 1]$. Il divise donc $d = \text{pgcd}(k, m)$. Par ailleurs, on a $\mathbb{U}_d \subset \mathbb{U}_k \cap \mathbb{U}_m$ donc $d = [\mathbb{U}_d : 1]$ divise $[\mathbb{U}_k \cap \mathbb{U}_m : 1]$. On en déduit que $d = [\mathbb{U}_k \cap \mathbb{U}_m : 1]$ et donc que $\mathbb{U}_d = \mathbb{U}_k \cap \mathbb{U}_m$.

d) $X^k - 1$ est produit de facteurs $(X - \lambda)$, où $\lambda \in \mathbb{U}_k$ et $X^m - 1$ est produit de facteurs $(X - \mu)$, où $\mu \in \mathbb{U}_m$. Leur pgcd est le produit des termes $(X - \lambda)$, où $\lambda \in \mathbb{U}_k \cap \mathbb{U}_m = \mathbb{U}_d$. Ainsi $\text{pgcd}(X^k - 1, X^m - 1) = X^d - 1$ où $d = \text{pgcd}(k, m)$.

e) Dans $\mathbb{R}[X]$, nous ne pouvons plus décomposer les deux polynômes comme produits de facteurs de degré un. Toutefois, le pgcd est le même car il est par ailleurs calculable par des divisions euclidiennes successives, qui donnent le même reste et le même quotient dans $\mathbb{C}[X]$ et dans $\mathbb{R}[X]$ en raison de l'unicité de la division dans $\mathbb{C}[X]$ (ch. 10).

1.8 Groupe quotient

Proposition.

Considérons un groupe G, un sous-groupe H de G et les relations d'équivalence R_H et R'_H introduites en 1-7. Les conditions suivantes sont équivalentes.

(i) *R_H est compatible avec la loi de composition interne de G.*

(ii) *R'_H est compatible avec la loi de composition interne de G.*

(iii) $R_H = R'_H$.

(iv) $xH = Hx$ *pour tout* $x \in G$.

(v) $xhx^{-1} \in H$ *pour tout* $x \in G$ *et pour tout* $h \in H$.

(vi) *H est distingué, soit* $\mathrm{Ad}_x(H) = H$ *pour tout* $x \in G$.

Si ces conditions sont vérifiées, le quotient G/H muni de l'opération quotient, est un groupe. L'application canonique $j : x \mapsto \overline{x}$ est un homomorphisme surjectif.

Démonstration. (i) $\Rightarrow$ (iii) Supposons R_H compatible avec l'opération de G.
Soient x et y dans G. Si $xR_H y$ alors $y^{-1}x \in H$ soit encore $y^{-1}xR_He$. On en déduit $y(y^{-1}x)y^{-1}R_H yey^{-1}$, c'est-à-dire $xy^{-1}R_H e$ soit encore $xy^{-1} \in H$ ce qui équivaut à $xR'_H y$.

De manière analogue, on vérifiera que $xR'_H y \Rightarrow xR_H y$ et donc que $R_H = R_{H'}$.

(ii) $\Rightarrow$ (iii) en raisonnant de manière analogue.

(iii) $\Leftrightarrow$ (iv) car les classes modulo R_H (resp. R'_H) sont les parties xH (resp. Hx) de G.

(iv) $\Leftrightarrow$ (vi) Les translations à droite étant bijectives, pour tout $x \in G$ on a

$$xH = Hx \quad \Leftrightarrow \quad xHx^{-1} = Hxx^{-1} \quad \Leftrightarrow \quad xHx^{-1} = H\,.$$

(vi) $\Rightarrow$ (v) est évident.

(v) $\Rightarrow$ (i) Si xR_Hx' et yR_Hy' alors $\exists\, h_1, h_2 \in H \quad x = x'h_1 \quad y = y'h_2$. D'où $xy = x'h_1y'h_2 = x'y'(y'^{-1}h_1y')h_2$ soit $xy \in x'y'H$ ce qui signifie $xyR_Hx'y'$.

(v) $\Rightarrow$ (ii) de manière analogue.

Enfin, G/H est un groupe et j est un homomorphisme, d'après 1-2, prop. ∎

Corollaire.

Soit H un sous-groupe du groupe G. Si $[G : H] = 2$, on a $H \triangleleft G$.

Démonstration. Soit $a \in G$. Si $a \in H$, on a $Ha = H = aH$. Si $a \notin H$, l'indice de H étant 2, la partition de G en classes à gauche (resp. à droite) est $G = H \cup Ha$ (resp. $G = H \cup aH$). On a donc $Ha = H^c = aH$. La condition (iv) est vérifiée. ∎

Exercice. Soient H, K deux sous-groupes du groupe G. Supposons H distingué.

a) Montrer que $HK = KH$ et que HK est un sous-groupe de G.

b) Si H et K sont distingués, montrer que HK est distingué.

Solution. a) Considérons l'homomorphisme $j : x \mapsto \overline{x}$, de G sur le groupe G/H. Il a pour noyau H. Alors $j(K)$ est un sous-groupe de G/H et $j^{-1}(j(K))$ est un sous-groupe de G. Or nous savons (1-6, lemme) que $j^{-1}(j(K)) = HK = KH$.

b) Puisque j est surjectif, on a $j(K) \triangleleft G/H$ et donc $HK = j^{-1}(j(K)) \triangleleft G$.

1.9 Factorisation des homomorphismes

Proposition.

Considérons un groupe G, un sous-groupe distingué H de G et l'homomorphisme canonique j de G sur G/H. Soit $f : G \to G'$ un homomorphisme de groupes. Si $H \subset Ker(f)$, il existe un homomorphisme $\overline{f} : G/H \to G'$, unique, tel que $\overline{f} \circ j = f$. Le noyau de $\overline{f}$ est $j(Ker(f))$ et l'image de $\overline{f}$ est égale à celle de f.

Démonstration. Comme f est constante sur H, de valeur l'élément neutre e' de G', on voit que f est constante sur toute classe $\overline{x} = xH = \{xh ; \quad h \in H\}$ modulo H. D'après 1-1, il existe une application $\overline{f}$ de $G/R_H = G/H$ dans G', unique, telle que $\overline{f} \circ j = f$. C'est un homomorphisme car pour tout $x \in G$ et pour tout $y \in G$, on a :

$$\overline{f}(\overline{x}\,\overline{y}) = \overline{f}(\overline{xy}) = f(xy) = f(x)f(y) = \overline{f}(\overline{x})\,\overline{f}(\overline{y}).$$

On a $\mathrm{Im}\left(\overline{f}\right) = \mathrm{Im}\,(f)$ car $\overline{f}(\overline{x}) = f(x)$ pour tout $x \in G$. On a $\mathrm{Ker}\left(\overline{f}\right) = j(\mathrm{Ker}\,(f))$ car

$$\overline{f}(\overline{x}) = e' \quad \Leftrightarrow \quad f(x) = e' \quad \Leftrightarrow \quad x \in \mathrm{Ker}\,(f).$$ ∎

Corollaire 1.

Soient G et G' deux groupes et $f \in Hom\,(G, G')$. Les groupes $G/Ker\,(f)$ et $f(G)$ sont isomorphes. Si G et G' sont finis, l'ordre de $f(G)$ divise $[G : 1]$ et $[G' : 1]$.

Démonstration. Utilisons la proposition avec $H = \mathrm{Ker}\,(f) \lhd G$. Le noyau de $\overline{f}$ se réduit à l'élément neutre de $G/\mathrm{Ker}\,(f)$ donc $\overline{f}$ est injectif. C'est un isomorphisme de $G/\mathrm{Ker}\,(f)$ sur $f(G)$. Si G et G' sont finis, $[f(G) : 1] = [G/\mathrm{Ker}\,(f) : 1] = [G : \mathrm{Ker}\,(f)]$ divise l'ordre de G d'après le th. de Lagrange. Il divise également $[G' : 1]$. ∎

Corollaire 2.

Soient H, K deux sous-groupes distingués du groupe G tels que $K \subset H$. Il existe un isomorphisme naturel de $(G/K)/(H/K)$ sur G/H.

Démonstration. Pour tout $x \in G$, notons $\overline{x}$ sa classe modulo H et $\overset{\circ}{x}$ sa classe modulo K. L'homomorphisme canonique $f : x \mapsto \overline{x}$ de G sur G/H a pour noyau H qui contient K. Il existe donc un homomorphisme $\overline{f} : G/K \to G/H$ tel que $\overline{f}(\overset{\circ}{x}) = \overline{x}$ pour tout $x \in G$. Il est surjectif car $\overline{f}$ a la même image que f. On a $\mathrm{Ker}\left(\overline{f}\right) = \{\overset{\circ}{x} ; \quad x \in H\} = H/K$. On factorise $\overline{f}$ à travers son noyau H/K. On obtient l'isomorphisme cherché. ∎

Exercice 1. Montrer que les groupes $\mathbb{R}/\mathbb{Z}$ et $\mathbb{U} = \{z \in \mathbb{C} \mid |z| = 1\}$ sont isomorphes.

Solution. Puisque $\mathbb{R}$ est commutatif, le sous-groupe $\mathbb{Z}$ est distingué. Notons p l'homomorphisme canonique $x \mapsto \overline{x}$ de $\mathbb{R}$ sur le groupe quotient $\mathbb{R}/\mathbb{Z}$. On sait que $f : x \mapsto \exp(2i\pi x)$ est un homomorphisme surjectif du groupe additif $\mathbb{R}$ sur le groupe multiplicatif $\mathbb{U}$ et que $\mathrm{Ker}\,(f) = \{x \in \mathbb{R} \mid e^{2i\pi x} = 1\} = \mathbb{Z}$. Factorisons f. Il existe un isomorphisme $\overline{f}$ de $\mathbb{R}/\mathbb{Z}$ sur $\mathbb{U}$ tel que $f = \overline{f} \circ p$. Ainsi $\mathbb{R}/\mathbb{Z}$ muni de l'opération quotient définie par $\overline{x} + \overline{y} = \overline{x+y}$ est identifiable avec $\mathbb{U}$.

En 1-1, nous avons déjà étudié le groupe $\mathbb{R}/\mathbb{Z}$ et montré qu'il s'identifie naturellement avec $[0, 1[$ muni de l'opération $(x, y) \mapsto (x + y) - E(x + y)$. L'isomorphisme $\overline{f}$ de $[0, 1[$ sur $\mathbb{U}$ est alors la restriction $x \mapsto \exp(2i\pi x)$ de f à $[0, 1[$.

Exercice 2. Etudier $\mathrm{Hom}(\mathbb{U}_{10}, \mathbb{U}_7)$ et $\mathrm{Hom}(\mathbb{U}_{10}, \mathbb{U}_6)$.

Solution. D'après le cor. 1, si $f \in \mathrm{Hom}(G, G')$, l'ordre de $f(G)$ divise $[G : 1]$ et $[G' : 1]$. Si les ordres de G et G' sont premiers entre eux, on a $f(G) = \{e\}$ et f est l'homomorphisme trivial $f_0 : x \mapsto e$. Ainsi $\mathrm{Hom}(\mathbb{U}_{10}, \mathbb{U}_7) = \{f_0\}$.

Considérons $f \in \mathrm{Hom}(\mathbb{U}_{10}, \mathbb{U}_6)$. L'ordre de $f(\mathbb{U}_{10})$ divise le pgcd de $[\mathbb{U}_{10} : 1] = 10$ et $[\mathbb{U}_6 : 1] = 6$. On a donc $[f(\mathbb{U}_{10}) : 1] = 1$ ou 2. Si $[f(\mathbb{U}_{10}) : 1] = 1$ alors $f = f_0$ est trivial. Si $[f(\mathbb{U}_{10}) : 1] = 2$ alors nécessairement $f(\mathbb{U}_{10}) = \{1, -1\}$ seul sous-groupe d'ordre 2 de $\mathbb{U}_6$. Posons $\zeta = \exp(\frac{2i\pi}{10})$. On devra avoir $f(\zeta) = -1$ (si $f(\zeta) = 1$ alors $f(\zeta^k) = 1$ pour tout k et f est trivial) et $f(\zeta^k) = (-1)^k$ pour tout k. Réciproquement, cette relation définit une application f de $\mathbb{U}_{10}$ dans $\{1, -1\}$. En effet, si $z \in \mathbb{U}_{10}$, il existe $k \in \mathbb{Z}$ tel que $z = \zeta^k$ et si $k' \in \mathbb{Z}$ est tel que $\zeta^k = \zeta^{k'}$, alors on a $k' \equiv k \pmod{10}$ et donc $(-1)^k = (-1)^{k'}$. Ainsi, f est bien définie. C'est un homomorphisme de $\mathbb{U}_{10}$ sur $\{1, -1\} \subset \mathbb{U}_6$ car $f(\zeta^k\zeta^{k'}) = f(\zeta^{k+k'}) = (-1)^{k+k'} = (-1)^k(-1)^{k'} = f(\zeta^k)f(\zeta^{k'})$. Donc $\mathrm{Hom}(\mathbb{U}_{10}, \mathbb{U}_6) = \{f_0, f\}$.

1.10 Produit direct de groupes

Proposition.

Soient H, K deux groupes. Pour tous $(h,k), (h',k') \in H \times K$ posons

$$(h,k)(h',k') = (hh', kk').$$

(i) *$G = H \times K$ muni de cette opération est un groupe.*

(ii) *Les projections canoniques $p : H \times K \to H$ et $q : H \times K \to K$ sont des homomorphismes surjectifs.*

(iii) *Les injections $\varphi : h \mapsto (h, e)$ et $\psi : k \mapsto (e, k)$ sont des isomorphismes de H sur $H' = H \times \{e\} = Ker(q)$ et de K sur $K' = \{e\} \times K = Ker(p)$.*

(iv) *Tout élément de H' commute avec tout élément de K' et on a*

$$H' \lhd G \quad , \quad K' \lhd G \quad , \quad H'K' = G \quad , \quad H' \cap K' = \{e\}.$$

Démonstration. Nous laissons les vérifications au lecteur. Notons que par factorisation des homomorphismes p et q à travers leur noyau, on voit que $(H \times K)/K$ est isomorphe à H et que $(H \times K)/H'$ est isomorphe à K. ∎

Définition.

Ce groupe $H \times K$ est appelé le produit direct des groupes H et K.

Plus généralement, soit $(H_i)_{i \in I}$ une famille de groupes. L'ensemble $G = \prod_{i \in I} H_i$ est un groupe si on définit le produit de $(x_i)_{i \in I}$ et $(y_i)_{i \in I}$ comme étant $(x_i y_i)_{i \in I}$. Les groupes H_i sont alors isomorphes à des sous-groupes distingués H_i' du produit.

Exercice. Soient E un ensemble, f la bijection de $\mathcal{P}(E)$ sur $\{0,1\}^E$ associant à toute partie A de E sa fonction indicatrice 1_A, (de valeur 1 sur A et 0 sur le complémentaire A^c de A). On identifie $\{0,1\}$ au groupe $\mathbb{Z}/2\mathbb{Z} = \{\overline{0}, \overline{1}\}$. On munit $G = \{\overline{0}, \overline{1}\}^E = (\mathbb{Z}/2\mathbb{Z})^E$ de la structure de groupe produit et on transporte cette structure de G à l'aide de f. Quelle structure de groupe obtient-on sur $\mathcal{P}(E)$?

Solution. Soient E, F des ensembles. L'ensemble $\mathcal{F}(E,F)$ des applications de E dans F s'identifie à F^E, en associant à toute application $\varphi \in \mathcal{F}(E,F)$ la famille $(\varphi(x))_{x\in E} \in F^E$ de ses valeurs. Les fonctions indicatrices 1_A des parties A de E, sont les applications de E dans $\{0,1\}$. Elles s'identifient avec les éléments de $G = \{0,1\}^E$. Identifions $\{0,1\}$ et $\mathbb{Z}/2\mathbb{Z} = \{\overline{0},\overline{1}\}$. Alors $\mathcal{F}(E,\{\overline{0},\overline{1}\}) = \{\overline{0},\overline{1}\}^E$ peut être muni de la structure de groupe produit, dont l'opération est définie, pour $\varphi \in \mathcal{F}(E,\{\overline{0},\overline{1}\})$ et $\psi \in \mathcal{F}(E,\{\overline{0},\overline{1}\})$, par

$$(1) \qquad (\varphi(x))_{x\in E} + (\psi(x))_{x\in E} = (\varphi(x)+\psi(x))_{x\in E} = ((\varphi+\psi)(x))_{x\in E}\,.$$

Pour $A, B \in \mathcal{P}(E)$ nous devons déterminer $f^{-1}(f(A)+f(B)) \in \mathcal{P}(E)$, c'est-à-dire la partie de E dont la fonction caractéristique à valeurs dans $\mathbb{Z}/2\mathbb{Z}$ est $1_A + 1_B$, somme calculée selon la formule (1).

- Pour $x \in A \cap B$ on a $1_A(x)+1_B(x) = \overline{1}+\overline{1} = \overline{0}$.
- Pour $x \in A \cap B^c$ on a $1_A(x)+1_B(x) = \overline{1}+\overline{0} = \overline{1}$.
- Pour $x \in A^c \cap B$ on a $1_A(x)+1_B(x) = \overline{0}+\overline{1} = \overline{1}$.
- Pour $x \in A^c \cap B^c$ on a $1_A(x)+1_B(x) = \overline{0}+\overline{0} = \overline{0}$.

On voit que l'on a obtenu la fonction caractéristique de la différence symétrique $A\Delta B = (A \setminus B) \cup (B \setminus A)$. Cela montre que $\mathcal{P}(E)$ muni de l'opération Δ est un groupe commutatif isomorphe par f au groupe $(\mathbb{Z}/2\mathbb{Z})^E$. On en déduit par exemple, que Δ est une opération associative, qu'elle a pour élément neutre la partie correspondant à $(\overline{0})_{x\in E}$, c'est-à-dire la partie vide (de fonction caractéristique nulle). L'inverse de $A \in \mathcal{P}(E)$, pour l'opération Δ est A car $1_A + 1_A = 0$ (on a $A\Delta A = \emptyset$).

Notons que $\mathbb{Z}/2\mathbb{Z}$ possède non seulement une addition mais aussi une multiplication définie par $\overline{x}\ \overline{y} = \overline{xy}$. C'est un anneau. De ce fait, $(\mathbb{Z}/2\mathbb{Z})^E = \mathcal{F}(E,\{\overline{0},\overline{1}\})$ est un anneau (anneau produit). L'opération qui correspond par f au produit $1_A 1_B$ (dont les valeurs sont calculées modulo 2) est la partie $A \cap B$ de E. Ainsi, $(\mathcal{P}(E), \Delta, \cap)$ est un anneau, isomorphe à $(\mathbb{Z}/2\mathbb{Z})^E$ (voir Ex. 9-1).

1.11 Caractérisation du produit direct

Proposition.

Soient G un groupe et H, K deux sous-groupes. On suppose que

$$H \lhd G \quad , \quad K \lhd G \quad , \quad HK = G \quad , \quad H \cap K = \{e\}\,.$$

Alors, $f : (h,k) \mapsto hk$ est un isomorphisme de groupes de $H \times K$ sur G.

Démonstration. Du fait que $G = HK$, pour tout $x \in G$ il existe $h \in H$ et $k \in K$ tels que $x = hk$. Cette expression de x est unique. En effet, si $x = h'k'$ avec $h' \in H$ et $k' \in K$, on a $hk = h'k'$, d'où $h^{-1}h' = kk'^{-1} \in H \cap K = \{e\}$. On en déduit que $h = h'$ et $k = k'$. Ainsi, $f : (h,k) \mapsto hk$ est bijective de $H \times K$ sur $HK = G$.

Comme H et K sont distingués, pour tout $h \in H$ et pour tout $k \in K$, on a :

$$h(h^{-1}kh) = kh = (khk^{-1})k \qquad \text{avec} \qquad khk^{-1} \in H \quad , \quad h^{-1}kh \in K\,.$$

L'unicité de l'expression de $kh \in G = HK$ impose $h = khk^{-1}$ soit $hk = kh$ et cela pour tout $h \in H$ et tout $k \in K$. Pour tous $h, h' \in H$ et $k, k' \in K$, on en déduit :

$$f((h,k)(h',k')) = f(hh',kk') = hh'kk' = hkh'k' = f(h,k)f(h',k')\,.$$

Donc f est un homomorphisme de groupes. C'est un isomorphisme de $H \times K$ sur G. ∎

Exercice. Montrer que le groupe commutatif $\mathbb{U}_6$ (des racines sixièmes de l'unité dans $\mathbb{C}^*$) est isomorphe au groupe $\mathbb{U}_2 \times \mathbb{U}_3$. Généraliser cet énoncé.

Solution. $H = \mathbb{U}_2$ et $K = \mathbb{U}_3$ sont des sous-groupes de $\mathbb{U}_6$. Leurs ordres étant premiers entre eux, $H \cap K = \{e\}$ (voir 1-7, ex.). Comme $\mathbb{U}_6$ est commutatif, HK est un sous-groupe (voir 1-8, ex.). Il contient H et K. Son ordre est donc divisible par $2 = [H : 1]$, par $3 = [K : 1]$, et donc par $\mathrm{ppcm}(3, 2) = 6$. On en déduit que $HK = \mathbb{U}_6$. D'après la proposition, $(z, z') \mapsto zz'$ est un isomorphisme de $\mathbb{U}_2 \times \mathbb{U}_3$ sur $\mathbb{U}_6$. Tout élément de $\mathbb{U}_6$ s'écrit de manière unique comme produit zz' avec $z \in \mathbb{U}_2$ et $z' \in \mathbb{U}_3$.

Si $n = dd'$, avec d et d' premiers entre eux, la même démonstration prouve que $(z, z') \mapsto zz'$ est un isomorphisme de $\mathbb{U}_d \times \mathbb{U}_{d'}$ sur $\mathbb{U}_n$.

1.12 Procédé de symétrisation

Nous allons détailler une construction algébrique formelle de $\mathbb{Z}$ à partir de $\mathbb{N}$. Si on pense à un entier relatif comme exprimant le bilan d'une soustraction $x - y$ de deux entiers naturels x, y, un autre couple (x', y') conduit au même bilan lorsque $x' - y' = x - y$ dans $\mathbb{Z}$. On doit donc considérer comme équivalents deux couples (x, y) et (x', y') de $\mathbb{N} \times \mathbb{N}$ tels que $x + y' = y + x'$.

Proposition.

Soit S un ensemble muni d'une addition associative, commutative, avec un élément neutre 0 et régulière. Sur $S \times S$ la loi de composition définie par

$$(x, y) * (x', y') = (x + x', y + y')$$

est compatible avec la relation d'équivalence définie par

$$(x, y)\, R\, (x', y') \quad \Leftrightarrow \quad x + y' = y + x'.$$

Le quotient $G = (S \times S)/R$ muni de l'opération quotient, que nous noterons additivement, est un groupe commutatif. L'application φ associant à tout $x \in S$ la classe de $(x, 0)$ modulo R est injective, telle que $\varphi(x + x') = \varphi(x) + \varphi(x')$ pour tous $x, x' \in S$. Elle permet d'identifier S avec une partie de G. On a alors $G = S - S$.

Le couple (G, φ) possède la propriété universelle suivante :

(P) *Si une application f de S dans un groupe commutatif G' est telle que $f(x + x') = f(x) + f(x')$ pour tout $x \in S$, tout $x' \in S$, il existe une application $\overline{f}$ unique de G dans G' prolongeant f et telle que $\overline{f}(x + x') = \overline{f}(x) + \overline{f}(x')$ pour tout $x \in G$ et pour tout $x' \in G$.*

Démonstration. Vérifions que R est transitive.

$$\begin{aligned}
&(x, y)\, R\, (x', y') \quad \text{et} \quad (x', y')\, R\, (x'', y'') \\
&\quad \Leftrightarrow \quad x + y' = y + x' \quad \text{et} \quad x' + y'' = y' + x'' \\
&\quad \Rightarrow \quad x + y' + y'' = y + x' + y'' \quad \text{et} \quad y + x' + y'' = y + y' + x'' \\
&\quad \Rightarrow \quad x + y' + y'' = y + y' + x'' \\
&\quad \Rightarrow \quad x + y'' = y + x'' \qquad \text{(car l'addition dans } S \text{ est régulière)} \\
&\quad \Leftrightarrow \quad (x, y)\, R\, (x'', y'').
\end{aligned}$$

La symétrie de R et la réflexivité de R sont évidentes. Donc R est une relation d'équivalence. Elle est compatible avec l'opération introduite sur $S \times S$ car :

$$\begin{aligned}
&(x_1,y_1)\,R\,(x_1',y_1') \quad \text{et} \quad (x_2,y_2)\,R\,(x_2',y_2')\\
&\quad\Leftrightarrow\quad x_1+y_1' \,=\, y_1+x_1' \quad \text{et} \quad x_2+y_2' \,=\, y_2+x_2'\\
&\quad\Rightarrow\quad x_1+x_2+y_1'+y_2' \,=\, y_1+y_2+x_1'+x_2'\\
&\quad\Leftrightarrow\quad [(x_1,y_1)*(x_2,y_2)]\;R\;[(x_1',y_1')*(x_2',y_2')]\,.
\end{aligned}$$

L'opération $*$ est associative, commutative, avec élément neutre $(0,0)$. D'après 1-2, le quotient sur $G=(S\times S)/R$ hérite de ces propriétés. Pour tout $\overline{(x,y)}\in G$, on a

$$\overline{(x,y)} \,+\, \overline{(y,x)} \;=\; \overline{(x+y,y+x)} \;=\; \overline{(0,0)}\,.$$

Tout élément $\overline{(x,y)}$ de G a donc pour opposé $\overline{(y,x)}$. Ainsi, G est un groupe.

L'application φ est injective car :

$$\varphi(x) \,=\, \varphi(y) \quad\Leftrightarrow\quad (x,0)\,R\,(y,0) \quad\Leftrightarrow\quad x+0 \,=\, 0+y \quad\Leftrightarrow\quad x \,=\, y\,.$$

On a $G=S-S$. En effet tout élément $\overline{(x,y)}$ peut s'écrire

$$\overline{(x,y)} \;=\; \overline{(x,0)*(0,y)} \;=\; \overline{(x,0)} \,+\, \overline{(0,y)} \;=\; \varphi(x)-\varphi(y)\,.$$

Pour vérifier (P), considérons $F : S\times S\to G'$ définie par $F(x,y)=f(x)-f(y)$. Comme F est constante sur les classes modulo R, elle définit par factorisation, une application $\overline{f}$ de S/R dans G' qui a les propriétés annoncées. ∎

Définition.

Le groupe G est appelé le symétrisé de S.

Remarque. Des axiomes habituellement considérés en théorie des ensembles (comme ceux de Peano), on déduit l'existence de $\mathbb{N}$ et ses propriétés. Nous venons de construire $\mathbb{Z}$ par un procédé algébrique. Nous verrons au ch. 9 que le corps $\mathbb{Q}$ se construit algébriquement à partir de $\mathbb{Z}$. La construction de $\mathbb{R}$ à partir de $\mathbb{Q}$ s'effectue par un procédé de complétion dans le cadre des espaces métriques. La construction de $\mathbb{C}$ à partir de $\mathbb{R}$ est algébrique et sera étudiée au ch. 11. Ainsi, à la fin de ce cours d'algèbre, nous aurons vu comment déduire de la théorie des ensembles les objets $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ ... sur lesquels repose l'essentiel des mathématiques.

1.13 Sous-groupes de $\mathbb{Z}$ et de $\mathbb{R}$

Définition.

Le symétrisé de $\mathbb{N}$ se note $\mathbb{Z}$. Ses éléments s'appellent les entiers relatifs.

Soit $x\in\varphi(\mathbb{N})\cap(-\varphi(\mathbb{N}))$. Il existe $a,b\in\mathbb{N}$ tels que $x=\overline{(a,0)}=\overline{(0,b)}$. On a $(a,0)R(0,b)$ soit $a+b=0$ et donc $a=0$, $b=0$. Ainsi $\varphi(\mathbb{N})\cap(-\varphi(\mathbb{N}))=\{0\}$.

L'ordre de $\mathbb{N}$ étant total, pour tout élément $\overline{(x,y)}$ de $\mathbb{Z}$, où $x,y\in\mathbb{N}$, on a

- soit $x\geqslant y$ et alors $\overline{(x,y)}=\overline{(x-y,0)}\in\varphi(\mathbb{N})$,
- soit $x\leqslant y$ et alors $\overline{(x,y)}=\overline{(0,y-x)}\in-\varphi(\mathbb{N})$.

Cela prouve que $\varphi(\mathbb{N})\cup(-\varphi(\mathbb{N}))=\mathbb{Z}$. D'après 1-12, l'application $\varphi : x\mapsto\overline{(x,0)}$ étant injective de $\mathbb{N}$ dans $\mathbb{Z}$, nous pouvons identifier $\mathbb{N}$ avec $\varphi(\mathbb{N})\subset\mathbb{Z}$. On a alors

$$\mathbb{N}\subset\mathbb{Z} \qquad,\qquad \mathbb{N}\cup(-\mathbb{N})=\mathbb{Z} \qquad,\qquad \mathbb{N}\cap(-\mathbb{N})=\{0\}\,.$$

Soient $x,y\in\mathbb{Z}$. En posant $x\leqslant y$ si $y-x\in\mathbb{N}$ on définit sur $\mathbb{Z}$ une relation d'ordre total compatible avec l'addition. On dit que $\mathbb{Z}$ est un *groupe totalement ordonné*.

En outre, le lecteur vérifiera que $(x_1, y_1)\,(x_2, y_2) = (x_1x_2 + y_1y_2\ ,\ x_1y_2 + x_2y_1)$ est une opération sur $\mathbb{N} \times \mathbb{N}$, associative, commutative, d'élément neutre $(1, 0)$ qui distribue $*$. Elle est compatible avec la relation d'équivalence R considérée en 1-12. D'après 1-1, ces propriétés se transmettent à $\mathbb{Z} = (\mathbb{N} \times \mathbb{N})/R$. Ainsi, non seulement $\mathbb{Z}$ est un groupe additif mais c'est un *anneau*, structure qui sera étudiée dans la partie III.

Proposition 1.

Les sous-groupes de $(\mathbb{Z}, +)$ sont les sous-ensembles $n\mathbb{Z}$, où $n \in \mathbb{N}$.

Démonstration. On a $0 \in n\mathbb{Z}$. Soient x, $x' \in n\mathbb{Z}$. Il existe k, $k' \in \mathbb{Z}$ tels que $x = nk$, $x' = nk'$. Alors $x - x' = n(k - k') \in n\mathbb{Z}$. Donc $n\mathbb{Z}$ est un sous-groupe de $\mathbb{Z}$.

Réciproquement, soit H un sous-groupe de $\mathbb{Z}$. Si $H = \{0\}$, alors $H = 0\mathbb{Z}$. Si $H \neq \{0\}$, il existe $x \neq 0$ dans H. On a aussi $-x \in H$ donc $H \cap \mathbb{N}^* \neq \emptyset$. Soit n le plus petit élément de $H \cap \mathbb{N}^*$. Pour tout $k \in \mathbb{N}$ on a $nk = n + \cdots + n \in H$ et $n(-k) = -(nk) \in H$. Cela prouve que $n\mathbb{Z} \subset H$. Soit $x \in H$, positif. La division par n donne $x = nq + r$ avec $0 \leqslant r < n$ et $q \in \mathbb{N}$. On en déduit que $r = x - (n + \cdots + n) \in H$ avec $0 \leqslant r < n$. Si r était non nul, le fait que n est le plus petit élément de $H \cap \mathbb{N}^*$ serait contredit. Donc $r = 0$ et $x = nq \in n\mathbb{Z}$. Si $x \in H$ est négatif, alors $-x \in H$ est positif et donc élément de $n\mathbb{Z}$. Ainsi, on a $H \subset n\mathbb{Z}$ et donc $H = n\mathbb{Z}$. ∎

Proposition 2.

Un sous-groupe de $\mathbb{R}$ est partout dense dans $\mathbb{R}$ ou de la forme $a\mathbb{Z}$, où $a \in \mathbb{R}_+$.

Démonstration. Soit H un sous-groupe de $\mathbb{R}$. Supposons $H \neq \{0\}$. Il existe $x_0 \neq 0$ dans H. Quitte à remplacer x_0 par $-x_0$, on peut supposer $x_0 > 0$. On a donc $H^+ = \{x \in H \mid x > 0\} \neq \emptyset$. Posons $a = \inf H^+$.

Supposons tout d'abord que $a \in H^+$ et que $a > 0$. Pour tout $k \in \mathbb{N}^*$ on a $ka = a + \cdots + a \in H$ et donc $\mathbb{Z}a \subset H$. Par ailleurs, pour tout $k \in \mathbb{Z}$, $]ka, (k+1)a[$ ne contient aucun élément h de H, sinon $x = h - ka \in H$ vérifierait $0 < x < a$ contredisant le fait que a est le plus petit élément de H^+. Donc $\mathbb{Z}a = H$ et $\mathbb{Z}a$ discret est fermé dans $\mathbb{R}$.

Supposons que $a \notin H^+$ ou que $a = 0$. La borne inférieure de H^+ est adhérente à H^+. Pour tout $\varepsilon > 0$, il existe $x \in H^+$ tel que $x - a < \varepsilon$, puis $y \in H^+$ tel que $0 < y < x$. On a alors $0 < x - y < \varepsilon$. Ainsi, pour tout $\varepsilon > 0$ on peut trouver $h \in H$ tel que $0 < h < \varepsilon$. Alors $\mathbb{Z}h$ est une progression arithmétique de pas $h < \varepsilon$ contenue dans H. On voit que H est partout dense dans $\mathbb{R}$: pour tout $t \in \mathbb{R}$ et pour tout $\varepsilon > 0$, en choisissant h comme ci-dessus pour cette valeur de ε, $]t - \varepsilon, t + \varepsilon[$ de longueur 2ε contient un élément de $\mathbb{Z}h$. ∎

Exercice. Montrer qu'un sous-groupe H de $\mathbb{U} = \{z \in \mathbb{C} \mid |z| = 1\}$ est soit fini, et alors égal à $\mathbb{U}_n$ où n est son ordre, soit partout dense dans $\mathbb{U}$.

Solution. Si H est fini d'ordre n, $H = \mathbb{U}_n$ (voir 1-14, ex. 1). Si H est infini, dans $\mathbb{U}$ compact, il admet un point d'accumulation l. Paramétrons $\mathbb{U}$ par la bijection continue $x \mapsto e^{i\pi x}$ de $[l-1, l+1[$ sur $\mathbb{U}$. Pour tout $\varepsilon > 0$, avec $\varepsilon < 1$, il existe $x \in H$ et $x' \in H$ tels que $x \neq x'$ avec x et x' dans le voisinage $]l - \varepsilon, l + \varepsilon[$ de l. On a $h = x' - x \in H$ et $|h| < \varepsilon$. Comme pour $\mathbb{R}$ ci-dessus, on voit que H est dense dans $\mathbb{U}$.

1.14 Sous-groupe engendré par un élément

Proposition.

Soient G un groupe et $a \in G$. L'application $f : k \mapsto a^k$ est un homomorphisme de $\mathbb{Z}$ sur le sous-groupe $\langle a \rangle$ engendré par a. Si f est injectif, alors $\langle a \rangle$ est isomorphe à $\mathbb{Z}$. Si f n'est pas injectif, $\langle a \rangle$ est isomorphe à $\mathbb{Z}/n\mathbb{Z}$, où $n \in \mathbb{N}^*$ est le plus petit entier non nul tel que $a^n = e$. Dans ce cas, les entiers k tels que $a^k = e$ sont les multiples de n et $\langle a \rangle = \{e, a, \ldots, a^{n-1}\}$.

Démonstration. L'application $f_0 : k \mapsto a^k$ de $\mathbb{N}$ dans $\langle a \rangle$ vérifie

$$\forall\, k \in \mathbb{N} \quad \forall\, k' \in \mathbb{N} \qquad f_0(k+k') = a^{k+k'} = a^k a^{k'} = f_0(k) f_0(k') .$$

La propriété universelle du symétrisé $\mathbb{Z}$ de $\mathbb{N}$ permet de prolonger f_0 en un homomorphisme f de $\mathbb{Z}$ dans $\langle a \rangle$. Pour $k = -|k| < 0$, on a $f(-|k|) = f(|k|)^{-1} = (a^{|k|})^{-1} = a^k$ (considéré en 1-2). On a donc $\mathrm{Im}\,(f) = \{a^k\,;\ k \in \mathbb{Z}\} = \langle a \rangle$.

D'après 1-13, il existe $n \in \mathbb{N}$ tel que $\mathrm{Ker}\,(f) = n\mathbb{Z}$. Si $n = 0$, f est injective. C'est un isomorphisme de $\mathbb{Z}$ sur $\langle a \rangle$. Si $n \neq 0$, par factorisation de f à travers son noyau $n\mathbb{Z}$, on obtient un isomorphisme $\overline{f}$ du groupe $\mathbb{Z}/n\mathbb{Z}$ sur $\langle a \rangle$. Le noyau de f est l'ensemble des $k \in \mathbb{Z}$ tels que $a^k = e$, c'est-à-dire l'ensemble $n\mathbb{Z}$ des multiples de n. Comme $0, 1, \ldots, n-1$ sont des représentants des n classes modulo $n\mathbb{Z}$, leurs images $e = a^0$, a, $\ldots$, a^{n-1} par $\overline{f}$ sont les éléments de $\mathrm{Im}\left(\overline{f}\right) = \mathrm{Im}\,(f) = \langle a \rangle$. ∎

Définition.

Dans le cas où il existe des entiers $k > 0$ tels que $a^k = e$, on dit a est d'ordre fini. Le plus petit entier $n > 0$ tel que $a^n = e$ est appelé l'ordre de a. Nous le noterons $o(a)$. C'est aussi l'ordre du sous-groupe $\langle a \rangle$ de G.

Corollaire 1.

Soit G un groupe fini. Pour tout $a \in G$ on a $a^{[G:1]} = e$.

Démonstration. D'après le th. de Lagrange, l'ordre $n = [\langle a \rangle : 1]$ de a divise $[G : 1]$. ∎

Corollaire 2.

Soient H et K des groupes finis et $(h, k) \in H \times K$. Alors $o(h,k) = \mathrm{ppcm}(o(h), o(k))$.

Démonstration. Pour tout $m \in \mathbb{N}$, on a $(h,k)^m = (h^m, k^m)$, d'où :

$$\begin{aligned} (h,k)^m = (e,e) &\Leftrightarrow h^m = e \quad \text{et} \quad k^m = e \\ &\Leftrightarrow o(h) \mid m \quad \text{et} \quad o(k) \mid m \quad \Leftrightarrow \quad \mathrm{ppcm}(o(h), o(k)) \mid m . \end{aligned}$$

Le plus petit $m \in \mathbb{N}^*$ tel que $(h,k)^m = (e,e)$ est donc $\mathrm{ppcm}(o(h), o(k))$. ∎

Exercice. a) Soient G un groupe et $x, y \in G$. Montrer que $o(xy) = o(yx)$.
b) Si $z \in G$ est d'ordre 2, unique, montrer que z appartient au centre Z de G.

Solution. a) Soient $a \in G$ et $\alpha \in \mathrm{Aut}\,(G)$. Pour tout $k \in \mathbb{N}$ on a $\alpha(a)^k = \alpha(a^k)$ donc $o(\alpha(a)) = o(a)$. L'assertion en résulte car $\mathrm{Ad}_x(yx) = x(yx)x^{-1} = xy$.

b) Pour tout $g \in G$, on a $o(gzg^{-1}) = o(\mathrm{Ad}_g(z)) = o(z) = 2$. D'après l'unicité de z, pour tout $g \in G$ on a $gzg^{-1} = z$ soit encore $gz = zg$. Ainsi $z \in Z$.

Exercices du chapitre 1

Ex 1 - 1

a) Caractériser les groupes G pour lesquels $\varphi : x \mapsto x^{-1}$ est un automorphisme.

b) Caractériser les groupes G pour lesquels $\psi : x \mapsto x^2$ est un endomorphisme.
En supposant G fini, à quelle condition ψ est-il un automorphisme ?

Ex 1 - 2

En étudiant sa table de multiplication, montrer qu'un groupe G d'ordre 4 ne peut avoir que deux structures.

Préciser la structure du groupe (multiplicatif) $\mathbb{U}_4 = \{1, i, -1, -i\}$, celle du groupe des isométries du plan euclidien qui conservent un rectangle $ABCD$ qui n'est pas un carré (groupe de Klein).

Ex 1 - 3

$\mathbb{R}$ est-il un groupe si on le munit de la loi de composition interne définie par
$x * y = x\sqrt{1+y^2} + y\sqrt{1+x^2}$?

Ex 1 - 4

Etudier le groupe $\mathrm{Aut}\left((\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/2\mathbb{Z})\right)$.

Ex 1 - 5

Soient K un corps commutatif et $n \geqslant 2$ un entier. Déterminer les centres Z et Z' des groupes $\mathrm{GL}(n,K)$ et $\mathrm{SL}(n,K) = \{A \in \mathcal{M}_n(K) \mid \det(A) = 1\}$.

Ex 1 - 6

Soient K un corps commutatif et $n \in \mathbb{N}^*$.

a) Soit $A \in \mathrm{GL}(n,K)$. En utilisant la méthode du pivot de Gauss, montrer qu'il existe des matrices de transvection $T_1, \ldots, T_k$ et une matrice de dilatation D telles que $A = T_1 \cdots T_k D$.

b) En déduire que $\mathrm{SL}(n,K)$ est engendré par les matrices de transvection.

c) Montrer que $\mathrm{SL}(n,\mathbb{C})$, $\mathrm{GL}(n,\mathbb{C})$ et $\mathrm{SL}(n,\mathbb{R})$ sont connexes, que $\mathrm{GL}(n,\mathbb{R})$ possède deux composantes connexes.

d) Soit $A = \begin{pmatrix} 0 & -1 & 1 \\ 0 & -1 & 0 \\ 1 & -1 & 0 \end{pmatrix}$. Montrer que $A \in \mathrm{SL}(3,\mathbb{R})$ et donner des matrices de transvection dont A soit le produit.

Ex 1 - 7

Soient G un groupe fini et H un sous-groupe distingué de G d'ordre m.

a) Soit K un sous-groupe de G tel que $[G : H]$ et $[K : 1]$ soient premiers entre eux. Montrer que $K \subset H$.

b) Si $[G : H]$ et $[H : 1]$ sont premiers entre eux, montrer que H est le seul sous-groupe de G d'ordre m.

Ex 1 - 8

Soient G un groupe et H, K deux sous-groupes de G.

a) On suppose H d'indice fini dans G. Montrer que $H \cap K$ est d'indice fini dans K et que $[K : H \cap K] \leqslant [G : H]$.

b) Montrer que l'on a l'égalité dans cette relation si et seulement si $KH = G$.

c) Si H et K sont d'indice fini, montrer que $[G : H \cap K] \leqslant [G : H][G : K]$ et que l'on a l'égalité dans cette relation si et seulement si $KH = G$.

d) Montrer que l'intersection d'une famille finie $(H_1, \ldots, H_p)$ de sous-groupes d'indice fini de G, est un sous-groupe de G d'indice fini (th. de Poincaré).

e) On suppose $[G : H]$ et $[G : K]$ finis, premiers entre eux.
Montrer que $G = KH = HK$.

Ex 1 - 9

Soient H et K des sous-groupes de $(\mathbb{Z},+)$, distincts de $\{0\}$. Montrer que $(\mathbb{Z},+)$ n'est pas produit direct de H et K.

Ex 1 - 10

Quels sont les éléments d'ordre 3 du groupe $(\mathbb{Z}/3\mathbb{Z}) \times (\mathbb{Z}/6\mathbb{Z})$?

Ex 1 - 11

On considère un groupe abélien fini G, noté additivement, et $x, y \in G$ d'ordres m et n premiers entre eux. Montrer que les deux sous-groupes $\langle x+y \rangle$ et $\langle x, y \rangle$ de G sont égaux, d'ordre mn.

Ex 1 - 12

Montrer que le produit direct $H \times K$ de deux groupes a la propriété universelle suivante

(P) Considérons un groupe G et $f \in \mathrm{Hom}(H,G)$, $g \in \mathrm{Hom}(K,G)$ tels que $\forall h \in H \, \forall k \in K \, f(h)g(k) = g(k)f(h)$. Il existe alors $\varphi \in \mathrm{Hom}(H \times K, G)$, unique, tel que $\forall h \in H \;\; f(h) = \varphi(h,e)$ et $\forall k \in K \;\; g(k) = \varphi(e,k)$.

Démontrer ainsi l'exercice précédent.

Indications

Ex 1 - 1

Chacune des conditions caractérise les groupes abéliens.

Ex 1 - 2

Voir cours 1-3, ex. On pourra distinguer le cas où tout $x \neq e$ est d'ordre 2 et le cas contraire.

Ex 1 - 3

Voir cours 1-4, ex. 1 et ex. 2.

Ex 1 - 4

Un automorphisme conserve l'ordre de chaque élément. On a $\mathrm{Aut}(G) \simeq \mathcal{S}_3$.

Ex 1 - 5

Montrer que tout $A \in Z$ commute avec les matrices E_{ij} de la base canonique de $\mathcal{M}_n(K)$. On a $Z' = \{\lambda I_n \,; \;\; \lambda \in K^*\}$ et $Z = \{\lambda I_n \,; \;\; \lambda \in K^* \,, \; \lambda^n = 1\}$.

Ex 1 - 6

Reprendre la méthode du pivot de Gauss et raisonner par récurrence sur n.

Ex 1 - 7

Considérer l'image $\varphi(K)$ par l'homomorphisme canonique $\varphi : G \to G/H$.

Ex 1 - 8

Revenir aux définitions des classes à gauche et de l'indice d'un sous-groupe.

Ex 1 - 9

Montrer que $H \cap K \neq \{0\}$.

Ex 1 - 10

Utiliser 1-14, cor. 2.

Ex 1 - 11

Utiliser la définition de l'ordre d'un élément et la relation de Bezout.

Ex 1 - 12

Pour établir (P), poser $\varphi(h,k) = f(h)g(k)$. Factoriser φ à travers son noyau.

Solutions des exercices du chapitre 1

Ex 1 - 1

a) Comme $\varphi \circ \varphi = \mathrm{Id}_G$, l'application φ est bijective et $\varphi^{-1} = \varphi$.

$$\begin{array}{rcll} \varphi \in \mathrm{End}\,(G) & \Leftrightarrow & \forall\, x \in G \quad \forall\, y \in G & \varphi(xy) = \varphi(x)\varphi(y) \\ & \Leftrightarrow & \forall\, x \in G \quad \forall\, y \in G & y^{-1}x^{-1} = x^{-1}y^{-1} \\ & \Leftrightarrow & \forall\, x \in G \quad \forall\, y \in G & yx = xy \end{array}$$

Donc φ est un automorphisme si et seulement si G est abélien.

b) $$\begin{array}{rcll} \psi \in \mathrm{End}\,(G) & \Leftrightarrow & \forall\, x \in G \quad \forall\, y \in G & \psi(xy) = \psi(x)\psi(y) \\ & \Leftrightarrow & \forall\, x \in G \quad \forall\, y \in G & xyxy = xxyy \\ & \Leftrightarrow & \forall\, x \in G \quad \forall\, y \in G & yx = xy \end{array}$$

Nous avons utilisé la régularité de la loi de composition du groupe. Ainsi, $\psi \in \mathrm{End}\,(G)$ si et seulement si G est abélien.

Si G est fini (abélien), l'endomorphisme ψ sera bijectif, si et seulement s'il est injectif. Pour cela il faut et il suffit que $\mathrm{Ker}\,(\psi) = \{x \in G \mid x^2 = e\}$ soit égal à $\{e\}$, c'est-à-dire qu'il n'existe pas d'élément d'ordre 2 dans G (l'élément neutre e est d'ordre 1).

Ex 1 - 2

Premier cas. Supposons que $x^2 = e$ pour tout $x \in G$. Dans la table de G, tous les termes diagonaux sont égaux à e. La deuxième ligne $\{ax\,;\quad x \in G\}$ se déduit de $\{e, a, b, c\}$ par la permutation $l_a : x \mapsto ax$. Elle contient donc une fois et une seule, chaque élément de G. De même pour chaque ligne et chaque colonne, d'où une seule possibilité pour compléter le tableau :

	e	a	b	c
e	e	a	b	c
a	a	e	.	.
b	b	.	e	.
c	c	.	.	e

	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

Réciproquement, le tableau obtenu est bien une loi de groupe : on retrouve par exemple la table de $(\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/2\mathbb{Z})$, qui est aussi celle du groupe de Klein des isométries conservant le rectangle $R = ABCD$ (groupe constitué de Id, des symétries s_D, $s_{D'}$, s_O par rapport aux médianes D et D' et au centre O de R).

Deuxième cas. Supposons qu'il existe $a \neq e$ tel que $a^2 \neq e$. On a $a^2 \neq a$ (sinon par régularité $a = e$). Posons $b = a^2$. On a $ab = a^3 \neq a$ (sinon par régularité $a^2 = e$), $ab \neq e$ (sinon dans la quatrième colonne c se répèterait), $ab = a^3 \neq a^2 = b$ (sinon $a = e$). Donc nécessairement, $a^3 = ab = c$. Ainsi, $G = \{e, a, a^2, a^3\}$, avec $a^4 = e$ car dans la 2 ème ligne de la table on doit trouver $a, a^2 = b, a^3 = c$ et $ac = e$. Ainsi G est un groupe *cyclique* d'ordre 4. Sa table de multiplication est évidemment la même que celle de $\mathbb{Z}/4\mathbb{Z}$ qui est additif cyclique engendré par la classe $\overline{1}$ ou de $\mathbb{U}_4 = \{1, i, -1, -i\}$ qui est multiplicatif cyclique engendré par i. Tous ces groupes sont isomorphes.

Ex 1 - 3

Posons $u = \operatorname{Argsh} x$ et $v = \operatorname{Argsh} y$. On a $x = \operatorname{sh} u$ et $y = \operatorname{sh} v$, d'où :

$$\begin{aligned} x * y &= \operatorname{sh} u \sqrt{1+\operatorname{sh}^2 v} + \operatorname{sh} v \sqrt{1+\operatorname{sh}^2 u} \\ &= \operatorname{sh} u \operatorname{ch} v + \operatorname{sh} v \operatorname{ch} u = \operatorname{sh}(u+v) = \operatorname{sh}[\operatorname{Argsh} x + \operatorname{Argsh} y]. \end{aligned}$$

Ainsi $(\mathbb{R}, *)$ est le groupe, déduit de $(\mathbb{R}, +)$ par transport de structure à l'aide de la bijection sh de $\mathbb{R}$ sur $\mathbb{R}$. Il est isomorphe à $(\mathbb{R}, +)$, d'élément neutre $\operatorname{Argsh}(0) = 0$.

Ex 1 - 4

La table de multiplication de $G = (\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/2\mathbb{Z}) = \{e, a_1, a_2, a_3\}$ est :

(1) $\forall i \quad e a_i = a_i \qquad \forall i \quad a_i^2 = e \qquad \forall i \ \forall j \neq i \quad a_i a_j = a_k \quad$ où $\quad k \neq i, k \neq j,$

où $i, j, k \in \{1, 2, 3\}$. Tout automorphisme f de G laisse fixe e. Il permute donc les autres éléments a_1, a_2, a_3. Réciproquement, pour toute permutation f de ces trois éléments, en posant $f(e) = e$, on obtient une bijection de G sur G qui respecte la table de multiplication (1). C'est donc un automorphisme. Ainsi $\operatorname{Aut}(G)$ est d'ordre $3\,! = 6$ et isomorphe au groupe $\mathcal{S}_3$ des permutations de $\{1, 2, 3\}$.

Ex 1 - 5

Notons (E_{ij}), où $i, j \in [1, \ldots, n]$, la base canonique de l'espace vectoriel $\mathcal{M}_n(K)$ des matrices carrées (tous les coefficients de E_{ij} sont nuls, sauf celui qui est sur la $i^{\text{ième}}$ ligne et la $j^{\text{ième}}$ colonne qui est égal à 1). Posons $\delta_{ij} = 0$ ou 1 selon que $i \neq j$ ou que $i = j$. Rappelons que dans l'algèbre $\mathcal{M}_n(K)$ on a :

$$E_{ij} E_{kl} = \delta_{jk} E_{il}.$$

Soit $A = (a_{ij})$ un élément du groupe $\mathrm{GL}(n, K)$, c'est-à-dire une matrice carrée inversible. Supposons que $A \in Z$ ou que $A \in Z'$. Comme A commute avec tout élément de $\mathrm{SL}(n, K)$, pour tout i et tout $j \neq i$ elle commute avec la matrice de transvection $T_{ij} = I_n + E_{ij}$ qui est triangulaires de déterminant 1. Donc A commute dans $\mathcal{M}_n(K)$ avec E_{ij} pour tous $i \neq j$. De plus, A commute avec E_{ii} pour tout i car en choisissant $j \neq i$ on a $E_{ii} = E_{ij} E_{ji}$. Puisque $A = (a_{ij}) = \sum_{ij} a_{ij} E_{ij}$, on en déduit que pour tout k et tout l les matrices

$$A E_{kl} = \sum_{ij} a_{ij} E_{ij} E_{kl} = \sum_i a_{ik} E_{il} \qquad \text{et} \qquad E_{kl} A = \sum_{ij} a_{ij} E_{kl} E_{ij} = \sum_j a_{lj} E_{kj}$$

sont égales. La famille (E_{ij}) étant une base de l'espace vectoriel $\mathcal{M}_n(K)$, on obtient $a_{ik} = 0$ si $i \neq k$, $a_{kk} = a_{ll}$ si $i = k$. Ainsi $A = \lambda I_n$, où $\lambda = a_{11}$. Réciproquement, si $A = \lambda I_n$, où $\lambda \in K^*$, alors $A \in \mathrm{GL}(n, K)$ et A commute avec tout élément de $\mathrm{GL}(n, K)$. Donc $Z = \{\lambda I_n \,;\ \lambda \in K^*\}$. Comme $\det(\lambda I_n) = \lambda^n$, on a $Z' = \{\lambda I_n \,;\ \lambda \in K^* \quad \lambda^n = 1\}$, groupe fini car dans le corps K, le polynôme $X^n - 1$ a au plus n racines.

Ex 1 - 6

Rappelons le principe de la méthode de Gauss pour résoudre, par éliminations successives des variables, un système de m équations linéaires à n inconnues, de matrice A :

$$\left\{ \begin{array}{lcl} a_{11}x_1 + \cdots + a_{1n}x_n &=& y_1 \\ \ldots\ldots\ldots\ldots\ldots &=& \ldots \\ a_{m1}x_1 + \cdots + a_{mn}x_n &=& y_m \end{array} \right. \qquad A = \begin{pmatrix} a_{11} & \cdots & a_{1n} \\ \cdot & \cdots & \cdot \\ a_{m1} & \cdots & a_{mn} \end{pmatrix} \quad I_m = \begin{pmatrix} 1 & \cdots & 0 \\ \cdot & \cdots & \cdot \\ 0 & \cdots & 1 \end{pmatrix}.$$

Les opérations utilisées sont les suivantes.

1- Transpositions $L_i \leftrightarrow L_j$ de deux équations du système. Cette opération transpose les lignes d'indices i et j dans les matrices des deux membres du système (A et I_m initialement). On obtient ce résultat en multipliant à gauche les deux matrices par une matrice $P_{ij} = (p_{kl}) \in \mathcal{M}_m(K)$ visible après opération sur le membre car $P_{ij}\, I_m = P_{ij}$. Ainsi, $p_{ij} = p_{ji} = 1$, $p_{ii} = p_{jj} = 0$, $p_{kk} = 1$ pour $k \notin \{i, j\}$ et les autres coefficients p_{kl} de P_{ij} sont nuls. On a $P_{ij}^2 = I_n$.

2- Ajouter à une ligne L_i un multiple d'une autre ligne L_j, soit $L_i \leftarrow L_i + \lambda L_j$. Cette opération est obtenue en multipliant à gauche les matrices des deux membres par une matrice $T_{ij}(\lambda) = (t_{kl})$ que l'on découvre si on fait cette opération sur I_m. On a $t_{kk} = 1$ pour $1 \leqslant k \leqslant m$, $t_{ij} = \lambda$ et les autres coefficients sont nuls. Cette matrice est triangulaire de diagonale principale faite de 1. C'est un élément de $\mathrm{SL}(n, K)$. Un endomorphisme qui a cette matrice dans une base est appelé une transvection.

3- Multiplier une ligne L_i par une constante non nulle soit $L_i \leftarrow \alpha L_i$. Pour cela, on multiplie les matrices des deux membres par la matrice diagonale $D_i(\alpha) = (d_{kl})$ obtenue en multipliant par α le coefficient $d_{ii} = 1$ de I_m, sans modifier les autres coefficients. Un endomorphisme qui a cette matrice dans une base est appelé une dilatation.

Par transposition des matrices, on voit comment réaliser des opérations analogues sur les colonnes d'une matrice par des multiplications à droite par les matrices P_{ij}, $T_{ji}(\lambda)$, $D_i(\alpha) \in \mathcal{M}_n(K)$. Rappelons que si on multiplie à gauche ou à droite une matrice, par une matrice inversible, on ne change pas son rang.

a) Montrons que si $A \in \mathrm{GL}(n, K)$, on peut, par un algorithme du pivot, la transformer en I_n sans utiliser les opérations du type 1 et en utilisant une fois seulement, pour terminer, une opération du type 3. Démontrons cela par récurrence sur n.
Pour $n = 1$, $A = (\alpha) = D$ est de la forme voulue avec zéro matrice de transvection.
Supposons $n \geqslant 2$. Admettons le résultat pour $\mathrm{GL}(n-1, K)$. Considérons $A \in \mathrm{GL}(n, K)$. La première colonne de A n'est pas nulle car A est inversible.
S'il existe $i \neq 1$ tel que $a_{i1} \neq 0$, alors $L_1 \leftarrow L_1 + \dfrac{1 - a_{11}}{a_{i1}} L_i$ remplace A par $T_1 A = B'$ telle que $b'_{11} = 1$ et T_1 est la matrice de transvection $T_{i1}(\lambda)$, où $\lambda = \frac{1-a_{11}}{a_{i1}}$.

Si pour tout $i \neq 1$, on a $a_{i1} = 0$, par $L_2 \leftarrow L_2 + L_1$ on remplace A par $B'' = T_2 A$ telle que $b''_{21} \neq 0$. Le procédé précédent, fournit $B' = T_1 T_2 A$ telle que $b'_{11} = 1$.

Ensuite, pour tout coefficient b'_{i1} non nul dans la première colonne, on effectue l'opération $L_i \leftarrow L_i - b'_{i1} L_1$. On arrive à :

$$B = \begin{pmatrix} 1 & b_{12} & \cdots & b_{1n} \\ 0 & b_{22} & \cdots & b_{2n} \\ \vdots & \vdots & & \vdots \\ 0 & b_{n2} & \cdots & b_{nn} \end{pmatrix}, \quad \text{avec } A' = \begin{pmatrix} b_{22} & \cdots & b_{2n} \\ \vdots & & \vdots \\ b_{n2} & \cdots & b_{nn} \end{pmatrix} \in \mathrm{GL}(n-1, K).$$

En effet, on a $n = \mathrm{rang}(A) = \mathrm{rang}(B)$ donc $\det(A') = \det(B) \neq 0$. Les lignes de A' constituent donc une base de K^{n-1}. Le vecteur $b = (b_{12}, \ldots, b_{1n})$ a donc une expression unique de la forme

$$b = \lambda_2 (b_{22}, \ldots, b_{2n}) + \cdots + \lambda_n (b_{n2}, \ldots, b_{nn}).$$

Les opérations $L_1 \leftarrow L_1 - \lambda_2 L_2$, ... , $L_1 \leftarrow L_1 - \lambda_n L_n$, c'est-à-dire les multiplications de B à gauche par $n-1$ matrices de transvection conduiront à :

$$C = \begin{pmatrix} 1 & 0 & \cdots & 0 \\ 0 & b_{22} & \cdots & b_{2n} \\ \vdots & \vdots & & \vdots \\ 0 & b_{n2} & \cdots & b_{nn} \end{pmatrix} , \quad \text{avec} \quad A' = \begin{pmatrix} b_{22} & \cdots & b_{2n} \\ \vdots & & \vdots \\ b_{n2} & \cdots & b_{nn} \end{pmatrix} \in \mathrm{GL}(n-1, K) .$$

Il existe donc des matrices de transvections $T_1, \ldots, T_r$ telles que $C = T_r \cdots T_1 A$. D'après l'hypothèse de récurrence, il existe une matrice de dilatation D', des matrices de transvection $T'_{r+1}, \ldots, T'_s$ telles que $A' = T'_{r+1} \cdots T'_s D'$. Dans $\mathrm{GL}(n-1, K)$ considérons les matrices d'expressions par blocs

$$T_{r+1} = \begin{pmatrix} 1 & 0 \\ 0 & T'_{r+1} \end{pmatrix} \quad , \ \ldots \ , \quad T_s = \begin{pmatrix} 1 & 0 \\ 0 & T'_s \end{pmatrix} \quad , \quad D = \begin{pmatrix} 1 & 0 \\ 0 & D' \end{pmatrix} .$$

On a $C = T_{r+1} \cdots T_s D$, d'où $A = T_1^{-1} \cdots T_r^{-1} T_{r+1} \cdots T_s D$. Le résultat s'en déduit car l'inverse de $T_{ij}(\lambda)$ est $T_{ij}(-\lambda)$.

b) $A \in \mathrm{SL}(n, K) \quad \Leftrightarrow \quad \det(A) = 1 \quad \Leftrightarrow \quad \det(D) = 1 \quad \Leftrightarrow \quad D = I_n$.

Ainsi tout élément de $\mathrm{SL}(n, K)$ est produit de matrices de transvections.

c) L'homomorphisme $\lambda \mapsto T_{ij}(\lambda)$ du groupe additif $(\mathbb{R}, +)$ dans $\mathrm{GL}(n, \mathbb{R})$ est continu de $\mathbb{R}$ dans l'espace vectoriel $\mathcal{M}_n(\mathbb{R}) \simeq \mathbb{R}^{n^2}$ car $t_{ij} = \lambda$ et les autres coefficients sont constants. Donc $t \mapsto T_{ij}(t\lambda)$, où $t \in [0, 1]$, est un chemin continu reliant I_n et $T_{ij}(\lambda)$ dans $\mathrm{SL}(n, \mathbb{R})$. De même dans le cas de $\mathrm{SL}(n, \mathbb{C})$.

Soit $A \in \mathrm{SL}(n, \mathbb{R})$ (resp. $\mathrm{SL}(n, \mathbb{C})$). D'après a), A est produit $A = T_{ij}(\lambda) \cdots T_{kl}(\mu)$ de matrices de transvection. Alors $t \mapsto T_{ij}(t\lambda) \cdots T_{kl}(t\mu)$ est un chemin continu de $[0, 1]$ dans $\mathrm{SL}(n, \mathbb{R})$ (resp. $\mathrm{SL}(n, \mathbb{C})$) reliant I_n et A . Le groupe $\mathrm{SL}(n, \mathbb{R})$ (resp. $\mathrm{SL}(n, \mathbb{C})$) est donc connexe par arc.

Soit $A \in \mathrm{GL}(n, \mathbb{C})$. D'après a), on a $A = T_{ij}(\lambda) \cdots T_{kl}(\mu) D(\alpha)$ où $D(\alpha)$ est une matrice de dilatation. Comme $\alpha = re^{i\theta} \neq 0$, en posant $\zeta = \ln r + i\theta$ on a $\alpha = e^{\zeta}$. Alors $t \mapsto D(e^{t\zeta})$ est un homomorphisme de groupes continu de $\mathbb{R}$ dans $\mathrm{GL}(n, \mathbb{C})$ reliant I_n et D_α quand t varie de 0 à 1 . On voit que $\mathrm{GL}(n, \mathbb{C})$ est connexe par arc.

Le groupe $\mathrm{GL}(n, \mathbb{R})$ n'est pas connexe car la fonction continue $\varphi : A \mapsto \det(A)$ applique $\mathrm{GL}(n, \mathbb{R})$ sur $\mathbb{R}^*$ non connexe. L'image réciproque $\mathrm{GL}(n, \mathbb{R})^+$ du sous-groupe $\mathbb{R}_+^*$ de $\mathbb{R}^*$ par l'homomorphisme φ est un sous-groupe distingué de $\mathrm{GL}(n, \mathbb{R})$. Ce sous-groupe est connexe par arc. En effet, dans l'expression de $A \in \mathrm{GL}(n, \mathbb{R})$ donnée en a), la dilatation $D(\alpha)$ a un rapport $\alpha = \det(A) > 0$ et s'écrit $\alpha = e^{\alpha}$. Le chemin continu $t \mapsto D(e^{t\alpha})$ relie I_n et D_α .

Posons $\mathrm{GL}(n, \mathbb{R})^- = \{A \in \mathrm{GL}(n, \mathbb{R}) \mid \det(A) < 0\}$. Choisissons $A_0 \in \mathrm{GL}(n, \mathbb{R})^-$. Pour tout $A \in \mathrm{GL}(n, \mathbb{R})^-$ on a $A_0^{-1} A \in \mathrm{GL}(n, \mathbb{R})^+$.
On voit que $\mathrm{GL}(n, \mathbb{R})^- = A_0 \, \mathrm{GL}(n, \mathbb{R})^+$. Cette classe à gauche modulo le sous-groupe $\mathrm{GL}(n, \mathbb{R})^+$ est image de $\mathrm{GL}(n, \mathbb{R})^+$ par $A \mapsto A_0 A$ continue. Donc $\mathrm{GL}(n, \mathbb{R})^-$ est connexe. On a deux composantes connexes dans $\mathrm{GL}(n, \mathbb{R})$ qui sont les deux classes modulo $\mathrm{GL}(n, \mathbb{R})^+$.

d) Dans cet exemple, la démarche exposée, conduit aux manipulations suivantes :

$L_1 \leftarrow L_1 + L_3$, $L_3 \leftarrow L_3 - L_1$, $L_2 \leftarrow L_2 + 2L_3$, $L_3 \leftarrow L_3 - L_2$,
$L_2 \leftarrow L_2 + 2L_3$, $L_1 \leftarrow L_1 - L_3$, $L_1 \leftarrow L_1 + 2L_2$.

On aboutit à I_3 donc $A \in \mathrm{SL}(3,\mathbb{R})$ (visible à priori si on calcule $\det(A)$) et

$$A = T_{13}(-1)\,T_{31}(1)\,T_{23}(-2)\,T_{32}(1)\,T_{23}(-2)\,T_{13}(1)\,T_{12}(-2)\,.$$

Ex 1 - 7

a) Soit $\varphi : G \to G/H$ l'homomorphisme canonique. D'après 1-9, cor. 1, $[\varphi(K) : 1]$ divise $[K : 1]$ et $[G/H : 1]$. On a donc $\varphi(K) = \{e\}$, soit $K \subset H$.

b) Si un sous-groupe K est d'ordre $m = [H : 1]$ et si $[H : 1] \wedge [G : H] = 1$, alors d'après a), on a $K \subset H$ et donc $K = H$ puisque K et H ont le même cardinal.

Ex 1 - 8

a) Posons $n = [G : H]$. On a n classes à gauche $g_1H, \ldots, g_nH$ qui constituent une partition de G . On en déduit la partition de K :

$$K = [(g_1H) \cap K] \cup \cdots \cup [(g_nH) \cap K] \qquad (1)$$

Si $(g_1H) \cap K \neq \emptyset$, il existe $k \in K$ tel que $k \in g_1H$, c'est-à-dire tel que $kH = g_1H$. La translation à gauche par k étant injective, on a $(g_1H) \cap K = (kH) \cap (kK) = k(H \cap K)$. Les parties non vides dans la partition (1) de K sont donc les classes de K modulo $(H \cap K)$. On a donc au plus n classes modulo $H \cap K$ dans K .

b) L'égalité $n = [K : H \cap K]$ a lieu si dans (1) toutes les parties $g_iH \cap K$ sont non vides. Pour tout $g \in G$, on a $(gH) \cap K \neq \emptyset$. Il existe donc $h \in H$ et $k \in K$ tels que $k = gh$, d'où $g = kh^{-1} \in KH$. Ainsi $G = KH$.

Réciproquement, supposons que $G = KH$. Pour $i = 1, \ldots, n$ il existe $k_i \in K$, $h_i \in H$ tels que $g_i = k_ih_i$, d'où $(g_iH) \cap K \neq \emptyset$. On en déduit que $[K : H \cap K] = n$.

c) D'après le th. de Lagrange, $[G : H \cap K] = [G : K][K : H \cap K]$. Si K et H sont d'indice fini, en utilisant a), on obtient $[G : H \cap K] \leqslant [G : K][G : H]$ fini, avec égalité si et seulement si $[K : H \cap K] = [G : H]$, soit si $G = KH$.

d) Pour $p \geqslant 2$, par récurrence c) donne $[G : \bigcap_{i=1}^{p} H_i] \leqslant \prod_{i=1}^{p} [G : H_i]$.

e) D'après le th. de Lagrange, $[G : H \cap K] = [G : K][K : H \cap K] = [G : H][H : H \cap K]$ est divisible par $[G : K]$ et par $[G : H]$ et donc par leur ppcm. Ces nombres étant premiers entre eux, ce ppcm est $[G : K]\,[G : H]$. Donc $[G : K][G : H]$ divise $[G : H \cap K]$. Compte tenu de c), ces nombres sont égaux et $G = KH$. En prenant les images par la bijection $x \mapsto x^{-1}$, on obtient $G = HK$.

Ex 1 - 9

Il existe $m \in \mathbb{N}^*$ et $n \in \mathbb{N}^*$ tels que $H = m\mathbb{Z}$ et $K = n\mathbb{Z}$. On a alors $\mathrm{ppcm}(m, n) \in H \cap K$ et donc $H \cap K \neq \{0\}$. Par contre, on peut avoir $H + K = \mathbb{Z}$. Cela se produit si et seulement s'il existe $u \in \mathbb{Z}$ et $v \in \mathbb{Z}$ tels que $um + vn = 1$, c'est-à-dire si m et n sont premiers entre eux (th. de Bezout).

Ex 1 - 10

On cherche $(\overline{x},\overline{y}) \in (\mathbb{Z}/3\mathbb{Z}) \times (\mathbb{Z}/6\mathbb{Z})$, tel que $3 = o(\overline{x},\overline{y}) = \text{ppcm}(o(\overline{x}), o(\overline{y}))$ (voir 1-14, cor. 2), c'est-à-dire tel que :

$$o(\overline{x}) = 1 \text{ et } o(\overline{y}) = 3 \quad \text{ou} \quad o(\overline{x}) = 3 \text{ et } o(\overline{y}) = 1 \quad \text{ou} \quad o(\overline{x}) = 3 \text{ et } o(\overline{y}) = 3$$

avec

$$\begin{array}{lll} o(\overline{x}) = 3 & \Leftrightarrow & \overline{x} = \overline{1} \text{ ou } \overline{2} \quad ; \quad o(\overline{y}) = 3 \Leftrightarrow \overline{y} = \overline{2} \text{ ou } \overline{4} \\ o(\overline{x}) = 1 & \Leftrightarrow & \overline{x} = \overline{0} \qquad\quad ; \quad o(\overline{y}) = 1 \Leftrightarrow \overline{y} = \overline{0}. \end{array}$$

D'où les éléments d'ordre 3 de $(\mathbb{Z}/3\mathbb{Z}) \times (\mathbb{Z}/6\mathbb{Z})$:

$$(\overline{0},\overline{2}) \ , \ (\overline{0},\overline{4}) \ , \ (\overline{1},\overline{0}) \ , \ (\overline{2},\overline{0}) \ , \ (\overline{1},\overline{2}) \ , \ (\overline{1},\overline{4}) \ , \ (\overline{2},\overline{2}) \ , \ (\overline{2},\overline{4}).$$

Ex 1 - 11

L'ordre m de x est le plus petit $m \in \mathbb{N}^*$ tel que $mx = 0$. Soit $k \in \mathbb{Z}$. On a $kx = 0$ si et seulement si k est un multiple de m. On a de même $ny = 0$. Ainsi, $mn(x+y) = 0$. Cela prouve que l'ordre de $x+y$ divise mn.

D'après le th. de Bezout, si m et n sont premiers entre eux, il existe $u, v \in \mathbb{Z}$ tels que $um + vn = 1$. On en déduit que :

$$x = umx + vnx = vnx = vn(x+y) \in \langle x+y \rangle ,$$

$$y = umy + vny = umy = um(x+y) \in \langle x+y \rangle .$$

On a donc $\langle x \rangle \subset \langle x,y \rangle \subset \langle x+y \rangle$ et d'après le th. de Lagrange,

$$m = [\langle x \rangle : 1] \mid [\langle x,y \rangle : 1] \mid [\langle x+y \rangle : 1] \mid mn .$$

On obtient un résultat analogue pour $n = o(y)$. Comme les multiples communs de m et de n sont les multiples de $\text{ppcm}(m,n) = mn$ (ici $m \wedge n = 1$), on déduit de tout cela que $mn = [\langle x,y \rangle : 1] = [\langle x+y \rangle : 1]$ et ensuite que $\langle x,y \rangle = \langle x+y \rangle$.

Ex 1 - 12

Pour tout $(h,k) \in H \times K$, posons $\varphi(h,k) = f(h)g(k)$. L'application φ ainsi définie est un homomorphisme, d'où (P). En effet, pour tous $(h,k), (h',k') \in H \times K$ on a :

$$\begin{array}{rcl} \varphi[(h,k)(h',k')] & = & \varphi(hh',kk') = f(hh')g(kk') = f(h)f(h')g(k)g(k') \\ & = & [f(h)g(k)][f(h')g(k')] = \varphi(h,k)\varphi(h',k') . \end{array}$$

Si $H = \langle x \rangle$ et $K = \langle y \rangle$, où $x, y \in G$ commutent, appliquons (P) à $f : h \mapsto h$ de H dans G et $g : k \mapsto k$ de K dans G. Alors, $\text{Ker}(\varphi)$ est isomorphe à $H \cap K$ car :

$$\begin{array}{rcl} (h,k) \in \text{Ker}(\varphi) & \Leftrightarrow & hk = e \quad \Leftrightarrow \quad h = k^{-1} \\ & \Leftrightarrow & (h,k) \in (H \cap K) \times (H \cap K) \quad \text{et} \quad k = h^{-1} . \end{array}$$

Si on suppose que $m = o(x) = [H : 1]$ et $n = o(y) = [K : 1]$ sont premiers entre eux, alors $[H \cap K : 1]$, qui divise ces deux nombres (d'après le th. de Lagrange), vaut 1 et $H \cap K = \{e\}$. Ainsi, φ est injectif. C'est un isomorphisme de $\langle x \rangle \times \langle y \rangle$ sur $\langle x,y \rangle = \{x^\alpha y^\beta \mid \alpha \in \mathbb{Z}, \beta \in \mathbb{Z}\}$. L'ordre de $\langle x,y \rangle$ est donc mn.
De plus, $o(xy) = o(\varphi(x,y)) = o((x,y)) = \text{ppcm}(o(x), o(y)) = mn$. On en déduit que $\langle xy \rangle = \langle x,y \rangle$.

Chapitre 2

Actions de groupes

2.1 Groupe agissant sur un ensemble

La plupart des théories mathématiques étudient des objets constitués d'un ensemble E muni d'une structure : espace métrique, espace topologique, groupe, espace vectoriel,... En général, l'ensemble G des applications bijectives de E sur lui-même, respectant cette structure, est alors stable par composition et l'application réciproque f^{-1} de tout $f \in G$ est élément de G. La composition des applications étant associative, G est un groupe d'élément neutre Id_E. Plus exactement, G est un sous-groupe du groupe $\mathcal{S}_E$ des bijections de E sur E. Par exemple, les situations suivantes entrent dans ce schéma.

a) E est un espace métrique et G est l'ensemble des bijections de E sur E qui conservent la distance (G est le groupe des isométries de E sur E),

b) E est un espace topologique et G est l'ensemble des bijections de E sur E qui sont continues ainsi que leur réciproque (groupe des homéomorphismes de E sur E),

c) E est un groupe et G est l'ensemble des bijections f de E sur E qui préservent la structure de groupe, c'est-à-dire telles que $f(xy) = f(x)f(y)$ pour tous $x, y \in E$ (groupe $\mathrm{Aut}(E)$ des automorphismes du groupe E),

d) E est un espace vectoriel et G est l'ensemble des applications linéaires bijectives de E sur E (groupe $\mathrm{GL}(E)$ des automorphismes de l'espace vectoriel E),

e) E est un espace vectoriel euclidien et G est l'ensemble des applications linéaires isométriques de E sur E (groupe orthogonal $\mathrm{O}(E)$ de E),

f) E est un espace vectoriel hermitien et G est l'ensemble des applications linéaires isométriques de E sur E (groupe unitaire $\mathrm{U}(E)$ de E).

etc...

Les exemples d), e), f) ci-dessus, sont particulièrement importants. En effet, on dispose sur E de tous les outils de l'algèbre linéaire pour étudier les éléments du groupe G : représentation matricielle de ses éléments, diagonalisation ou réduction des endomorphismes, etc... Depuis un siècle, pour étudier un groupe donné, les mathématiciens ont pris l'habitude de le plonger dans l'un des trois derniers exemples cités. Cela s'appelle faire une *représentation* du groupe G. Ainsi, un groupe G opérant sur un ensemble E est le cadre naturel de nombreux groupes classiques. C'est aussi un outil fondamental des mathématiques contemporaines. Précisons ce que l'on entend par là.

Définition.

On appelle action à gauche du groupe G sur un ensemble X, un homomorphisme t de G dans le groupe $\mathcal{S}_X$ des bijections de X sur X, c'est-à-dire une application t de G dans $\mathcal{S}_X$ telle que $t(gg') = t(g) \circ t(g')$ pour tout $g \in G$ et pour tout $g' \in G$.

Si l'homomorphisme t est injectif, on dit que cette action est *fidèle*.

Si E est non seulement un ensemble mais un objet d'une catégorie plus particulière, par exemple un espace métrique (resp. un groupe, un espace vectoriel,...) et si $t(g)$ est pour tout $g \in G$ un isomorphisme de cette catégorie, on dira que t est une action de G sur E par isométries (resp. par automorphismes de groupes, par automorphismes d'espaces vectoriels, ...)

Pour simplifier l'écriture, on note $g{\cdot}x$ l'image $t(g)(x)$ de $x \in X$ par $t(g) \in \mathcal{S}_X$.

Puisque t est un homomorphisme, on a $t(e) = \mathrm{Id}_E$ et $t(g) \circ t(g') = t(gg')$ pour tous $g, g' \in G$. L'application $(g, x) \mapsto g{\cdot}x$ de $G \times X$ dans X vérifie donc :

(α) $\forall\, x \in X \quad e{\cdot}x = x$ (action de l'élément neutre),

(β) $\forall\, g \in G \quad \forall\, g' \in G \quad \forall\, x \in X \quad g{\cdot}(g'{\cdot}x) = (gg'){\cdot}x$ (associativité de l'action).

Réciproquement, si on considère une application $(g, x) \mapsto g{\cdot}x$ de $G \times X$ dans X ayant les propriétés (α) et (β) précédentes, alors à tout $g \in G$ est associé une application $t(g) : x \mapsto g{\cdot}x$ de X dans X. D'après (α) on a $t(e) = \mathrm{Id}_E$. En appliquant (β), avec $g' = g^{-1}$ on obtient $t(g) \circ t(g^{-1}) = t(gg^{-1}) = t(e) = \mathrm{Id}_E$ et de même, $t(g^{-1}) \circ t(g) = \mathrm{Id}_E$. Donc $t(g) \in \mathcal{S}_X$. Ensuite, (β) montre que $t(gg') = t(g) \circ t(g')$ pour tout $g \in G$ et pour tout $g' \in G$. On retrouve la situation considérée dans la définition. Les deux points de vue sont équivalents pour définir une action à gauche de G sur X.

Définition.

On appelle action à droite de G sur un ensemble X, un antihomomorphisme t de G dans le groupe $\mathcal{S}_X$ des bijections de X sur X, c'est-à-dire une application t de G dans $\mathcal{S}_X$ telle que $t(gg') = t(g') \circ t(g)$ pour tout $g \in G$, et pour tout $g' \in G$.

En posant $x{\cdot}g = t(g)(x)$, l'application $(x, g) \mapsto x{\cdot}g$ de $X \times G$ dans X vérifie :

(α') $\forall\, x \in X \quad x{\cdot}e = x$ (action de l'élément neutre),

(β') $\forall\, g \in G \quad \forall\, g' \in G \quad \forall\, x \in X \quad (x{\cdot}g){\cdot}g' = x{\cdot}(gg')$ (associativité de l'action).

Réciproquement, considérons une application $(x, g) \mapsto x{\cdot}g$ de $X \times G$ dans X ayant les propriétés (α') et (β'). Alors, pour tout $g \in G$ l'application $t(g) : x \mapsto x{\cdot}g$ de X dans X est bijective de réciproque $t(g^{-1})$ et $t : g \mapsto t(g)$ de G dans $\mathcal{S}_X$ est telle que $t(gg') = t(g') \circ t(g)$ pour tout $g \in G$ et pour tout $g' \in G$. On retrouve les données de la définition précédente. Les deux points de vue sont équivalents.

Si le groupe G est commutatif, toute action à gauche de G sur X est aussi une action à droite et vice-versa.

Dans la suite de ce paragraphe 2, nous considèrerons uniquement le cas des actions à gauche. Il est facile d'adapter aux actions à droite les propriétés démontrées. D'ailleurs, si $t : g \mapsto t(g)$ est une action à gauche de G sur E, alors $t' : g \mapsto t(g^{-1})$ est une action à droite de G sur E. Si t est une action à droite, alors t' est une action à gauche.

Exemples.

a) Soit E un ensemble. Le groupe $\mathcal{S}_E$ des bijections de E sur E agit à gauche sur E, de manière naturelle, en posant $g{\cdot}x = g(x)$ pour $g \in \mathcal{S}_E$ et $x \in E$. L'homomorphisme t du groupe $\mathcal{S}_E$ dans $\mathcal{S}_E$ définissant cette action est ici l'application identique.

b) Soit $t : G \to \mathcal{S}_E$ une action du groupe G sur un ensemble E. La restriction t' de t à un sous-groupe H de G est un élément de Hom $(H, \mathcal{S}_E)$. C'est une action de H sur E.

En particulier, tout sous-groupe H de $\mathcal{S}_E$ agit naturellement à gauche sur E.

Exercice. Considérons une action du groupe G sur l'ensemble E.

a) Montrer qu'on définit une action à gauche de G sur $\mathcal{P}(E)$ en posant :

$$\forall\, g \in G \quad \forall\, X \in \mathcal{P}(E) \qquad g{\cdot}X \,=\, t_g(X) \,=\, \{g{\cdot}x\,;\;\; x \in X\}\,.$$

b) Si F est un autre ensemble, montrer qu'on définit une action à droite de G sur l'ensemble $\mathcal{F}(E,F)$ des applications de E dans F en posant :

$$\forall\, g \in G \quad \forall\, \varphi \in \mathcal{F}(E,F) \qquad (\varphi{\cdot}g)(x) = \varphi(g{\cdot}x)\,.$$

Solution. a) $\forall\, X \in \mathcal{F}(E,F) \qquad e{\cdot}X \,=\, \{e{\cdot}x\,;\;\; x \in X\} \,=\, \{x\,;\;\; x \in X\} \,=\, X\,.$

$\forall g \;\; \forall g' \;\; \forall X \qquad g{\cdot}(g'{\cdot}X) = \{g{\cdot}(g'{\cdot}x)\,;\;\; x \in X\} = \{gg'{\cdot}x\,;\;\; x \in X\} = gg'{\cdot}X\,.$

b) $\forall\, \varphi \in \mathcal{F}(E,F) \qquad \varphi{\cdot}e = \varphi \quad$ car $\quad \forall\, x \in E \qquad (\varphi{\cdot}e)(x) \,=\, \varphi(e{\cdot}x) \,=\varphi(x)\,.$

$\forall g \;\; \forall g' \;\; \forall \varphi \;\; \forall x \quad [(\varphi{\cdot}g){\cdot}g'](x) = (\varphi{\cdot}g)(g'{\cdot}x) = \varphi(g{\cdot}(g'{\cdot}x)) = \varphi(gg'{\cdot}x) = (\varphi{\cdot}gg')(x).$
Les conditions (α) et (β) sont donc vérifiées.

2.2 Orbite, stabilisateur d'un point

Proposition.

Considérons une action à gauche du groupe G sur un ensemble E.
(i) *Posons* $xRy \;\Leftrightarrow\; (\,\exists g \in G\,;\;\; g{\cdot}x = y\,)$. *C'est une relation d'équivalence sur E.*
(ii) *Soit* $x \in E$. *Alors* $G_x \,=\, \{g \in G \mid g{\cdot}x = x\}$ *est un sous-groupe de G.*
(iii) *Considérons* $x \in E$, $g_0 \in G$, *puis* $y = g_0{\cdot}x$. *Alors on a*

$$G_y = g_0 G_x g_0^{-1} \qquad \textit{et} \qquad \{\, g \in G \mid g{\cdot}x = y \,\} = g_0 G_x\,.$$

Démonstration. (i) Pour tout $x \in E$ on a xRx car $e{\cdot}x = x$. La relation binaire R est donc réflexive. Elle est symétrique en effet : Si xRy alors $\exists g \in G \quad g{\cdot}x = y$ d'où en utilisant (β) et (α) on obtient $x = g^{-1}{\cdot}y$ c'est-à-dire yRx.

D'après (β), elle est transitive : $\quad (g{\cdot}x = y \quad \text{et} \quad g'{\cdot}y = z\,) \quad \Rightarrow \quad (g'g{\cdot}x = z)\,.$

(ii) Vérifions que G_x est un sous-groupe de G. On a $e \in G_x$ car $e{\cdot}x = x$.
$\forall g \in G_x \quad g{\cdot}x = x$ d'où $g^{-1}{\cdot}(g{\cdot}x) = g^{-1}{\cdot}x$ c'est-à-dire $x = g^{-1}{\cdot}x$ soit $g^{-1} \in G_x$.
$\forall g \in G_x \quad \forall g' \in G_x \quad (g'g){\cdot}x = g'{\cdot}(g{\cdot}x) = g'{\cdot}x = x$ donc $g'g \in G_x$.

(iii) $\forall g \in G \qquad$
$$\begin{aligned} g \in G_y \;&\Leftrightarrow\; g{\cdot}(g_0{\cdot}x) = g_0{\cdot}x \\ &\Leftrightarrow\; (g_0^{-1}gg_0){\cdot}x = x \\ &\Leftrightarrow\; g_0^{-1}gg_0 \in G_x \\ &\Leftrightarrow\; g \in g_0 G_x g_0^{-1}\,. \end{aligned}$$

$g{\cdot}x = y \;\Leftrightarrow\; g{\cdot}x = g_0{\cdot}x \;\Leftrightarrow\; g_0^{-1}g{\cdot}x = x \;\Leftrightarrow\; g_0^{-1}g \in G_x \;\Leftrightarrow\; g \in g_0 G_x\,.$ ∎

Définitions.

La relation d'équivalence R définie dans (i), *s'appelle la relation de conjugaison : les éléments x et y de E sont conjugués, s'il existe $g \in G$ tel que $g{\cdot}x = y$.*

On appelle orbite de x sous l'action de G, la classe d'équivalence $\{g\cdot x\,;\ g\in G\}$ de $x\in E$. Les orbites O_x des divers éléments x de E, constituent une partition de E.

Le sous-groupe G_x de G, formé des éléments de G qui laissent fixe $x\in E$, s'appelle le stabilisateur de x.

L'action de G sur E est dite transitive s'il existe une seule orbite (égale à E). Cela signifie que pour tout couple (x,y) d'éléments de E il existe $g\in G$ tel que $g\cdot x=y$.

On dit que l'action est libre si pour tout couple (x,y) d'éléments de E il existe au plus un élément g de G tel que $g\cdot x=y$ (il en existe exactement un si x et y ont la même orbite et aucun sinon).

Exemples.

Pour qu'une partie X de l'ensemble E soit stable pour l'action t du groupe G sur E, (telle que $g\cdot x\in X$ pour tout $x\in X$ et pour tout $g\in G$), il faut et il suffit que X soit une réunion d'orbites.

Dans ce cas $t'\ :\ g\ \mapsto\ t_g|_X$ est une action de G sur X. Si t est libre, cette action t' est libre. Cette action est transitive, si et seulement si X est une orbite.

b) Un groupe G agit à gauche sur lui-même par translations à gauche. En effet, d'après 1-3, $l_g\ :\ g'\ \mapsto\ gg'$ est pour tout $g\in G$ une bijection de G sur G et $t\ :\ g\ \mapsto\ l_g$ est un homomorphisme de groupes de G dans $\mathcal{S}_G$. Cette action est libre et transitive.

Soit H un sous-groupe de G. La restriction de l'homomorphisme t à H, est une action de H sur G. Elle est libre mais elle n'est pas transitive. L'orbite de $x\in G$ sous cette action est la classe à droite Hx de x. On retrouve ainsi que les classes à droite modulo H forment une partition de G.

De même, G agit à droite sur lui-même par translations à droite. En restreignant à H cette action, on retrouve la partition de G en classes à gauche modulo H.

Exercice. Soit E un espace vectoriel de dimension finie n. Montrer que le groupe $\mathrm{GL}(E)$ agit naturellement sur l'ensemble X des sous-espaces vectoriels de E. Déterminer l'orbite, le stabilisateur, de $F\in X$. Combien existe-t-il d'orbites ?

Solution. $\mathrm{GL}(E)$ est un sous-groupe du groupe $\mathcal{S}_E$ des bijections de E. Il agit à gauche sur E (2-1, ex. b) et donc sur $\mathcal{P}(E)$ (2-1, exerc). Soient $g\in\mathrm{GL}(E)$ et $F\in X$. Alors $g(F)$ est un sous-espace vectoriel de E. Donc X est une partie stable de $\mathcal{P}(E)$ et $(g,F)\ \mapsto\ g(F)$ est une action de $\mathrm{GL}(E)$ sur X (rem. a) ci-dessus).

Soit $F\in X$ de dimension k. Pour tout $g\in\mathrm{GL}(E)$ on a $\dim(g(F))=k$.
Réciproquement, soit $F'\in X$ tel que $\dim(F')=k$. Choisissons des bases $(e_1,\dots,e_k)$ de F et $(e'_1,\dots,e'_k)$ de F'. On peut compléter ces familles libres de E et obtenir des bases $(e_1,\dots,e_k,e_{k+1},\dots,e_n)$ et $(e'_1,\dots,e'_k,e'_{k+1},\dots,e'_n)$ de E. Il existe $g\in\mathcal{L}(E)$ unique tel que $g(e_i)=e'_i$ pour $i=1,\dots,n$. On a $g\in\mathrm{GL}(E)$ car le rang de g est n et $g(F)=F'$. Ainsi, F' appartient à l'orbite de F. L'orbite de F est donc l'ensemble des sous-espaces vectoriels de E de même dimension que F. Il existe donc $n+1$ orbites pour cette action.

Le stabilisateur de F est l'ensemble des $g\in\mathrm{GL}(E)$ qui laissent F invariant. C'est l'ensemble des $g\in\mathcal{L}(E)$ qui ont, dans la base $(e_1,\dots,e_k,e_{k+1},\dots,e_n)$ précédente, une matrice de la forme $M=\begin{pmatrix}A & B\\ 0 & C\end{pmatrix}$, avec $A\in\mathcal{M}_k$, $B\in\mathcal{M}_{k,n-k}$, $C\in\mathcal{M}_{n-k}$ et avec A et C inversibles car $\det(A)\det(C)=\det(M)\neq 0$.

2.3 Action d'un groupe fini sur un ensemble fini

Proposition.

Considérons un groupe fini G, une action de G sur un ensemble fini E, les orbites $O_1, \ldots, O_k$ pour cette action. Pour $i = 1, \ldots, k$ soit $x_i \in O_i$. Pour tout $g \in G$ notons $fix(g) = \{x \in E \mid g \cdot x = x\}$ l'ensemble des éléments de E fixes par g.

(i) $card(E) = \sum_{i=1}^{k} card(O_i)$ et $card(O_i) = \frac{[G:1]}{[G_{x_i}:1]}$ (équation des classes).

(ii) *Le nombre d'orbites est* $k = \frac{1}{[G:1]} \sum_{g \in G} card(fix(g))$ (formule de Burnside).

Démonstration. (i) Les orbites forment une partition de E, d'où la première relation. Soit $y = g_0 \cdot x_i$ un élément de l'orbite O_i. D'après la prop. 2-2 (iii), l'ensemble des $g \in G$ tels que $g \cdot x_i = y$ est la classe à gauche $g_0 G_{x_i}$. Elle a le même cardinal que G_{x_i}. Regroupons tous les éléments de G qui appliquent x_i sur un même élément y de O_i. On partage ainsi G en $\text{card}(O_i)$ parties disjointes qui ont toutes pour cardinal $[G_{x_i} : 1]$. On a donc $[G : 1] = [G_{x_i} : 1] \times \text{card}(O_i)$, d'où la deuxième relation.

(ii) Il suffit de calculer le cardinal de $F = \{(g, x) \in G \times E \mid g \cdot x = x\}$ de deux façons :

$$\text{card}(F) = \sum_{g \in G} \sum_{x \in E} \text{card}(\{(g,x) \mid g \cdot x = x\}) = \sum_{g \in G} \text{card}(\text{fix}(g)),$$

$$\text{card}(F) = \sum_{x \in E} [G_x : 1] = \sum_{x \in E} \frac{[G:1]}{\text{card}(O_x)} = \sum_{i=1}^{k} \sum_{x \in O_i} \frac{[G:1]}{\text{card}(O_x)}$$

$$= [G : 1] \sum_{i=1}^{k} \sum_{x \in O_i} \frac{1}{\text{card}(O_{x_i})} = [G : 1] \sum_{i=1}^{k} 1 = [G : 1] \times k. \qquad \blacksquare$$

Corollaire.

Soit G un groupe d'ordre $[G : 1] = p^m$, avec p premier, agissant sur un ensemble fini E. Le nombre s de points de E fixes pour l'action est congru à $card(E)$ modulo p.

Démonstration. Si $m = 0$, le résultat est évident. Supposons $m \neq 0$. D'après (i), le cardinal $\text{card}(O_i) = \frac{[G:1]}{[G_{x_i}:1]}$ de toute orbite O_i est un diviseur de $[G : 1] = p^m$. Il est de la forme p^{m_i}. Si $O_1, \ldots, O_r$ sont les orbites non ponctuelles et si $\{x_1\}, \ldots, \{x_s\}$ sont les orbites ponctuelles, l'équation des classes $\text{card}(E) = \sum_{i=1}^{k} \text{card}(O_i)$ donne :

$$\text{card}(E) = \sum_{i=1}^{r} p^{m_i} + 1 + \cdots + 1 = \sum_{i=1}^{r} p^{m_i} + s. \qquad \blacksquare$$

Exemple. Soit $p \in \mathbb{N}$ premier. Faisons agir $\mathbb{Z}/p\mathbb{Z}$ par translations sur $X = \mathbb{Z}/p\mathbb{Z}$, puis sur $\mathcal{P}(X)$. Si $A \in \mathcal{P}(X)$ est de cardinal k, avec $1 \leqslant k \leqslant p-1$, pour tout $\overline{m} \in \mathbb{Z}/p\mathbb{Z}$ on a $\text{card}(\overline{m} \cdot A) = k$. L'ensemble $\mathcal{P}_k(X)$ des parties de X de cardinal k est donc stable par l'action et donc réunion disjointe d'orbites. Or le cardinal d'une orbite divise $[\mathbb{Z}/p\mathbb{Z} : 1] = p$ et vaut donc 1 ou p. Dans $\mathcal{P}(X)$, les seules orbites ponctuelles sont $\{\emptyset\}$ et $\{X\}$. Donc $\mathcal{P}_k(X)$ est, pour $1 \leqslant k \leqslant p-1$, réunion disjointe d'orbites ayant p éléments et $C_p^k = \text{card}(\mathcal{P}_k(X))$ est divisible par p.

Exercice 1. Soient X un ensemble fini de cardinal $n \in \mathbb{N}^*$ et p un nombre premier. On considère la permutation circulaire $c = (1, 2, \ldots, p) \in \mathcal{S}_p$.

a) Montrer que l'on définit une action du groupe $\mathbb{Z}/p\mathbb{Z}$ sur X^p en posant :

(1) $\forall\, \overline{k} \in \mathbb{Z}/p\mathbb{Z} \quad \forall x = (x_1, \ldots, x_p) \in X^p \qquad \overline{k} \cdot x = (x_{c^k(1)}, \ldots, x_{c^k(p)})$

b) En utilisant l'équation des classes, montrer que $n^p \equiv n \pmod{p}$.

c) En appliquant la formule de Burnside, retrouver ce théorème (dû à Fermat).

Solution. a) Comme n'importe quel groupe, $\mathbb{Z}/p\mathbb{Z}$ agit par translations sur lui-même en posant $\overline{k}\cdot\overline{m} = \overline{k}+\overline{m} = \overline{k+m}$. Avec $k=1$, on obtient le cycle $c : \overline{m} \mapsto \overline{1+m}$. On a $c^k : \overline{m} \mapsto \overline{k+m} = \overline{k}\cdot\overline{m}$. D'après 2-1, ex. on en déduit une action sur $\mathcal{F}(\mathbb{Z}/p\mathbb{Z}, X) = X^p$, d'expression donnée par (1).

b) $x = (x_1, \ldots, x_p) \in X^p$ a une orbite ponctuelle, si et seulement si on a :

$$\overline{1}\cdot x = (x_2, \ldots, x_p, x_1) = x \qquad \text{soit si} \qquad x_1 = x_2 = \cdots = x_p .$$

Il existe donc n orbites ponctuelles associées aux n choix de $x_1 \in X$.

Soit k le nombre total d'orbites (dont n ponctuelles). Le cardinal de chacune des $k-n$ orbites non ponctuelles divise $[\mathbb{Z}/p\mathbb{Z} : 1] = p$ premier et vaut donc p. L'équation des classes donne $n^p = \text{card}\,(X^p) = n + (k-n)p$.

c) D'après la formule de Burnside,

$$kp = k\,[\mathbb{Z}/p\mathbb{Z} : 1] = \sum_{\overline{k}\in\mathbb{Z}/p\mathbb{Z}} \text{card}\left(\text{fix}(\overline{k})\right) = n^p + n(p-1) .$$

En effet pour $\overline{k} = \overline{0}$, on a $\text{fix}(\overline{k}) = \text{fix}(\text{Id}_{X^p}) = X^p$ de cardinal n^p.
Pour $\overline{k} \neq \overline{0}$, on a $o(\overline{k}) = p$ et donc $\text{fix}(\overline{k}) = \{(x, \ldots, x) ;\ x \in X\}$ de cardinal n.

Exercice 2. On dispose d'un fil circulaire, de 4 perles bleues, de 3 perles blanches et de 2 perles oranges. Combien de colliers différents peut-on faire avec ce matériel ?

Solution. Sur le cercle, réservons 9 emplacements $A_0, A_1, \ldots, A_8$ régulièrement espacés. Notons P cet ensemble de points et O le centre du cercle. Pour faire un collier, on réservera l'une des $\frac{9!}{4!3!2!} = 1260$ partitions $(4,3,2)$ de P. Soit X l'ensemble de ces partitions. Deux partitions, éléments de X, donneront deux colliers identiques, si on passe de l'une à l'autre par l'une des 9 rotations r^k d'angle $k\frac{2\pi}{9}$, où $0 \leqslant k \leqslant 8$, ou encore par l'une des neuf symétries orthogonales conservant le polygone P. Le nombre k de colliers différents est donc le nombre d'orbites dans X sous l'action du groupe diédral D_9 (D_9 agit sur P et donc sur $\mathcal{P}(P)$ et sur X qui est une partie stable de $\mathcal{P}(P)$). Calculons k à l'aide de la formule de Burnside. Soit $g \in D_9$. Une partition élément de X appartient à $\text{fix}(g)$, si g laisse globalement invariant les trois ensembles des perles bleues, des perles blanches, des perles oranges.

- Si $g = \text{Id}$, on a $\text{card}\,(\text{fix}(g)) = \text{card}\,(X) = 1260$.

- Si $g = r^k$, où $0 < k \leqslant 8$, l'ordre de g divise $o(r) = 9$ et vaut 3 ou 9. Les orbites dans P sous l'action de g (et ses puissances) ont toutes 3 ou 9 éléments. Une partie de P invariante par g est une réunion de telles orbites. Elle a donc un cardinal multiple de 3. L'ensemble des perles bleues qui a 4 éléments ne peut être globalement invariant par g. Aucun élément de X n'est invariant par g. Donc $\text{fix}(g)$ est vide.

- Si g est une symétrie, par exemple autour de la droite (OA_0), alors en A_0 il y a nécessairement une perle blanche car les parties invariantes par g sont réunions de couples de points symétriques (distincts si on excepte A_0). Pour constituer un collier invariant par g, il suffit de placer, comme on voudra, 2 perles bleues, 1 perle blanche, 1 perle rouge en A_1, A_2, A_3, A_4, puis de compléter le collier par symétrie par rapport à (OA_0). Cela laisse $\frac{4!}{2!1!1!} = 12$ possibilités. La formule de Burnside donne :

$$k = \frac{1}{[D_9 : 1]} \sum_{g\in D_g} \text{card}\,(\text{fix}(g)) = \frac{1}{18}[1260 + 12\times 9] = 76 .$$

2.4 Théorème de Cauchy

Proposition. (th. de Cauchy)

Soit G un groupe fini d'ordre n et soit p un facteur premier de n. Il existe dans G des éléments d'ordre p.

Démonstration. Soit $E = \{(x_1, \dots, x_p) \in G^p \mid x_1 \cdots x_p = e\}$. Soit $c = (1, 2, \dots, p) \in \mathcal{S}_p$. On définit une action du groupe $\mathbb{Z}/p\mathbb{Z}$ sur G^p (voir 2-3, ex. 1) en posant :

$$(1) \qquad \forall\, \overline{k} \in \mathbb{Z}/p\mathbb{Z} \quad \forall\, x = (x_1, \dots, x_p) \in G^p \qquad \overline{k}\cdot x = (x_{c^k(1)}, \dots, x_{c^k(p)})\,.$$

Alors, $E = \{(x_1, \dots, x_p) \in G^p \mid x_1 \cdots x_p = e\}$ est une partie de G^p stable pour cette action. En effet, si $x = (x_1, \dots, x_p) \in E$, on a :

$$\overline{1}\cdot x = (x_2, \dots, x_p, x_1) \quad \text{avec} \quad x_2 \cdots x_p x_1 = x_1^{-1}(x_1 x_2 \cdots x_p)x_1 = x_1^{-1} e x_1 = e\,.$$

On a donc $\overline{1}\cdot x \in E$. Par récurrence $\overline{k}\cdot x = \overline{1}\cdot(\overline{k-1}\cdot x) \in E$ pour $1 \leqslant k \leqslant p-1$.

Un élément $x = (x_1, \dots, x_p)$ de E est défini en donnant $(x_1, \dots, x_{p-1}) \in G^{p-1}$. La valeur de x_p se déduit ensuite de la relation $x_1 \cdots x_p = e$. Donc $\operatorname{card}(E) = n^{p-1}$. Comme en 2-3, ex. 1, b), l'orbite de x est ponctuelle si et seulement si $x_1 = \cdots = x_p$. Les orbites ponctuelles correspondent aux éléments x_1 de G tels que $x_1^p = e$, c'est-à-dire dont l'ordre divise p. A part e d'ordre 1, on obtiendra ainsi les éléments de G d'ordre p. Soit k le nombre total d'orbites et soit s le nombre d'orbites ponctuelles. Le cardinal d'une orbite non ponctuelle divise $[\mathbb{Z}/p\mathbb{Z} : 1] = p$ et vaut p. L'équation des classes donne $n^{p-1} = \operatorname{card}(E) = s + (k-s)p$. Par hypothèse on a $n \equiv 0 \pmod p$ et donc $s \equiv 0 \pmod p$. On a $s \neq 0$ car $e \in E$ a une orbite ponctuelle. Il existe donc au moins p orbites ponctuelles et donc au moins $p-1$ éléments d'ordre p dans G. ∎

Corollaire.

Soient G un groupe fini et $p \in \mathbb{N}$ premier. Pour que l'ordre de G soit une puissance de p, il faut et il suffit que l'ordre de tout élément de G soit une puissance de p.

Démonstration. D'après le th. de Lagrange la condition est nécessaire. D'après la proposition, elle est suffisante : si la décomposition en facteurs premiers de $[G : 1]$ comportait un facteur premier $q \neq p$, il existerait un élément d'ordre q dans G. ∎

2.5 Théorème d'isomorphisme de Noether

Soit G un groupe. D'après 1-6, ex., $x \mapsto \mathrm{Ad}_x$ est un homomorphisme de G dans le groupe $\mathrm{Aut}(G)$. C'est une action par automorphismes de G sur G. Pour cette action, l'orbite de $y \in G$ est l'ensemble $\{xyx^{-1} \mid x \in G\}$ des conjugués de y.

On a vu en 2-1, ex. que G agit sur $\mathcal{P}(E)$. Soient H est un sous-groupe de G et $x \in G$. Alors $x\cdot H = \mathrm{Ad}_x(H)$ est un sous-groupe de G. Ainsi, G laisse stable l'ensemble des sous-groupes de G et agit donc sur cet ensemble. Le stabilisateur du sous-groupe H pour cette action,

$$N_H = \{\, g \in G \mid gHg^{-1} = H \,\},$$

est un sous-groupe de G. Il contient H et on a $H \triangleleft N_H$.

Définition.

On appelle N_H le normalisateur de H dans G.

Proposition. (th. de E. Noether)

Soient G un groupe, H, K des sous-groupes de G tels que $K \subset N_H$.
(i) *On a $HK = KH$ et c'est le sous-groupe de G engendré par H et K.*
(ii) *$H \cap K$ est un sous-groupe distingué de K et H est distingué dans HK.*
(iii) *Les groupes HK/H et $K/(H \cap K)$ sont canoniquement isomorphes.*

Démonstration. (i) Pour tout $h \in H$ et pour tout $k \in K$, on a $hk = k(k^{-1}hk) \in KH$ car K normalise H. De même, $kh = (khk^{-1})k \in HK$. On a donc $HK = KH$. De plus, HK est un sous-groupe de G car pour tous $h, h' \in H$ et pour tous $k, k' \in K$,

$$(hk)(h'k') = [h(kh'k^{-1})]kk' \in HK \quad \text{et} \quad (hk)^{-1} = k^{-1}h^{-1} \in KH = HK.$$

Ce sous-groupe contient H et K et contient donc le sous-groupe engendré par H et K. Or, ce dernier contient tous les éléments hk de HK. Il est donc égal à HK.

(ii) Pour $h \in H \cap K$ et $k \in K$ on a $khk^{-1} \in H$ car $K \subset N_H$ et $khk^{-1} \in K$ car K est un sous-groupe. Ainsi $khk^{-1} \in H \cap K$ et $H \cap K$ est distingué dans K. Comme H est distingué dans N_H, il est distingué dans HK puisque $H \subset HK \subset N_H$.

(iii) Notons f l'homomorphisme de K dans HK/H obtenu en restreignant au sous-groupe K l'homomorphisme $x \mapsto \overline{x}$ de HK sur HK/H. Cet homomorphisme est surjectif car tout élément de HK/H est de la forme $\overline{hk} = \overline{e}\overline{k} = \overline{k}$. Pour $k \in K$, on a :

$$k \in \mathrm{Ker}\,(f) \quad \Leftrightarrow \quad \overline{k} = \overline{e} \quad \Leftrightarrow \quad k \in H \quad \Leftrightarrow \quad k \in H \cap K.$$

Ainsi $\mathrm{Ker}\,(f) = H \cap K$. Par factorisation de f à travers son noyau $H \cap K$ on obtient un isomorphisme de $K/(H \cap K)$ sur HK/H. ∎

Remarque. Un sous-groupe H de G est distingué, si et seulement si $N_H = G$. Pour tout sous-groupe K de G on a alors $K \subset N_H$. Le th. de Noether s'applique. En particulier, HK est un sous-groupe de G (voir 1-8, ex.). Si G est fini et si on connait les ordres de $H, K, H \cap K$, on déduit du th. de Noether l'ordre de HK.

En particulier, si H et K sont deux sous-groupes d'un groupe commutatif, les groupes $(H + K)/H$ et $K/(H \cap K)$ sont isomorphes.

Exercice. Soit G un groupe d'ordre $2p$, avec $p > 2$ premier. Montrer qu'il existe dans G des sous-groupes H et K d'ordres p et 2 et que l'on a $G = HK$, $H \triangleleft G$ et $H \cap K = \{e\}$.

Solution. Il existe dans G un élément a d'ordre p et un élément b d'ordre 2 (th. de Cauchy). Les sous-groupes H et K, engendrés par a et b, sont d'ordres p et 2. D'après le th. de Lagrange, H est d'indice $\frac{[G:1]}{[H:1]} = 2$. Il est donc distingué (1-8, cor.). D'après le th. de Noether, HK est un sous-groupe de G. D'après le th. de Lagrange, puisque HK contient H et K, son ordre est multiple de $p = [H : 1]$ et de $2 = [K : 1]$ et donc multiple de $\mathrm{ppcm}(p, 2) = 2p$. On a $[HK : 1] \geqslant 2p$ et donc $HK = G$. L'ordre de $H \cap K$ divise $p = [H : 1]$ et $2 = [K : 1]$ et vaut donc 1. Ainsi $H \cap K = \{e\}$.

2.6 Produits semi-directs

Proposition.

Soit $\alpha : k \mapsto \alpha_k$ une action par automorphismes d'un groupe K sur un autre groupe H. Alors, $G = H \times K$ muni de la loi de composition interne définie par :

$$(h\,,k)\,(h'\,,k') \;=\; (h\,\alpha_k(h')\,,kk')\,.$$

est un groupe, $f : h \mapsto (h,e)$ et $g : k \mapsto (e,k)$ sont des homomorphismes injectifs de H et K sur des sous-groupes $H' = H \times \{e\}$ et $K' = \{e\} \times K$ de G et on a :

$$H' \lhd G \quad , \quad H' \cap K' = \{e\} \quad , \quad H'K' = K'H' = G\,.$$

Démonstration. On a $\alpha_e = \mathrm{Id}_H$ car $\alpha \in \mathrm{Hom}\,(K, \mathrm{Aut}\,(H))$. Pour tout $k \in K$, on a $\alpha_k(e) = e$ car $\alpha_k \in \mathrm{Aut}\,(H)$. On en déduit que pour tout $(h,k) \in H \times K$,

$$(h\,,k)\,(e\,,e) = (h\,\alpha_k(e)\,,ke) = (h\,,k) \quad \text{et} \quad (e\,,e)\,(h\,,k) = (e\,\alpha_e(h)\,,ek) = (h\,,k)\,.$$

Ainsi (e,e) est élément neutre. La loi de composition est associative. En effet, comme $\alpha_{kk'} = \alpha_k \circ \alpha_{k'}$, les expressions suivantes sont égales :

$$\begin{array}{rcl} [(h\,,k)\,(h'\,,k')]\,(h''\,,k'') & = & (h\,\alpha_k(h')\,,kk')\,(h''\,,k'') \;=\; (h\,\alpha_k(h')\,\alpha_{kk'}(h'')\,,kk'k'') \\ (h\,,k)\,[(h'\,,k')\,(h''\,,k'')] & = & (h\,,k)(h'\,\alpha_{k'}(h'')\,,k'k'') \;=\; (h\,\alpha_k[h'\,\alpha_{k'}(h'')]\,,kk'k'') \end{array}$$

On vérifiera que tout $(h,k) \in G$ a pour inverse $(\alpha_{k^{-1}}(h^{-1}), k^{-1})$. Donc G est un groupe. Les applications injectives f et g sont des homomorphismes car :

$$\begin{array}{rcl} f(h)f(h') & = & (h\,,e)\,(h'\,,e) \;=\; (h\,\alpha_e(h')\,,e) \;=\; (hh'\,,e) \;=\; f(hh')\,, \\ g(k)g(k') & = & (e\,,k)\,(e\,,k') \;=\; (e\,\alpha_k(e)\,,kk') \;=\; (e\,,kk') \;=\; g(kk')\,. \end{array}$$

Comme $s : (h\,,k) \mapsto k$ est un homomorphisme de groupes, son noyau H' est un sous-groupe distingué de G. D'après 1-6, lemme, on a $G = s^{-1}(s(K')) = H'K' = K'H'$. Il est clair que $H' \cap K' = \{e\}$. ∎

Définition.

Ce groupe G est appelé le produit semi-direct associé à l'action α de K sur H. On le note $H \times_\alpha K$.

Remarque. L'homomorphisme $s : (h\,,k) \mapsto k$ est surjectif, de $H \times_\alpha K$ sur K. Son noyau est $H' = H \times \{e\}$ isomorphe par f à H. Par factorisation de s on voit que $(H \times_\alpha K)/H'$ est isomorphe à K. Dans la suite

$$\{e\} \quad \xrightarrow{\mathrm{Id}} \quad H \quad \xrightarrow{f} \quad H \times_\alpha K \quad \xrightarrow{s} \quad K \quad \xrightarrow{j} \quad \{e\}\,,$$

l'image de chaque homomorphisme est le noyau du suivant. On exprime cette propriété en disant que cette suite d'homomorphismes est *exacte*.

De plus, on a $s \circ g = \mathrm{Id}_K$, où $g : k \mapsto (e,k)$. L'homomorphisme g est une "section" de la surjection s et plonge $K \simeq G/K'$ injectivement dans $H \times_\alpha K$.

Exercice. Considérons un espace vectoriel E, l'action $\alpha : (u, \overrightarrow{x}) \mapsto u(\overrightarrow{x})$ du groupe $\mathrm{GL}(E)$ sur E. Montrer que le groupe $G = E \times_\alpha \mathrm{GL}(E)$ est isomorphe à un sous-groupe du groupe $\mathcal{S}_E$ des permutations de E (bijections de E sur E).

Solution. L'opération de G est définie par $(\overrightarrow{a},u)(\overrightarrow{b},v) = (\overrightarrow{a}+u(\overrightarrow{b}),uv)$. Notons $t_{\vec{a}}$ la translation de vecteur $\overrightarrow{a}$ et posons $\varphi(\overrightarrow{a},u) = t_{\vec{a}} \circ u$. On a $t_{\vec{a}} \in S_E$ et donc $t_{\vec{a}} \circ u \in S_E$. Vérifions que $\varphi \in \mathrm{Hom}\,(G, S_E)$. Comme $u \circ t_{\vec{a}} \circ u^{-1} = t_{u(\vec{a})}$, on a

$$\begin{aligned}\varphi(\overrightarrow{a},u)\varphi(\overrightarrow{b},v) &= t_{\vec{a}} \circ u \circ t_{\vec{b}} \circ v = t_{\vec{a}} \circ (u \circ t_{\vec{b}} \circ u^{-1}) \circ u \circ v \\ &= t_{\vec{a}+u(\vec{b})} \circ (u \circ v) = \varphi[(\overrightarrow{a}+u(\overrightarrow{b}),u \circ v)] = \varphi[(\overrightarrow{a},u)(\overrightarrow{b},v)]\,.\end{aligned}$$

De plus, φ est injectif. En effet,

$$\begin{aligned}(\overrightarrow{a},u) \in \mathrm{Ker}\,(\varphi) &\Leftrightarrow t_{\vec{a}} \circ u = \mathrm{Id}_E \\ &\Leftrightarrow u = t_{-\vec{a}} \\ &\Rightarrow \overrightarrow{0} = u(\overrightarrow{0}) = t_{-\vec{a}}(\overrightarrow{0}) = -\overrightarrow{a} \\ &\Rightarrow \overrightarrow{a} = \overrightarrow{0}\,,\end{aligned}$$

d'où $u = \mathrm{Id}_E$. Ainsi G est isomorphe au sous-groupe $\varphi(G)$ de $\mathcal{S}_E$ dont les éléments sont les composés d'une application linéaire bijective u et d'une translation (qui elle n'est pas linéaire). C'est le groupe des isomorphismes affines de E que nous étudierons en détail dans la partie II de cet ouvrage. Si $E = \mathbb{R}$, c'est le groupe des transformations $x \mapsto ax+b$, où $a \in \mathbb{R}^*$ et $b \in \mathbb{R}$. Si $E = \mathbb{C}$, c'est le groupe des similitudes directes du plan d'expression $z \mapsto az+b$, où $a \in \mathbb{C}^*$ et $b \in \mathbb{C}$.

2.7 Caractérisation des produits semi-directs

Proposition.

Soient G un groupe et H et K deux sous-groupes tels que

$$H \lhd G \quad , \quad H \cap K = \{e\} \quad , \quad HK = G\,.$$

Alors $f : (h,k) \mapsto hk$ de $H \times K$ dans G est un isomorphisme du produit semi-direct $H \times_\alpha K$ sur G, où α désigne l'action $\alpha : k \mapsto \mathrm{Ad}_k\,|_H$ de K sur H.

Démonstration. Tout automorphisme intérieur Ad_k de G laisse stable $H \lhd G$ et induit par restriction un automorphisme $\alpha_k = \mathrm{Ad}_k\,|_H$ de H. Ainsi, $\alpha : k \mapsto \mathrm{Ad}_k\,|_H$ est une action par automorphismes de K sur H.

L'application f est surjective puisque $HK = G$. Si $hk = h'k'$ on a $kk'^{-1} = h^{-1}h'$ et cet élément appartient à $H \cap K = \{e\}$ donc $k = k'$ et $h = h'$. Cela prouve que f est injective et donc bijective. Pour tous (h,k), $(h',k') \in H \times_\alpha K$, on a

$$\begin{aligned}f(h,k)\,f(h',k') &= hkh'k' = hkh'k^{-1}kk' = h\alpha_k(h')kk' \\ &= f(h\alpha_k(h'),kk') = f((h,k)(h',k'))\,.\end{aligned}$$

Donc f est un isomorphisme de $H \times_\alpha K$ sur G. ∎

Corollaire.

Avec les données de la proposition, les conditions suivantes sont équivalentes.

(i) *Le groupe $G = HK$ est le produit direct des sous-groupes H et K.*

(ii) *K est distingué dans G.*

(iii) *$hk = kh$ pour tout $h \in H$ et pour tout $k \in K$.*

(iv) *L'action $\alpha : k \mapsto \mathrm{Ad}_k\,|_H$ est triviale (telle que $\alpha_k = \mathrm{Id}_H$, pour tout $k \in K$).*

Démonstration. (i) ⇔ (ii) d'après la caractérisation des produits directs, en 1-11.

(iii) ⇔ (iv) car $\alpha_k = \mathrm{Id}_H \quad \Leftrightarrow \quad \forall\, h \in H \quad khk^{-1} = h \quad \Leftrightarrow \quad \forall\, h \in H \quad kh = hk$.

(i) $\Rightarrow$ (iii) a été vu en 1-11.

(iii) $\Rightarrow$ (ii) Supposons que $hk = kh$ pour tout $h \in H$ et pour tout $k \in K$. Pour tout $k' \in K$ et tout élément $g = hk$ de G, (où $h \in H$ et $k \in K$), on a

$$gk'g^{-1} = (hk)k'(k^{-1}h^{-1}) = h(kk'k^{-1})h^{-1} = (kk'k^{-1})hh^{-1} = kk'k^{-1} \in K.$$

Donc K est distingué dans G. ∎

Exercice 1. Une suite $\ldots \to H_{i-1} \overset{f_i}{\to} H_i \overset{f_{i+1}}{\to} H_{i+1} \to \ldots$d'homomorphismes de groupes est dite exacte si $\mathrm{Im}\,(f_i) = \mathrm{Ker}\,(f_{i+1})$ pour tout i. On suppose

$$(1) \qquad \{e\} \xrightarrow{\mathrm{Id}} H \xrightarrow{f} G \xrightarrow{s} K \xrightarrow{j} \{e\}$$

exacte et on suppose qu'il existe $g \in \mathrm{Hom}\,(K, G)$ tel que $s \circ g = \mathrm{Id}_K$. Montrer que G est isomorphe à un produit semi-direct $H \times_\alpha K$.

Solution. On a $\mathrm{Ker}\,(f) = \mathrm{Im}\,(\mathrm{Id}) = \{e\}$ donc f est injectif. C'est un isomorphisme de H sur $H' = f(H)$. On a $H' = \mathrm{Im}\,(f) = \mathrm{Ker}\,(s)$ et donc $H' \lhd G$. On a $\mathrm{Im}\,(s) = \mathrm{Ker}\,(j) = K$ donc s est surjectif. On a g injectif car $s \circ g = \mathrm{Id}_K$ donc $K' = g(K)$ est un sous-groupe de G isomorphe à K. Soit $x \in H' \cap K'$. On a $x \in H' = \mathrm{Ker}\,(s)$ donc $s(x) = e$. Comme $x \in K' = g(K)$, il existe $y \in K$ tel que $x = g(y)$. On en déduit que $e = s(x) = s(g(y)) = y$, puis $x = g(y) = e$. Ainsi $H' \cap K' = \{e\}$. Considérons $x \in G$ et posons $k' = g(s(x)) \in K'$. Puisque $s \circ g = \mathrm{Id}_K$, on a $s(x) = (s \circ g)(s(x)) = s(k')$. Il existe donc $h' \in H' = \mathrm{Ker}\,(s)$ tel que $x = h'k'$, ce qui prouve que $H'K' = G$. Ainsi, G est isomorphe à un produit semi-direct de H' par K' et donc isomorphe à un produit semi-direct de H par K.

Quand on a une suite exacte comme (1), on dit que G est une extension du groupe H par K. S'il existe un homomorphisme g section de s, on dit que cette extension est scindée. D'après cet exercice, l'extension est scindée si et seulement si G est un produit demi-direct.

Exercice 2. Reprenons l'étude d'un groupe G d'ordre $2p$ avec $p > 2$ premier (2-5, ex.). Admettons, (vu en 3-5), qu'un groupe d'ordre p premier est isomorphe à $\mathbb{Z}/p\mathbb{Z}$. Montrer qu'à isomorphisme près G n'a que deux structures possibles.

Solution. D'après 2-5, ex., il existe des sous-groupes H et K de G d'ordres p et 2 et vérifiant $H \lhd G$, $HK = G$, $H \cap K = \{e\}$. La proposition montre que $G \simeq H \times_\varphi K$ avec $\varphi : k \mapsto \mathrm{Ad}_k\,|_H$. La propriété admise montre que $G \simeq (\mathbb{Z}/p\mathbb{Z}) \times_\alpha (\mathbb{Z}/2\mathbb{Z})$, où $\alpha \in \mathrm{Hom}\,(\mathbb{Z}/2\mathbb{Z}, \mathrm{Aut}\,(\mathbb{Z}/p\mathbb{Z}))$. D'après 1-9, cor. 1, $[\mathrm{Im}\,(\alpha) : 1]$ divise $2 = [\mathbb{Z}/2\mathbb{Z} : 1]$.

- Si $[\mathrm{Im}\,(\alpha) : 1] = 1$, alors α est trivial. D'après le corollaire ci-dessus, G est isomorphe au produit direct $(\mathbb{Z}/p\mathbb{Z}) \times (\mathbb{Z}/2\mathbb{Z})$ (commutatif, isomorphe à $\mathbb{Z}/2p\mathbb{Z}$ d'après 3-4).

- Si $[\mathrm{Im}\,(\alpha) : 1] = 2$, alors $\gamma = \alpha(\overline{1})$ est un automorphisme de $\mathbb{Z}/p\mathbb{Z}$ d'ordre 2. Posons $\overline{k} = \gamma(\overline{1}) \in \mathbb{Z}/p\mathbb{Z}$. On a $\overline{1} = \gamma^2(\overline{1}) = \gamma(\overline{k}) = \gamma(k\overline{1}) = k\gamma(\overline{1}) = k\overline{k} = \overline{k^2} = (\overline{k})^2$. Comme p est premier, $\mathbb{Z}/p\mathbb{Z}$ est un corps donc $\overline{k} = \overline{1}$ et $\overline{k} = -\overline{1}$ sont les seules racines du polynôme $X^2 - \overline{1}$. Puisque α n'est pas trivial, on a $\gamma \neq \mathrm{Id}$ et donc $\overline{k} \neq \overline{1}$. Ainsi, $\overline{k} = -\overline{1}$ et $\gamma(\overline{m}) = -\overline{m}$ pour tout $\overline{m} \in \mathbb{Z}/p\mathbb{Z}$. On connait donc parfaitement l'action α : on a $\alpha(\overline{0}) = \mathrm{Id}$ et $\alpha(\overline{1}) : \overline{k'} \mapsto -\overline{k'}$. Alors, d'après la proposition 2-6, la loi de composition interne du groupe $(\mathbb{Z}/p\mathbb{Z}) \times_\alpha (\mathbb{Z}/2\mathbb{Z})$ est définie par :

$$(\overline{k}, \overline{0})(\overline{k}', \overline{m}) = (\overline{k} + \overline{k}', \overline{m}) \quad , \quad (\overline{k}, \overline{1})(\overline{k}', \overline{m}) = (\overline{k} - \overline{k}', \overline{1+m}).$$

Ce groupe est isomorphe au groupe diédral D_{2p} (voir 5-2, cor.).

Exercices du chapitre 2

Ex 2 - 1

Soit G un groupe opérant à gauche sur l'ensemble $E = \{1, \ldots, n\}$. Montrer que G agit naturellement sur l'ensemble $\mathcal{P}_{n_1,\ldots,n_s}$ des partitions de E en s parties ayant $n_1, \ldots, n_s$ éléments, où s et $n_1, \ldots, n_s$ sont donnés (avec $\sum_{i=1}^{n} n_i = n$).

Si $G = \mathcal{S}_n$, groupe des permutations de $E = \{1, \ldots, n\}$, calculer le cardinal, de l'orbite, du stabilisateur d'une partie X de E (respectivement d'une partition $(X_1, \ldots, X_s) \in \mathcal{P}_{n_1,\ldots,n_s}$). Retrouver ainsi des formules classiques.

Ex 2 - 2

On considère une action non triviale du groupe $\mathbb{Z}/p\mathbb{Z}$, où p est premier, sur un ensemble E ayant p éléments. Montrer que $\mathbb{Z}/p\mathbb{Z}$ agit transitivement sur E. Pour l'action sur $\mathcal{P}(E)$ qui en résulte, écrire l'équation des classes, la formule de Burnside. Commenter le résultat.

Ex 2 - 3

Combien de colliers différents peut-on confectionner avec 4 perles rouges, 6 perles blanches, 4 perles jaunes ?

Ex 2 - 4

Soient G un groupe, H un sous-groupe.

a) Montrer qu'en posant $g \cdot aH = (ga)H$, où $a \in G$, $g \in G$, on définit une action de G sur l'ensemble G/H des classes à gauche modulo H.

b) Montrer que cette action est transitive. Déterminer le stabilisateur de aH.

c) On suppose G fini. Calculer le cardinal d'une orbite et retrouver un théorème classique.

Ex 2 - 5

Soient G un groupe, H, K deux sous-groupes de G.

a) Montrer que les parties Hg, où $g \in G$, constituent une partition de G.

b) Soit $g \in G$. Montrer que
$\Gamma_g = \{(h,k) \in H \times K \mid hg = gk\}$
est un sous-groupe du groupe $H \times K$.

c) On suppose que G est fini et que $HK = G$.
Montrer que $[\Gamma_g : 1]$ ne dépend que de H et de K et non de $g \in G$. Calculer sa valeur pour $g = e$ et en déduire que $[G : 1][H \cap K : 1] = [H : 1][K : 1]$.
Si $H \triangleleft G$, donner une autre démonstration de cette relation.

Ex 2 - 6

Soient G un groupe, H un sous-groupe d'indice fini de G. En utilisant le th. de Poincaré (Ex. 1-8), montrer qu'il existe un sous-groupe distingué de G, d'indice fini, inclus dans H.

Ex 2 - 7

Considérons un corps commutatif K et $E = \mathcal{M}_{m,n}(K)$ (où $m \geqslant 1$, $n \geqslant 1$).

a) Montrer qu'en posant $(P,Q) \cdot A = PAQ^{-1}$ on définit une action du groupe $G = \mathrm{GL}(m,K) \times \mathrm{GL}(n,K)$ sur l'espace vectoriel $E = \mathcal{M}_{m,n}(K)$.

b) Décrire la relation de conjugaison pour cette action, les orbites. Donner le cardinal de l'ensemble des orbites.

Ex 2 - 8

Soit $\mathrm{GL}(n,\mathbb{Z})$ l'ensemble des matrices $A \in \mathcal{M}_n(\mathbb{Z})$ telles qu'il existe $B \in \mathcal{M}_n(\mathbb{Z})$ vérifiant $AB = I_n$. On note (E_{ij}) la base canonique de $\mathcal{M}_n(\mathbb{R})$.

a) Soit $A \in \mathcal{M}_n(\mathbb{Z})$. Montrer que A est élément de $\mathrm{GL}(n,\mathbb{Z})$ si et seulement si $\det(A) \in \{1,-1\}$. Montrer que $\mathrm{SL}(n,\mathbb{Z}) = \{A \in \mathrm{GL}(n,\mathbb{Z}) | \det(A) = 1\}$ est un sous-groupe distingué de $\mathrm{GL}(n,\mathbb{Z})$, d'indice 2.

b) Pour $i \neq j$ on pose $T_{ij} = I_n + E_{ij}$ et pour $k \in \mathbb{Z}$ on pose $T_{ij}(k) = I_n + kE_{ij}$, de sorte que $T_{ij}(1) = T_{ij}$.

(i) Montrer que $\varphi : k \mapsto T_{ij}(k)$ est un homomorphisme de groupes injectif de $\mathbb{Z}$ dans $\mathrm{SL}(n,\mathbb{Z})$. Montrer que $(T_{ij})^k = T_{ij}(k)$. Quelle est la matrice inverse de $T_{ij}(k)$?

(ii) Quels sont les coefficients des matrices $S_{ij} = T_{ij}T_{ji}^{-1}T_{ij}$ et $(S_{ij})^2$.

(iii) Si on multiplie à gauche une matrice $A \in \mathcal{M}_n(\mathbb{Z})$, par $T_{ij}(k)$ ou S_{ij} ou $(S_{ij})^2$, indiquer comment les lignes de A sont modifiées.

c) On considère le sous-groupe G de $\mathrm{SL}(n,\mathbb{Z})$ engendré par la famille $\mathcal{T}$ des matrices T_{ij} où $i \neq j$. Pour $(P,Q) \in G \times G$ et $A \in \mathcal{M}_n(\mathbb{Z})$ on pose $(P,Q)\cdot A = PAQ^{-1}$.
Montrer que l'on définit ainsi une action du groupe $G \times G$ sur $\mathcal{M}_n(\mathbb{Z})$.

d) Soit $A \in \mathcal{M}_n(\mathbb{Z})$ non nulle.

(i) En adaptant la méthode de Gauss classique pour réduire une matrice, montrer que l'ensemble $\mathcal{E}$ des $B \in \mathrm{GL}(n,\mathbb{Z})$ qui sont conjuguées de A et telles que $b_{11} > 0$, est non vide.

(ii) Soit d le minimum des valeurs de b_{11} sur l'ensemble $\mathcal{E}$ et soit $B \in \mathcal{E}$ pour laquelle le minimum d est atteint. En utilisant la méthode du pivot de Gauss, montrer que d divise $b_{21}, \ldots, b_{n1}$.

(iii) Montrer qu'il existe C, conjuguée de A, de la forme

$$\begin{pmatrix} d & 0 & \ldots & 0 \\ 0 & c_{22} & \ldots & c_{2n} \\ . & . & \ldots & . \\ 0 & c_{n2} & \ldots & c_{nn} \end{pmatrix}.$$

(iv) Pour $2 \leqslant i \leqslant n$, $2 \leqslant j \leqslant n$, montrer que d divise c_{ij}.

(v) Montrer qu'il existe $D \sim A$ dont les seuls termes non nuls sont $d_{11} = d_1$, $d_{22} = d_2, \ldots, d_{rr} = d_r$, ces termes étant tels que $d_1 \mid d_2 \mid \ldots \mid d_r$.

e) Déduire de ce qui précède, que $\mathrm{SL}(n,\mathbb{Z})$ est engendré par les matrices T_{ij} où $i \neq j$.

f) Montrer que pour tout $A \in \mathrm{GL}(n,\mathbb{Z})$ il existe des matrices de transvections $T_1, \ldots, T_s$ du type $T_{ij}(k)$ où $k \in \mathbb{Z}$ et une matrice diagonale D_α, de diagonale $(1, \ldots, 1, \alpha)$ où $\alpha = \pm 1$ telles que $A = T_1 \cdots T_s D_\alpha$.

g) (i) Montrer que $T = T_{21}$ et $T' = T_{12}$ engendrent le groupe $\mathrm{SL}(2,\mathbb{Z})$. Montrer que T et $S = S_{12}$ constituent un autre système de générateurs.

(ii) Vérifier que $A = \begin{pmatrix} 0 & -1 & 1 \\ 0 & -1 & 0 \\ 1 & -1 & 0 \end{pmatrix}$ est un élément de $\mathrm{SL}(3,\mathbb{Z})$ et écrire explicitement A en fonction des générateurs T_{ij} de $\mathrm{SL}(3,\mathbb{Z})$.

Ex 2 - 9

Soit K un corps commutatif. Pour

$$\lambda \in K^*, \text{ soit } D_\lambda = \begin{pmatrix} 1 & 0 & \cdots & 0 \\ 0 & 1 & \cdots & 0 \\ . & . & \cdots & . \\ 0 & 0 & \cdots & \lambda \end{pmatrix}$$

(matrice de dilatation).
Montrer que $D = \{D_\lambda ;\ \lambda \in K^*\}$ est un sous-groupe de $\mathrm{GL}(n,K)$ et que $\mathrm{GL}(n,K)$ est un produit semi-direct de $\mathrm{SL}(n,K)$ par D.

Ex 2 - 10

Soient G un groupe, H un sous-groupe distingué de G tel que G/H soit un groupe monogène infini. Montrer que G est isomorphe à un produit semi-direct $H \times_\varphi \mathbb{Z}$.

Ex 2 - 11

On considére des groupes H, H', K et une action par automorphismes $\varphi : k \mapsto \varphi_k$ de K sur H. Montrer que $\psi : k \mapsto \psi_k$, où $\psi_k(h, h') = (\varphi_k(h), h')$ est une action par automorphismes de K sur le groupe $H \times H'$ et que les groupes $(H \times H') \times_\psi K$ et $(H \times_\varphi K) \times H'$ sont isomorphes.

Ex 2 - 12

Considérons les groupes $H = \mathbb{Z}/q\mathbb{Z}$ et $K = \mathbb{Z}/p\mathbb{Z}$ où p, q sont des nombres premiers. Supposons que q ne soit pas congru à 1 modulo p. En admettant que pour q premier, $\mathrm{Aut}\,(\mathbb{Z}/q\mathbb{Z})$ est isomorphe à $\mathbb{Z}/(q-1)\mathbb{Z}$ (3-2, rem.), montrer que tout produit semi-direct $H \times_\alpha K$ est direct.

Indications

Ex 2 - 1

On retrouve les valeurs des coefficients du binôme $\binom{n}{k}$ et de $\binom{n}{n_1 \dots n_s}$.

Ex 2 - 2

On obtient $M_p = 2^p - 1 \equiv 1 \pmod p$.

Ex 2 - 3

Voir cours 2-3, ex. 2

Ex 2 - 4

a) Penser à vérifier que la formule posée a un sens.

b) Le stabilisateur de aH est aHa^{-1}.

c) On retrouve le th. de Lagrange.

Ex 2 - 5

a) Introduire une action de $H \times K$.

b) Voir Γ_g comme le stabilisateur d'un élément.

c) L'action introduite en a) est transitive. Exprimer le cardinal de l'orbite.

Ex 2 - 6

Montrer que l'ensemble des conjugués de H est fini et prendre l'interserction.

Ex 2 - 7

La relation de conjugaison est l'équivalence des matrices. Les orbites sont classifiées par le rang.

Ex 2 - 8

Adapter la méthode du pivot de Gauss et utiliser la division euclidienne de $\mathbb{Z}$.

Ex 2 - 9

Vérifier les conditions qui caractérisent la situation de produit semi-direct.

Ex 2 - 10

Mettre en évidence un sous-groupe de G isomorphe à $\mathbb{Z}$.

Ex 2 - 11

$\theta : ((h, k), h') \mapsto ((h, h'), k)$ est un isomorphisme.

Ex 2 - 12

Montrer que la seule action de $\mathbb{Z}/p\mathbb{Z}$ sur $\mathbb{Z}/(q-1)\mathbb{Z}$ est l'action triviale.

Solutions des exercices du chapitre 2

Ex 2 - 1

Une action de G sur E est un homomorphisme $\varphi : g \mapsto \varphi_g$ de G dans $\mathcal{S}_n$. En posant $g\cdot X = \varphi_g(X)$, où $g \in G$, $X \in \mathcal{P}(E)$, on définit une action de G sur $\mathcal{P}(E)$ (2-1, ex.). En posant $g\cdot(X_1,\dots,X_s) = (g\cdot X_1,\dots,g\cdot X_s)$ on définit une action de G sur $\mathcal{P}(E)^s$. Le sous-ensemble $\mathcal{P}_{n_1,\dots,n_s}$ de $\mathcal{P}(E)^s$ est stable pour cette action car φ_g étant une bijection, si $(X_1,\cdots,X_s)$ est une partition de E alors $(\varphi_g(X_1),\dots,\varphi_g(X_s))$ est une autre partition de E et $\text{card}\,(g\cdot X_i) = \text{card}\,(X_i)$ pour $i = 1,\dots,s$. En restreignant l'action des éléments de G sur $\mathcal{P}(E)^s$ à cette partie stable, on obtient une action de G sur $\mathcal{P}_{n_1,\dots,n_s}$.

Supposons que $G = \mathcal{S}_n$. Soit $X \in \mathcal{P}(E)$. Pour tout $Y \in O_X$ il existe $g \in G$ tel que $\varphi_g(X) = Y$ donc $\text{card}\,(X) = \text{card}\,(Y)$ car φ_g est bijective. Réciproquement, si $Y \in \mathcal{P}(E)$ a le même cardinal k que X, il existe une bijection α de X sur Y. Les complémentaires X^c et Y^c ayant le même cardinal $n-k$, il existe une bijection β de X^c sur Y^c. En posant $g(x) = \alpha(x)$ pour $x \in X$ et $g(x) = \beta(x)$ pour $x \in X^c$, on définit une bijection g de E sur E telle que $g\cdot X = Y$. L'orbite O_X est donc l'ensemble des parties de E de même cardinal que X. On a $n+1$ orbites puisque $0 \leqslant \text{card}\,(X) \leqslant n$.

On a $g \in G_X$ si $g\cdot X = X$ et alors $g\cdot X^c = X^c$ car φ_g est bijective. On détermine donc $g \in G_X$ en donnant une permutation α de X et une permutation β de X^c. Ainsi $G_X \simeq \mathcal{S}_k \times \mathcal{S}_{n-k}$ a pour cardinal $k\,!\,(n-k)\,!$. La formule $\text{card}\,(O_X) = \frac{[G:1]}{[G_X:1]} = \frac{n\,!}{k\,!\,(n-k)\,!}$ donne le cardinal C_n^k de l'ensemble des parties de E ayant k éléments.

De même, si $Y = (X_1,\dots,X_s) \in \mathcal{P}_{n_1,\dots,n_s}$, on a $G_Y \simeq \mathcal{S}_{n_1} \times \cdots \times \mathcal{S}_{n_s}$ et l'orbite de Y est $\mathcal{P}_{n_1,\dots,n_s}$. Donc $\text{card}\,(\mathcal{P}_{n_1,\dots,n_s}) = \frac{n\,!}{n_1\,!\cdots n_s\,!}$.

Ex 2 - 2

Ici, $\text{card}\,(O_x) = [(\mathbb{Z}/p\mathbb{Z}) : (\mathbb{Z}/p\mathbb{Z})_x]$ divise p (th. de Lagrange). Comme p est premier, $\text{card}\,(O_x) = 1$ ou p. L'action étant non triviale, il existe $\overline{k} \in \mathbb{Z}/p\mathbb{Z}$ et $x \in E$ tels que $x \neq \overline{k}\cdot x$. Ainsi, on a $\text{card}\,(O_x) \geqslant 2$ et donc $\text{card}\,(O_x) = p$. Comme $\text{card}\,(E) = p$, on a $E = O_x$. L'action est transitive. Les éléments de E sont $\overline{0}\cdot x = x$, $\overline{1}\cdot x$, $\overline{2}\cdot x = \overline{1}\cdot(\overline{1}\cdot x)$, …, $\overline{p-1}\cdot x$, avec $\overline{p}\cdot x = x$. Ainsi, $s : y \mapsto \overline{1}\cdot y$ est une permutation circulaire des éléments de $O_x = E$ et $\overline{k}\cdot y = s^k(y)$.

Pour l'action de $\mathbb{Z}/p\mathbb{Z}$ sur $\mathcal{P}(E)$, $\{\emptyset\} = \mathcal{P}_0(E)$ est une orbite ponctuelle. Soit $\{A\}$ une autre orbite ponctuelle et soit $a \in A \neq \emptyset$. Alors $A = s^k(A)$ contient $s^k(a) = \overline{k}\cdot a$ pour $0 \leqslant k \leqslant p-1$ et contient donc tout E. Ainsi, $\{\emptyset\} = \mathcal{P}_0(E)$ et $\{E\} = \mathcal{P}_p(E)$ sont les seules orbites ponctuelles pour l'action sur $\mathcal{P}(E)$. Soient $O_1,\dots,O_\alpha$ les autres orbites (non ponctuelles) dans $\mathcal{P}(E)$. L'équation des classes donne :

$$\text{card}\,(\mathcal{P}(E)) = 2^p = 1 + 1 + \textstyle\sum_{i=1}^{\alpha} p = 2 + \alpha p \quad \text{d'où} \quad M_p = 2^p - 1 = \alpha p + 1\,.$$

Le nombre d'orbites, soit $2+\alpha$, est $\frac{1}{[\,\mathbb{Z}/p\mathbb{Z} : 1\,]} \sum \text{card}\left(\text{fix}(\overline{k})\right)$ (formule de Burnside). Pour $\overline{k} = \overline{0}$, toute partie de E est fixe par $s^0 = \text{Id}$ donc $\text{card}\left(\text{fix}(\overline{0})\right) = 2^p$. Comme nous l'avons dit, pour $1 \leqslant k \leqslant p-1$, les seuls éléments de $\mathcal{P}(E)$ fixes par $\overline{k}$ (qui engendre $\mathbb{Z}/p\mathbb{Z}$) sont $\emptyset$ et E donc $\text{card}\left(\text{fix}(\overline{k})\right) = 2$. On retrouve l'expression précédente des nombres de Mersenne $M_p = 2^p - 1$:

$$\alpha + 2 = \tfrac{1}{p}\,[2^p + (p-1)2] \qquad \text{d'où} \qquad 2^p - 1 = \alpha p + 1\,.$$

Ex 2 - 3

Soient $\Sigma = \{A_0, \ldots, A_{13}\}$ l'ensemble des sommets d'un polygone régulier P à 14 côtés et X l'ensemble des partitions du type $(4,6,4)$, de Σ. Le groupe symétrique $\mathcal{S}_{14}$ agit naturellement sur X. D'après Ex. 2-1, $\text{card}\,(X) = \frac{14!}{4!\,6!\,4!} = 210210$. A l'aide de la formule de Burnside, calculons le nombre d'orbites de l'action du groupe diédral $D_{14} \subset \mathcal{S}_{14}$ sur X. Notons r la rotation de centre O (centre de P), d'angle $\frac{2\pi}{14}$. Pour $k \in \{1, \ldots, 13\}$, l'ordre de r^k est $o(r^k) = \frac{14}{14 \wedge k}$ (voir 3-1). Pour $k = 7$, l'ordre de r^k est 2. C'est la symétrie par rapport à O, Pour avoir un collier invariant par r^k, il suffit de placer arbitrairement 2 perles rouges, 3 blanches, 2 jaunes, en $A_0, \ldots, A_6$ et de compléter le collier par symétrie par rapport à O. On a $\frac{7!}{2!\,3!\,2!} = 210$ possibilités. Pour les autres valeurs de k, on a $o(r^k) = 7$ ou 14. Aucune partition (4, 6, 4) n'est invariant par r^k car les parties de Σ invariantes par r^k ont un cardinal multiple de 7.

Pour chacune des sept symétries s de P par rapport à une médiatrice d'un côté, on a $\text{card}\,(\text{fix}(s)) = \frac{7!}{2!\,3!\,2!} = 210$ (comme pour la symétrie par rapport à O).

Considérons le cas d'une des sept symétries par rapport à une diagonale, par exemple la symétrie par rapport à $[A_0A_7]$. Les perles placées en A_0 et A_7 doivent avoir la même couleur, sinon il est impossible de placer les perles restantes, (en nombre impair pour certaines couleurs), par couples symétriques. Si on place en A_0 et A_7 deux perles rouges (ou jaunes), il reste $\frac{6!}{1!\,3!\,2!} = 60$ possibilités pour placer les 12 perles restantes par couples symétriques. Si on place en A_0 et A_7 deux perles blanches, on a $\frac{6!}{2!\,2!\,2!} = 90$ possibilités. En appliquant la formule de Burnside, on voit que l'on peut confectionner,

$$\tfrac{1}{28}\,[210210 + 8 \times 210 + 2 \times 60 + 90] \;=\; 7575 \qquad \text{colliers différents.}$$

Ex 2 - 4

a) Posons $X = G/H$. Soient $g \in G$, $x \in X$ et $a, a' \in G$ deux représentants de la classe à gauche x. On a $aH = a'H = x$ ou encore $a^{-1}a' \in H$. Or,
$(ga)^{-1}ga' = a^{-1}g^{-1}ga' = a^{-1}a' \in H$ donc $gaH = ga'H$.
Si on remplace a par un autre représentant a' de la classe $x = aH$, alors $ga'H = gaH$.
La formule a bien un sens et définit une application de $G \times X$ dans X. C'est une action de G sur X :
$\forall\, x = aH \in X \quad e{\cdot}x = eaH = aH = x$,
$\forall\, x = aH \in X \quad \forall\, g \in G \quad \forall\, g' \in G$

$$g{\cdot}(g'{\cdot}x) \;=\; g{\cdot}(g'aH) \;=\; g(g'a)H \;=\; (gg')aH = gg'{\cdot}x\,.$$

b) Quels que soient $x = aH \in X$, $y = bH \in X$, il existe $g \in G$ tel que $g{\cdot}x = y$ (prendre $g = ba^{-1}$). Il existe donc une seule orbite, égale à X.

Le stabilisateur de $x = aH$ est aHa^{-1} car :

$$g \in G_x \;\Leftrightarrow\; gaH = aH \;\Leftrightarrow\; a^{-1}gaH = H \;\Leftrightarrow\; a^{-1}ga \in H \;\Leftrightarrow\; g \in aHa^{-1}\,.$$

c) Puisqu'on a $G_x = aHa^{-1} = \text{Ad}_a(H) \simeq H$, on retrouve le th. de Lagrange :

$$[G\,:\,H] \;=\; \text{card}\,(G/H) \;=\; \text{card}\,(\text{orb}(x)) \;=\; \tfrac{[G:1]}{[G_x:1]} \;=\; \tfrac{[G:1]}{[H:1]}.$$

Ex 2 - 5

a) Le groupe H agit sur G par les translations à gauche $l_h : g \mapsto hg$ et K agit sur G par les translations à droite $r_k : g \mapsto gk^{-1}$. On a $l_h \circ r_k = r_k \circ l_h$ pour tout $h \in H$ et tout $k \in K$ donc $\varphi : (h,k) \mapsto l_h \circ r_k$ est un homomorphisme de groupes de $\Gamma = H \times K$ dans le groupe $\mathcal{S}_G$ des bijections de G sur G (voir Ex. 1-12). Pour cette action, l'orbite de $g \in G$ est $\{hgk^{-1}\,;\ \ h \in H\,,\, k \in K\} = HgK$. Ces parties constituent donc une partition de G.

b) Le stabilisateur de $g \in G$ est le sous-groupe Γ_g de $\Gamma = H \times K$, ensemble des $(h,k) \in \Gamma$ tels que $hgk^{-1} = g$ c'est-à-dire tels que $hg = gk$.

c) $HK = HeK$ est l'orbite de e. Donc $HK = G$ si et seulement si l'action est transitive. Dans ce cas, les stabilisateurs Γ_g des éléments $g \in G$ sont conjugués dans $H \times K$ et ont donc le même cardinal. Calculons-le. On a :

$$[G\,:\,1] = \text{card}\,(\text{orb}(g)) = \tfrac{[H\times K:1]}{[\Gamma_g:1]} \qquad \text{d'où} \qquad [\Gamma_g\,:\,1] = \tfrac{[H:1][K:1]}{[G:1]}.$$

Si $g = e$, on a $\Gamma_e \simeq H \cap K$ car

$\Gamma_e = \{(h,k) \in \Gamma \mid hek^{-1} = e\} = \{(h,k) \in \Gamma \mid h = k\} = \{(h,h)\,;\ \ h \in H \cap K\}$.

La relation précédente donne $[G\,:\,1][H \cap K\,:\,1] = [H\,:\,1][K\,:\,1]$.

Si $H \lhd G$ ou plus généralement si K est contenu dans le normalisateur de H, le th. de Noether montre que $G/H \simeq K/(K \cap H)$ et on retrouve que $\frac{[G:1]}{[H:1]} = \frac{[K:1]}{[H\cap K:1]}$.

Ex 2 - 6

Faisons agir G par automorphismes intérieurs sur lui-même, puis sur l'ensemble de ses sous-groupes. Le stabilisateur de H est ici son normalisateur N_H. On a $H \subset N_H$ et donc $[G\,:\,H] = [G\,:\,N_H][N_H\,:\,H]$. Ainsi, $k = [G\,:\,N_H] = \frac{[G:1]}{[N_H:1]}$ est fini. L'orbite de H est donc finie et possède $k = [G\,:\,N_H]$ éléments $g_1Hg_1^{-1}, \ldots, g_kHg_k^{-1}$. D'après le th. de Poincaré, le sous-groupe $\bigcap\limits_{g\in G} gHg^{-1} = \bigcap\limits_{i=1}^{n} g_iHg_i^{-1}$ est d'indice fini. Ce sous-groupe est évidemment distingué dans G.

Ex 2 - 7

a) $\forall\, A \in E \quad (I_m, I_n)\cdot A = I_mAI_n = A$.
$\forall\, (P,Q) \in G \quad \forall\, (P',Q') \in G \quad \forall\, A \in E$
$(P,Q)\cdot[(P',Q')\cdot A] = (P,Q)\cdot(P'AQ'^{-1}) = P(P'AQ'^{-1})Q^{-1}$
$= (PP')A(QQ')^{-1} = (PP', QQ')\cdot A = [(P,Q)(P',Q')]\cdot A$.

On a bien une action de G sur E. De plus, tout $(P,Q) \in G$ agit sur $E = \mathcal{M}_{m,n}(K)$ par un isomorphisme $\varphi_{P,Q} : A \mapsto PAQ^{-1}$ de l'espace vectoriel E.

b) La relation d'équivalence de conjugaison :

$$A \sim A' \quad \Leftrightarrow \quad \exists\, (P,Q) \in \text{GL}(m,K)\times\text{GL}(n,K) \qquad A' = PAQ^{-1}\,,$$

est la notion classique de matrices équivalentes. Rappelons que si $u \in \mathcal{L}(E_1,E_2)$ a pour matrice A dans les bases $\mathcal{B}_1$ et $\mathcal{B}_2$ de E_1 et E_2, alors dans d'autres bases $\mathcal{B}'_1$

et $\mathcal{B}'_2$ la matrice de u est $A' = PAQ^{-1}$, où P est la matrice de passage de $\mathcal{B}_2$ à $\mathcal{B}'_2$ et Q la matrice de passage de $\mathcal{B}_1$ à $\mathcal{B}'_1$. Toutes les matrices équivalentes à A s'obtiennent ainsi et ont le même rang, qui est le rang de u.

La méthode du pivot de Gauss montre qu'en multipliant à gauche A par des matrices élémentaires (voir Ex. 1-6), on arrive à une matrice échelonnée

$$A' = \begin{pmatrix} 1 & \cdots & \alpha_{1r} & \alpha_{1,r+1} & \cdots & \alpha_{1n} \\ \cdot & \cdots & \cdot & \cdot & \cdots & \cdot \\ 0 & \cdots & 1 & \alpha_{r,r+1} & \cdots & \alpha_{rn} \\ 0 & \cdots & 0 & 0 & \cdots & 0 \\ \cdot & \cdots & \cdot & \cdot & \cdots & \cdot \\ 0 & \cdots & 0 & 0 & \cdots & 0 \end{pmatrix}$$

Des multiplications à droite par des matrices élémentaires (ce qui revient à effectuer sur ${}^tA'$ des opérations du type précédent) amènent à $I_{m,n,r} = \begin{pmatrix} I_r & 0 \\ 0 & 0 \end{pmatrix} \in \mathcal{M}_{m,n}(K)$. Ainsi A est équivalente à $I_{m,n,r}$, où r est le rang de A. Toutes les matrices de l'orbite $\{PAQ^{-1}\,;\ (P,Q) \in G\}$ de A ont le même rang qui est r rang de $I_{m,n,r}$. Réciproquement, toute matrice $A' \in E$ de rang r est équivalente à $I_{m,n,r}$ d'après ce que nous venons de voir et donc équivalente à A. L'orbite de A est exactement l'ensemble des matrices de rang r. Les orbites sont donc en bijection avec les entiers r tels que $0 \leqslant r \leqslant \min(m,n)$. On a donc $1 + \min(m,n)$ orbites.

Ex 2 - 8

a) S'il existe $B \in \mathcal{M}_n(\mathbb{Z})$ telle que $AB = I_n$, alors $\det(A)\det(B) = 1$ avec $\det(A) = \sum_{s \in S_n} \varepsilon(\sigma) a_{\sigma(1),1} \cdots a_{\sigma(n),n} \in \mathbb{Z}$ et $\det(B) \in \mathbb{Z}$. On a donc $\det(A) \in \{1,-1\}$.

Réciproquement, si $\det(A) \in \{1,-1\}$, la matrice A est inversible dans $\mathrm{GL}(n,\mathbb{R})$ et a pour inverse $A^{-1} = \frac{1}{\det(A)}\,{}^tC$ où C est la comatrice de A. Les coefficients $(-1)^{i+j}\Delta_{i,j}$ de C, où $\Delta_{i,j}$ est le déterminant mineur de a_{ij}, appartiennent à $\mathbb{Z}$. On a donc $A^{-1} \in \mathcal{M}_n(\mathbb{Z})$. Ainsi $A \in \mathrm{GL}(n,\mathbb{Z})$.

L'application $f : A \mapsto \det(A)$, de $\mathrm{GL}(n,\mathbb{Z})$ dans $\{1,-1\}$, est un homomorphisme de groupes car $\det(AB) = \det(A)\det(B)$. Son noyau $\mathrm{SL}(n,\mathbb{Z})$ est un sous-groupe distingué puisque f est surjectif. Ce sous-groupe est d'indice deux. En effet, en factorisant f on obtient un isomorphisme de $\mathrm{GL}(n,\mathbb{Z})/\mathrm{SL}(n,\mathbb{Z})$ sur $\{1,-1\}$.

b) (i) Soient $i \neq j$. Pour tout $k \in \mathbb{Z}$ la matrice $T_{ij}(k) = I_n + kE_{ij}$ est triangulaire, de termes diagonaux égaux à 1, et donc élément de $\mathrm{SL}(n,\mathbb{Z})$.
On sait que $E_{ij}E_{kl} = \delta_{jk}E_{il}$. On en déduit que φ est un homomorphisme car pour tous $k,k' \in \mathbb{Z}$ on a :

$$T_{ij}(k)T_{ij}(k') = (I_n + kE_{ij})(I_n + k'E_{ij}) = I_n + (k+k')E_{ij}$$

On en déduit que $(T_{ij})^k = \varphi(1)^k = \varphi(k) = T_{ij}(k)$ et que
$T_{ij}(k)^{-1} = \varphi(k)^{-1} = \varphi(-k) = T_{ij}(-k)$. De plus, φ est injectif car $k \in \mathrm{Ker}(\varphi)$ si et seulement si $T_{ij}(k) = I_n$, c'est-à-dire si $k = 0$.

(ii) $S_{ij} = T_{ij}T_{ji}^{-1}T_{ij} = (I_n + E_{ij})(I_n - E_{ji})(I_n + E_{ij}) = I_n - E_{ii} - E_{jj} + E_{ij} - E_{ji}$,

Cette matrice $S_{ij} = (s_{kl})$ a une diagonale principale faite de 1, sauf $s_{ii} = s_{jj} = 0$. En dehors de cette diagonale, tous les coefficients sont nuls sauf $s_{ij} = 1$ et $s_{ji} = -1$.

Par exemple, si $n = 2$, $S_{21} = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$.

On a $(S_{ij})^2$ diagonale, de diagonale $(1, \ldots, 1, -1, 1, \ldots, 1, -1, 1, \ldots, 1)$, avec -1 en $i^{\text{ième}}$ et $j^{\text{ième}}$ places.

c) Comme dans l'exercice précédent, on vérifie que l'on définit une action. Notons $A \sim B$ la relation de conjugaison associée.

d) (i) Si $a_{11} \neq 0$, quitte à remplacer A par $(S_{21})^2 A$ on aura $a_{11} > 0$.
Si $a_{11} = 0$, puisque $A \neq 0$, il existe un coefficient a_{ij} de A non nul. On peut permuter les lignes L_1 et L_i, avec changement des signes pour L_i, en multipliant à gauche A par S_{1i}, et permuter ensuite les colonnes C_1 et C_j, avec changement des signes pour C_1, en multipliant à droite A par S_{1j}. On obtient $A' = S_{1i} A S_{1j} \sim A$ avec $a'_{11} \neq 0$. On est ramené au cas précédent. Donc $\mathcal{E} \neq \emptyset$.

(ii) D'après (i), d et B existent. Supposons qu'il existe $i \neq 1$ tel que $b_{i1} \neq 0$. La division par d donne $b_{i1} = dq + r$ avec $0 \leqslant r < d$. Si on avait $r \neq 0$, alors $[T_{i1}(-q)]B = B'$ serait telle que $b'_{i1} = r$ et pour $S_{1i} B' = B''$ on aurait $b''_{11} = -r$. Alors $B''' = (S_{1i})^2 B'' \sim A$ serait telle que $b'''_{11} = r$ avec $0 < r < d$, ce qui contredirait la minimalité de d. Donc $r = 0$ et d divise b_{i1} pour $2 \leqslant i \leqslant n$.

(iii) D'après (ii), pour tout $i \geqslant 2$ il existe k tel que $b_{i1} = kd$. Alors $B' = [T_{i1}(-k)]B \sim B$ est telle que $b'_{11} = d$ et $b'_{i1} = 0$, d'où l'existence d'une matrice conjuguée de A, telle que $b_{i1} = 0$ pour $2 \leqslant i \leqslant n$. Ensuite, en multipliant à droite par des matrices $T_{1i}(-k)$ convenables, on obtient C de la forme voulue.

(iv) Appliquons (ii) à $CT_{21} \sim C$, dont la première colonne est somme des deux premières colonnes de C. On voit que d divise $c_{22}, \ldots, c_{n2}$. De même pour les autres colonnes de C en considérant CT_{j1} pour $j \geqslant 2$.

(v) Raisonnons par récurrence. Pour $n = 1$ l'assertion est évidente. Admettons le résultat pour toute matrice de $\mathcal{M}_{n-1}(\mathbb{Z})$. Soit $A \in \mathcal{M}_n(\mathbb{Z})$.
D'après (iii), $A \sim C = \begin{pmatrix} d_1 & 0 \\ 0 & C' \end{pmatrix}$ avec $C' \in \mathcal{M}_{n-1}(\mathbb{Z})$. D'après l'hypothèse de récurrence, il existe $P' \in G$, $Q' \in G$ telles que $P'C'Q'^{-1}$ soit diagonale, de diagonale principale $(d_2, d_3, \ldots)$ où $d_2 \mid d_3 \ldots$ Alors $P = \begin{pmatrix} 1 & 0 \\ 0 & P' \end{pmatrix}$, $Q = \begin{pmatrix} 1 & 0 \\ 0 & Q' \end{pmatrix}$ sont des éléments de G tels que PCQ^{-1} soit diagonale, de diagonale $(d_1, d_2, d_3, \ldots)$. D'après (iv), d_1 divise tous ses coefficients et en particulier d_2.

e) Si $A \in \mathrm{SL}(n, \mathbb{Z})$, on a $n = \mathrm{rang}(D) = r$ car des matrices équivalentes au sens usuel ont le même rang (voir exercice précédent). De plus, $1 = \det(A) = d_1 \cdots d_n$. Comme $d_i \in \mathbb{N}$ pour $i = 1, \ldots, n$, nécessairement $1 = d_1 = \cdots = d_n$. Il existe donc $P \in G$ et $Q \in G$ tels que $PAQ^{-1} = I_n$, d'où $A = P^{-1}Q \in G$. Ainsi, le sous-groupe G de $\mathrm{SL}(n, \mathbb{Z})$ engendré par les matrices T_{ij} est égal à $\mathrm{SL}(n, \mathbb{Z})$.

f) Soit $A \in \mathrm{GL}(n, \mathbb{Z})$. D'après a), $\det(A) \in \{1, -1\}$. Si $\det(A) = 1$, d'après (f), $A \in G$ est de la forme $T_1 \cdots T_s$ souhaitée. Si $\det(A) = -1$, alors $AD_{-1} \in \mathrm{SL}(n, \mathbb{Z})$ est de la forme $T_1 \cdots T_s$ et $A = T_1 \cdots T_s D_{-1}$.

g) (i) D'après f), le sous-groupe $G' = \langle T, T' \rangle$ de $\mathrm{GL}(2, \mathbb{Z})$ est égal à $\mathrm{SL}(2, \mathbb{Z})$. Comme $S_{12} = T_{12} T_{21}^{-1} T_{12}$, on a $TT'^{-1}T = S$ et donc $T' = T^{-1} S T^{-1}$. Ainsi, $\langle T, S \rangle$ contient T et T' qui engendrent $\mathrm{SL}(2, \mathbb{Z})$ donc $\langle T, S \rangle = \mathrm{SL}(2, \mathbb{Z})$.

(ii) Voir Ex. 1-6, d).

Ex 2 - 9

Puisque $\det(D_\lambda) = \lambda \neq 0$ on a $D_\lambda \in \mathrm{GL}(n,K)$. On a $D_\lambda D_{\lambda'} = D_{\lambda\lambda'}$ pour tous $\lambda, \lambda' \in \mathbb{R}$ donc $f : \lambda \mapsto D_\lambda$ est un homomorphisme de groupes. Son image D est un sous-groupe de $\mathrm{GL}(n,K)$. Si $\det(D_\lambda) = 1$ alors $D_\lambda = I_n$ donc $\mathrm{SL}(n,K) \cap D = \{I_n\}$. Soit $A \in \mathrm{GL}(n,K)$. Posons $\lambda = \det(A)$. On a $B = AD_\lambda^{-1} \in \mathrm{SL}(n,K)$ et $A = BD_\lambda$. Ainsi $\mathrm{GL}(n,K) = [\mathrm{SL}(n,K)]\, D$. Comme $\mathrm{SL}(n,K)$ est le noyau de l'homomorphisme $A \mapsto \det(A)$, il est distingué dans $\mathrm{GL}(n,K)$. On peut appliquer 2-7, prop.

Notons que nous avions déjà vu (Ex. 1-6) que tout $A \in \mathrm{GL}(n,K)$ est produit $A = TD_\lambda$, de manière unique, d'un élément T de $\mathrm{SL}(n,K)$ produit de matrices de transvection et d'une matrice de dilatation D_λ.

Ex 2 - 10

Notons j l'homomorphisme canonique de G sur G/H. Soit $a \in G$ tel que $\overline{a}$ engendre G/H. Alors $K = \langle a \rangle$ est monogène et infini puisque $j(K) = \langle \overline{a} \rangle = G/H$ est infini. Donc $f : k \mapsto a^k$ est un isomorphisme de $\mathbb{Z}$ sur K (1-14, prop.). De même $g : k \mapsto \overline{a}^k$ est un isomorphisme de $\mathbb{Z}$ sur $\langle \overline{a} \rangle$. On voit ainsi que $h = f \circ g^{-1}$ est un isomorphisme de G/H sur K, tel que $j \circ h = \mathrm{Id}_{G/H}$. On a donc $G \simeq H \times_\varphi \mathbb{Z}$ où $\varphi : k \mapsto \mathrm{Ad}_k \mid_K$ (voir 2-7, ex. 1). Plus brièvement, on peut dire que pour tout $g \in G$, il existe $k \in \mathbb{Z}$ unique tel que $\overline{g} = \overline{a}^{\,k}$. On a de manière unique $g = ha^k$ avec $h \in H$. L'assertion en résulte.

Ex 2 - 11

Nous sautons les vérifications du fait que $\psi_k = (\varphi_k, \mathrm{Id}_{H'}) : (h,h') \mapsto (\varphi_k(h),h')$ est pour tout $k \in K$ un automorphisme de $H \times H'$ et que $k \mapsto \psi_k$ est un homomorphisme de groupes de K dans $\mathrm{Aut}\,(H \times H')$, c'est-à-dire une action.

L'application $\theta : ((h,k),h') \mapsto ((h,h'),k)$ est bijective de $(H \times_\varphi K) \times H'$ sur $(H \times H') \times_\psi K$. Vérifions que c'est un homomorphisme.
Considérons $h_1 \in H$, $h_2 \in H$, $h_1' \in H'$, $h_2' \in H'$, $k_1 \in K$, $k_2 \in K$. On a

$$\begin{aligned}\theta[((h_1,k_1)\,,h_1')((h_2,k_2)\,,h_2')] &= \theta[((h_1,k_1)(h_2,k_2)\,,h_1'h_2')] \\ &= \theta[((h_1\varphi_{k_1}(h_2),k_1k_2)\,,h_1'h_2')] = ((h_1\varphi_{k_1}(h_2),h_1'h_2')\,,k_1k_2)]\,,\end{aligned}$$

$$\begin{aligned}\theta((h_1,k_1)\,,h_1')\theta((h_2,k_2),h_2') &= ((h_1,h_1')\,,k_1)((h_2,h_2')\,,k_2) \\ &= ((h_1,h_1')\psi_{k_1}(h_2,h_2')\,,k_1k_2) = ((h_1,h_1')(\varphi_{k_1}(h_2),h_2')\,,k_1k_2) \\ &= ((h_1\varphi_{k_1}(h_2),h_1'h_2')\,,k_1k_2)\,,\end{aligned}$$

d'où le résultat.

Ex 2 - 12

L'ordre de $\mathrm{Im}\,(\alpha) \simeq K/\mathrm{Ker}\,(\alpha)$ divise $p = [K : 1] = [K : \mathrm{Ker}\,(\alpha)][\mathrm{Ker}\,(\alpha) : 1]$ (th. de Lagrange) et $[\mathrm{Aut}\,(H) : 1] = q - 1$ (1-9, cor. 1). Puisque p et $q-1$ sont premiers entre eux, $[\mathrm{Im}\,(\alpha) : 1] = 1$. On a $\mathrm{Im}\,(\alpha) = \{\mathrm{Id}_H\}$ donc α est trivial et le produit semi-direct considéré est direct (2-7, cor.).

Chapitre 3

Groupes abéliens finis

3.1 Groupes cycliques, générateurs

Définition.

On dit qu'un groupe G est cyclique lorsqu'il est monogène et fini. Tout élément a de G tel que $\langle a \rangle = G$ est appelé un générateur de G.

Soient $m, n \in \mathbb{N}$. Nous noterons $m \wedge n$ le pgcd de m et n. Nous écrirons $m \mid n$ pour exprimer que m divise n.

Pour $n \geqslant 2$, on note $\varphi(n)$ le cardinal de l'ensemble des entiers k tels que $0 \leqslant k \leqslant n-1$ et $k \wedge n = 1$. On convient que $\varphi(1) = 1$. La fonction φ de $\mathbb{N}^*$ dans $\mathbb{N}^*$ ainsi définie est appelée la fonction d'Euler.

Exemples. Le groupe additif $\mathbb{Z}/n\mathbb{Z} = \{\overline{0}, \overline{1}, \ldots, \overline{n-1}\}$ est engendré par $\overline{1}$ car :

$$\overline{1}+\overline{1} = \overline{2} \quad , \ldots , \quad (n-1) \times \overline{1} = \overline{n-1} \quad , \quad n \times \overline{1} = \overline{n} = \overline{0}.$$

C'est donc un groupe cyclique d'ordre n.

Le groupe multiplicatif $\mathbb{U}_n = \{1, \zeta, \zeta^2, \cdots, \zeta^{n-1}\}$ des racines $n^{\text{ièmes}}$ de l'unité dans $\mathbb{C}$, est engendré par $\zeta = \exp\left(\frac{2i\pi}{n}\right)$. Il est cyclique d'ordre n.

Les générateurs du groupe $\mathbb{U}_n$, sont appelés les racines $n^{\text{ièmes}}$ *primitives* de l'unité.

Exercice 1. Montrer que $\varphi(p) = p-1$ si et seulement si p est premier.

Solution. Supposons p premier. Les entiers qui ne sont pas premiers avec p sont les multiples de p. Il existe donc $p-1$ éléments dans $[0, p-1]$ qui sont premiers avec p, qui sont $1, \ldots, p-1$. Réciproquement, si $\varphi(p) = p-1$, comme 0 n'est pas premier avec p, nécessairement les $p-1$ autres éléments $1, \ldots, p-1$ sont premiers avec p. Ils ne divisent donc pas p. Cela signifie que p est premier (principe du crible d'Eratosthène, voir ch. 12).

Proposition.

Soient G un groupe cyclique d'ordre n et a un générateur de G. Pour tout $k \in \mathbb{Z}$, l'ordre de $a^k \in G$ est $o(a^k) = \dfrac{n}{n \wedge k}$.

En particulier, a^k est un générateur de G si et seulement si $n \wedge k = 1$.

Il existe $\varphi(n)$ générateurs distincts dans G.

Démonstration. Soit $k \in \mathbb{Z}$. Posons $d = n \wedge k \in \mathbb{N}^*$. On a $n = dn'$, $k = dk'$ avec $n' \wedge k' = 1$. Pour tout $m \in \mathbb{N}$ on a

$$(a^k)^m = e \quad \Leftrightarrow \quad a^{km} = e \quad \Leftrightarrow \quad n \,|\, km \quad \Leftrightarrow \quad n' \,|\, k'm \quad \Leftrightarrow \quad n' \,|\, m\,.$$

Ainsi n' est le plus petit entier non nul tel que $(a^k)^{n'} = e$. On a donc $n' = o(a^k)$. ∎

Exercice 2. Déterminer les générateurs du groupe additif $\mathbb{Z}/12\mathbb{Z}$ et ceux du groupe multiplicatif $\mathbb{U}_{18}$.

Solution. Pour que $k\overline{1} = \overline{k}$ soit gérérateur de $\mathbb{Z}/12\mathbb{Z}$, il faut et il suffit que $k \wedge 12 = 1$, d'où les générateurs $\overline{1}, \overline{5}, \overline{7}, \overline{11}$ de ce groupe (on a donc $\varphi(12) = 4$).

Puisque $\zeta = \exp(\frac{2i\pi}{18})$ engendre $\mathbb{U}_{18}$, l'ensemble des générateurs de $\mathbb{U}_{18}$ est

$$\{\, \zeta^k ;\ \ 0 \leqslant k \leqslant 17\,,\ k \wedge 18 = 1 \,\} \ = \ \{\, \zeta^1\,, \zeta^5\,, \zeta^7\,, \zeta^{11}\,, \zeta^{13}\,, \zeta^{17} \,\}\,.$$

Exercice 3. Combien existe-t-il d'éléments d'ordre 2 dans $\mathbb{Z}/n\mathbb{Z}$, où $n \geqslant 2$?

Solution. Soit $\overline{k} \in \mathbb{Z}/n\mathbb{Z}$. On a $o(\overline{k}) = \frac{n}{n \wedge k}$. Si $o(\overline{k}) = 2$, alors nécessairement $n = 2(n \wedge k)$ est pair. (C'est aussi une conséquence du th. de Lagrange.)

Réciproquement, supposons que $n = 2q$ avec $q \in \mathbb{N}^*$. Alors, pour $0 \leqslant k \leqslant n-1$,

$$\begin{array}{lllll} o(\overline{k}) = 2 & \Leftrightarrow & \frac{2q}{(2q) \wedge k} = 2 & \Leftrightarrow & q = (2q) \wedge k \\ & \Rightarrow & q \,|\, k & \Leftrightarrow & k = q \quad \text{ou} \quad k = 0\,. \end{array}$$

Pour $k = 0$ on a $\overline{k} = \overline{0}$ et $o(\overline{k}) = 1$. Pour $k = q$ on a $o(\overline{k}) = \frac{2q}{(2q) \wedge q} = 2$.

Ainsi, $\overline{q}$ est le seul élément d'ordre 2 de $\mathbb{Z}/n\mathbb{Z}$ (voir aussi 3-3).

3.2 Homomorphismes entre groupes cycliques

Lemme.

Soient G un groupe cyclique d'ordre n et a un générateur de G. L'homomorphisme $k \mapsto a^k$ de $\mathbb{Z}$ sur G se factorise et définit un isomorphisme $\alpha_a : \overline{k} \mapsto a^k$, où $0 \leqslant k < n$, du groupe $\mathbb{Z}/n\mathbb{Z}$ sur G.

Démonstration. L'homomorphisme $f : k \mapsto a^k$ de $\mathbb{Z}$ dans G est surjectif car $\langle a \rangle = G$. Son noyau est $n\mathbb{Z}$ où n est l'ordre $o(a) = [\langle a \rangle : 1]$ de a (voir 1-14). Par factorisation, on en déduit un isomorphisme $\overline{f} : \overline{k} \mapsto a^k$ de $\mathbb{Z}/n\mathbb{Z}$ sur G (1-9, cor. 1). ∎

Proposition.

Soient G un groupe cyclique d'ordre n et a un générateur de G.

(i) *Soit f un homomorphisme surjectif de G sur un groupe G'. Alors G' est cyclique, $a' = f(a)$ engendre G' et $[G' : 1]$ divise n. En particulier, tout groupe quotient de G est cyclique.*

(ii) *Soit G' un groupe cyclique dont l'ordre n' divise l'ordre de G. Soit $a' \in G'$. Il existe un unique homomorphisme f de G dans G' tel que $f(a) = a'$. Pour que f soit surjectif, il faut et il suffit que a' soit un générateur de G'.*

Démonstration. (i) Puisque f est surjectif, pour tout $y \in G'$ il existe $x \in G$ tel que $f(x) = y$, puis $k \in [0, n-1]$ tel que $x = a^k$. On a $y = f(a^k) = f(a)^k$ donc $f(a)$ engendre G'. De plus, $[G' : 1]$ divise $[G : 1] = n$ car G' est isomorphe à $G/\mathrm{Ker}\,(f)$.

(ii) D'après le th. de Lagrange, $m = o(a')$ divise n' et n' divise l'ordre n de G. On a donc $n\mathbb{Z} \subset m\mathbb{Z}$. L'homomorphisme canonique $k \mapsto a'^k$ de $\mathbb{Z}$ sur $\langle a' \rangle$ a pour noyau $m\mathbb{Z}$. Il se factorise à travers $n\mathbb{Z}$ et définit un homomorphisme β de $\mathbb{Z}/n\mathbb{Z}$ sur $\langle a' \rangle$ tel que $\beta(\bar{k}) = a'^k$ pour tout $\bar{k} \in \mathbb{Z}/n\mathbb{Z}$. Soit α_a l'isomorphisme de $\mathbb{Z}/n\mathbb{Z}$ sur G donné par le lemme. Alors $f = \beta \circ \alpha_a^{-1} \in \mathrm{Hom}\,(G, G')$ est tel que $f(a) = \beta(\alpha_a^{-1}(a)) = \beta(\bar{1}) = a'$. Il est unique car la donnée de $f(a) = a'$ détermine $f(a^k) = a'^k$ pour tout $k \in \mathbb{Z}$. Pour que f soit surjectif, il faut et il suffit que a' engendre G' car $\mathrm{Im}\,(f) = \mathrm{Im}\,(\beta) = \langle a' \rangle$. ∎

Corollaire 1.

Deux groupes cycliques G et G' sont isomorphes si et seulement s'ils ont le même ordre. Supposons cette condition vérifiée. Soit a un générateur de G. Alors $\theta : \alpha \mapsto \alpha(a)$ est une bijection de $\mathrm{Isom}(G, G')$ *sur l'ensemble E des générateurs de G'.*

Démonstration. Si G et G' sont isomorphes, ils ont même cardinal. Réciproquement, si $[G : 1] = [G' : 1] = n$, le lemme montre que G et G' sont isomorphes à $\mathbb{Z}/n\mathbb{Z}$.

L'assertion (i) de la proposition montre que θ prend ses valeurs dans E. D'après (ii), si a' est un générateur de G', il existe un homomorphisme surjectif f de G dans G' tel que $f(a) = a'$. Comme G et G' ont le même cardinal, f est bijectif. C'est un isomorphisme. Ainsi θ est surjective. La donnée de $\alpha(a) = a'$ détermine α donc θ est injective. ∎

Corollaire 2.

Soit G un groupe cyclique d'ordre n. Le groupe $Aut\,(G)$ est d'ordre $\varphi(n)$ et ses éléments sont les applications $\alpha_k : x \mapsto x^k$ où $k \in [0, n-1]$ est premier avec n.

Démonstration. Soit a un générateur de G. D'après le cor. 1, les automorphismes de G sont déterminés par le choix d'un générateur a' de G, c'est-à-dire par le choix de a^k où $k \in \Delta = \{k \in [0, n-1] \mid k \wedge n = 1\}$. On a donc $\varphi(n)$ automorphismes. L'automorphisme α_k associé au choix de $k \in \Delta$ applique tout $x = a^m \in G$ sur $\alpha_k(x) = \alpha_k(a^m) = \alpha_k(a)^m = (a^k)^m = (a^m)^k = x^k$. ∎

Remarque. En notation additive, par exemple dans $\mathbb{Z}/n\mathbb{Z}$, les automorphismes ont pour expression $\bar{x} \mapsto k\bar{x}$ où $k \in \Delta$ et on a $k\bar{x} = \bar{x} + \cdots + \bar{x} = \overline{x + \cdots + x} = \overline{kx}$.

Nous verrons en III que $\mathbb{Z}/n\mathbb{Z}$ est non seulement un groupe additif mais un anneau, dont le produit est défini par $\bar{k}\bar{p} = \overline{kp}$. Le groupe $(\mathbb{Z}/n\mathbb{Z})_*$ des éléments inversibles de cet anneau commutatif est justement l'ensemble des $\bar{k} \in \mathbb{Z}/n\mathbb{Z}$ où $k \in \Delta$.

Cela montre que les automorphismes du groupe additif $\mathbb{Z}/n\mathbb{Z}$ sont les multiplications $\alpha_k : \bar{x} \mapsto \bar{k}\bar{x}$ par les éléments $\bar{k}$ inversibles dans l'anneau $\mathbb{Z}/n\mathbb{Z}$. L'automorphisme réciproque est la multiplication $\bar{x} \mapsto \bar{k}^{-1}\bar{x}$ par l'inverse de $\bar{k}$ dans cet anneau. Ainsi $\bar{k} \mapsto \alpha_k$ est un isomorphisme du groupe $(\mathbb{Z}/n\mathbb{Z})_*$ des éléments inversibles de l'anneau $\mathbb{Z}/n\mathbb{Z}$ sur le groupe $\mathrm{Aut}\,(\mathbb{Z}/n\mathbb{Z})$ des automorphismes du groupe additif $\mathbb{Z}/n\mathbb{Z}$ (cela sera revu en 12-2, ex.).

Ces propriétés ont une conséquence intéressante. Si $p \in \mathbb{N}$ est premier, on verra que $\mathbb{Z}/p\mathbb{Z}$ est un corps et que le groupe $(\mathbb{Z}/p\mathbb{Z})_*$ des éléments inversibles de $\mathbb{Z}/p\mathbb{Z}$ est cyclique, d'ordre $p-1$. Donc pour p premier, le groupe $\mathrm{Aut}\,(\mathbb{Z}/p\mathbb{Z})$ des automorphismes du groupe additif $\mathbb{Z}/p\mathbb{Z}$ est cyclique, d'ordre $p-1$. Nous utiliserons ce résultat sans attendre de l'avoir démontré au ch. 10.

3.3 Sous-groupes d'un groupe cyclique

Proposition.

Soient G un groupe cyclique d'ordre n et a un générateur de G. Tout sous-groupe de G est cyclique et pour tout diviseur d de n, il existe un unique sous-groupe H_d de G d'ordre d. En posant $\delta = n/d$, ce sous-groupe est caractérisé par :

$$(1) \qquad H_d = \{x \in G \mid x^d = e\} = \{x \in G \mid \exists y \in G \quad y^\delta = x\} = < a^\delta > .$$

Démonstration. Comme G est abélien, $f_k : x \mapsto x^k$ est pour tout $k \in \mathbb{N}$ un endomorphisme de G. Soit d un diviseur de n et posons $\delta = n/d$. Pour tout $x \in G$ on a $(x^d)^\delta = (x^\delta)^d = x^n = e$ et donc $\mathrm{Im}\,(f_d) \subset \mathrm{Ker}\,(f_\delta)$ et $\mathrm{Im}\,(f_\delta) \subset \mathrm{Ker}\,(f_d)$. D'après 3-1, $o(a^\delta) = d$ et $o(a^d) = \delta$. Donc $\langle a^\delta \rangle$ est un sous-groupe d'ordre d de G et $\langle a^d \rangle$ un sous-groupe d'ordre δ. On a $\mathrm{Im}\,(f_d) = \{(a^k)^d \mid 0 \leqslant k \leqslant n-1\} = \{(a^d)^k \mid 0 \leqslant k \leqslant n-1\} = \langle a^d \rangle$. De même $\mathrm{Im}\,(f_\delta) = \langle a^\delta \rangle$. Ainsi $[\mathrm{Im}\,(f_d) : 1] = \delta$ et $[\mathrm{Im}\,(f_\delta) : 1] = d$. Comme $[\mathrm{Im}\,(f_d) : 1] = \frac{[G:1]}{[\mathrm{Ker}(f_d):1]}$, on voit que $[\mathrm{Ker}\,(f_d) : 1] = d$. De même $[\mathrm{Ker}\,(f_\delta) : 1] = \delta$. Les inclusions précédentes sont donc des égalités puisque les cardinaux des deux membres sont égaux. Nous avons ainsi prouvé que $\langle a^\delta \rangle = \mathrm{Ker}\,(f_d) = \mathrm{Im}\,(f_\delta)$. Ce sous-groupe de G, appelons-le H_d, est d'ordre d, il vérifie les relations (1) et il est cyclique.

Enfin H_d est le seul sous-groupe d'ordre d. En effet, si K est un sous-groupe d'ordre d, alors tout $x \in K$ est tel que $x^d = e$ d'après le th. de Lagrange. On a donc $K \subset H_d$ et donc $K = H_d$ puisque $[K : 1] = d = [H_d : 1]$. ∎

Corollaire.

Soit G un groupe cyclique. L'ensemble E des sous-groupes de G, ordonné par inclusion est isomorphe à l'ensemble D des diviseurs de $[G : 1]$ ordonné par la relation de divisibilité $d|d'$.

Démonstration. D'après la proposition, $d \mapsto H_d$ est bijective de D sur E. Si $d, d' \in D$ vérifient $d|d'$, alors on a $H_d = \{x \in G \mid x^d = e\} \subset H_{d'} = \{x \in G \mid x^{d'} = e\}$. Réciproquement, si $H_d \subset H_{d'}$, le th. de Lagrange donne $d = [H_d : 1] | d' = [H_{d'} : 1]$. ∎

Exercice 1. Déterminer les sous-groupes de $\mathbb{Z}/20\mathbb{Z}$.

Solution. Les sous-groupes H_d correspondent aux diviseurs d de $20 = 2^2 \times 5$, qui sont 1 , 2 , 2^2 , 5 , 2×5 , $2^2 \times 5$. On a donc six sous-groupes :
$H_1 = \{\overline{0}\}$, d'ordre 1 ,
H_2 d'ordre 2, image de $f_{10} : \overline{x} \mapsto 10\,\overline{x}$, soit $H_2 = \{\overline{0}, \overline{10}\} = \langle \overline{10} \rangle$.
H_4 d'ordre 4, image de $f_5 : \overline{x} \mapsto 5\,\overline{x}$, soit $H_4 = \{\overline{0}, \overline{5}, \overline{10}, \overline{15}\} = \langle \overline{5} \rangle$, etc...

Exercice 2. Déterminer les éléments d'ordre 6 dans le groupe $\mathbb{U}_{30}$.

Solution. Si $a \in \mathbb{U}_{30}$ est d'ordre 6, alors $\langle a \rangle = \{1, a, \ldots, a^5\}$ est un sous-groupe d'ordre 6 et $\langle a \rangle$ qui est cyclique possède $\varphi(6) = 2$ générateurs qui sont a et a^5 (3-1, prop.). Réciproquement, d'après la proposition ci-dessus, tout sous-groupe d'ordre 6 est cyclique et fournira deux éléments d'ordre 6. Puisque $\mathbb{U}_{30}$ est cyclique et $6 \,|\, 30$, il existe un unique sous-groupe d'ordre 6 qui est $\langle \zeta^5 \rangle$, où $\zeta = \exp\left(\frac{2i\pi}{30}\right)$. On a donc 2 éléments d'ordre 6 dans $\mathbb{U}_{30}$ qui sont $a = \zeta^5 = \exp\left(\frac{i\pi}{3}\right)$ et $a^5 = \zeta^{25} = \exp\left(\frac{5i\pi}{3}\right)$.

Exercice 3. Soit $n \in \mathbb{N}^*$. Montrer que $n = \sum_{d \mid n} \varphi(d)$.

Solution. D'après le th. de Lagrange, l'ordre de tout élément de $\mathbb{U}_n$ divise n. On a donc une partition $\mathbb{U}_n = \bigcup_{d \mid n} \Lambda_d$, où pour tout diviseur d de n on pose $\Lambda_d = \{ x \in \mathbb{U}_n \mid o(x) = d \}$. D'après la proposition, si d divise n, il existe dans le groupe cyclique $\mathbb{U}_n$ un unique sous-groupe d'ordre d. C'est $\mathbb{U}_d$ car $\mathbb{U}_d \subset \mathbb{U}_n$. Chacun des $\varphi(d)$ générateurs de $\mathbb{U}_d$ est un élément de Λ_d. Réciproquement, si $x \in \mathbb{U}_n$ est d'ordre d, alors $\langle x \rangle$ est un sous-groupe d'ordre d de $\mathbb{U}_n$. Il est donc égal à $\mathbb{U}_d$ d'après l'unicité du sous-groupe d'ordre d dans $\mathbb{U}_n$. Ainsi, x est un générateur de $\mathbb{U}_d$. Finalement, Λ_d est l'ensemble des générateurs de $\mathbb{U}_d$ et on a $\operatorname{card}(\Lambda_d) = \varphi(d)$ d'où la relation.

$$n = \operatorname{card}(\mathbb{U}_n) = \sum_{d \mid n} \operatorname{card}(\Lambda_d) = \sum_{d \mid n} \varphi(d).$$

3.4 Produit de deux groupes cycliques

Proposition.

Le produit $G_1 \times G_2$ de deux groupes est cyclique si et seulement si G_1 et G_2 sont cycliques d'ordres m et n premiers entre eux. Dans ce cas, (a, b) est un générateur de $G_1 \times G_2$ si et seulement si a et b sont des générateurs de G_1 et G_2 respectivement.

Démonstration. Supposons $G = G_1 \times G_2$ cyclique, engendré par (a, b). Les projections p_1 et p_2 de G sur G_1 et G_2 sont des homomorphismes surjectifs. D'après 3-2, $G_1 = p_1(G)$ et $G_2 = p_2(G)$ sont cycliques, engendrés par a et b. D'après 1-14, cor. 2, on a :

$$mn = [G_1 : 1] \times [G_2 : 1] = [G : 1] = o(a, b) = \operatorname{ppcm}(m, n).$$

Cette égalité nécessite que $m \wedge n = 1$.

Réciproquement, supposons que G et G_2 sont cycliques d'ordres m et n premiers entre eux. Soient a et b des générateurs de G_1 et G_2. D'après 1-14, cor. 2, on a $o(a, b) = \operatorname{ppcm}(m, n) = mn = [G : 1]$. Le sous-groupe engendré par (a, b) est donc égal à G. ∎

Corollaire 1.

Le produit $G = G_1 \times \cdots \times G_k$ de k groupes cycliques est cyclique si et seulement si les ordres $n_1, \ldots, n_k$ de ces groupes sont deux à deux premiers entre eux.

Démonstration. Raisonnons par récurrence sur k. D'après la proposition, le résultat est vrai pour $k = 2$. Admettons ce résultat pour $k - 1$ groupes. Considérons k groupes cycliques $G_1, \ldots, G_k$.

Supposons $n_1, \ldots, n_k$ deux à deux premiers entre eux. D'après l'hypothèse de récurrence, $G' = G_1 \times \cdots \times G_{k-1}$ est cyclique. De plus, son ordre $n_1 \cdots n_{k-1}$ est premier avec l'ordre n_k de G_k. D'après la proposition, $G = G' \times G_k$ est cyclique.

Réciproquement, si $G = G' \times G_k$ est cyclique alors G' est cyclique car la projection de G sur G' est un homomorphisme surjectif. D'après l'hypothèse de récurrence $n_1, \ldots, n_{k-1}$ sont deux à deux premiers entre eux. D'après la proposition, n_k est premier avec $[G' : 1] = n_1 \cdots n_{k-1}$ et donc avec $n_1, \ldots, n_{k-1}$. ∎

Corollaire 2.

(i) *La fonction d'Euler φ est multiplicative dans le sens suivant :*

$$\forall\, m \in \mathbb{N}^* \quad \forall\, n \in \mathbb{N}^* \qquad m \wedge n = 1 \quad \Rightarrow \quad \varphi(mn) = \varphi(m)\varphi(n)\,.$$

(ii) *Si la décomposition en facteurs premiers de $n \geqslant 2$ est $n = p_1^{s_1} \cdots p_k^{s_k}$ alors on a*

$$\varphi(n) \;=\; n\,(1 - \tfrac{1}{p_1}) \cdots (1 - \tfrac{1}{p_k})\,.$$

Démonstration. (i) Pour $m \geqslant 2$, notons Δ_m l'ensemble des générateurs du groupe $\mathbb{Z}/m\mathbb{Z}$. Supposons $m \wedge n = 1$. D'après la proposition, $\Delta_m \times \Delta_n$ est l'ensemble des générateurs de $(\mathbb{Z}/m\mathbb{Z}) \times (\mathbb{Z}/n\mathbb{Z})$ et ce groupe cyclique est isomorphe à $\mathbb{Z}/mn\mathbb{Z}$ donc

$$\varphi(m)\,\varphi(n) = \text{card}\,(\Delta_m \times \Delta_n) = \text{card}\,(\Delta_{mn}) = \varphi(mn)\,.$$

(ii) Supposons que $k = 1$, soit $n = p^s$, avec p premier. Les éléments de $[0, n-1]$ qui ne sont pas premiers avec n, sont $0,\ p,\ 2p,\ \ldots,\ (p^{s-1}-1)p$. On a donc $\text{card}\,(\Delta_n) = p^s - p^{s-1} = p^s(1 - \frac{1}{p})$. Supposons $k \geqslant 2$, d'où $n = p_1^{s_1} \cdots p_k^{s_k}$. D'après (i) on a :

$$\varphi(n) \;=\; \varphi(p_1^{s_1}) \cdots \varphi(p_k^{s_k}) \;=\; p_1^{s_1}(1 - \tfrac{1}{p_1}) \cdots p_k^{s_k}(1 - \tfrac{1}{p_k})\,. \qquad \blacksquare$$

Exercice. Soient $m, n \in \mathbb{N}^*$. Montrer que $\varphi(mn) = \varphi(m)\varphi(n)\frac{d}{\varphi(d)}$, où $d = \text{pgcd}(m, n)$.

Solution. Les facteurs premiers de mn sont les facteurs premiers de m seul (qui ne sont pas facteurs de n), les facteurs premiers de n seul et les facteurs premiers communs à m et n qui sont les facteurs premiers du pgcd d. Si on applique (ii) à m et n, on voit que $\varphi(m)\varphi(n)$ contient tous les termes de $\varphi(mn)$ mais que $\prod_{p|d}(1 - \frac{1}{p}) = \frac{\varphi(d)}{d}$ est compté deux fois. En divisant $\varphi(m)\varphi(n)$ par ce terme, on obtient bien $\varphi(mn)$.

3.5 Groupes d'ordre premier

Définition.

Un groupe G est dit simple si $\{e\}$ et G sont les seuls sous-groupes distingués de G.

Proposition.

Un groupe G est d'ordre premier si et seulement s'il est cyclique et simple.

Démonstration. Supposons $p = [G : 1]$ premier et soit $x \in G$ distinct de e. D'après le th. de Lagrange, $o(x)$ divise p, avec $o(x) \neq 1$. On a donc $o(x) = p$ et $\langle x \rangle = G$. Cela prouve que G est cyclique et que tout sous-groupe $H \neq \{e\}$ est égal à G.

Réciproquement, si G est cyclique, simple, alors 3-3, cor. montre que $p = [G : 1]$ n'a pas d'autre diviseur que 1 et p. Donc p est premier. $\blacksquare$

Lemme 1.

Soit G un groupe fini. Supposons qu'il existe un sous-groupe H du centre $Z(G)$ de G tel que G/H soit cyclique. Alors G est abélien.

Démonstration. Tout sous-groupe du centre $Z(G)$ étant distingué, G/H est un groupe. Puisque G/H est cyclique, il existe $a \in G$ tel que $\overline{a}$ engendre G/H. Soient $x, y \in G$. Il existe $k, l \in \mathbb{N}$ tels que $\overline{x} = \overline{a}^k$ et $\overline{y} = \overline{a}^l$. Il existe alors $z, z' \in H \subset Z(G)$ tels que $x = a^k z$ et $y = a^l z'$. On a $yx = xy$ car a^k, a^l, z, z' commutent deux à deux. Donc G est abélien. ∎

Lemme 2.

Soit G un groupe fini d'ordre p^m, avec p premier et $m \in \mathbb{N}^*$. Le centre $Z(G)$ de G n'est pas réduit à $\{e\}$.

Démonstration. Faisons agir G sur lui-même par automorphismes intérieurs. Alors $x \in G$ a une orbite ponctuelle, si et seulement si $gxg^{-1} = x$ pour tout $g \in G$, c'est-à-dire si $x \in Z(G)$. D'après l'équation des classes (cor. 2-3), card $(G) = p^m$ et $[Z(G) : 1]$ sont congrus modulo p. Donc $[Z(G) : 1]$ est divisible par p. Comme le centre $Z(G)$ contient l'élément neutre e, il possède au moins p éléments. ∎

Corollaire 1.

Si un groupe G est d'ordre p^2, avec p premier, alors G est abélien.

Démonstration. D'après le th. de Lagrange, $[Z(G) : 1]$ divise $[G : 1] = p^2$. D'après le lemme 2, $Z(G)$ est d'ordre p ou p^2. Supposons que $[Z(G) : 1] = p$. Le groupe quotient $G/Z(G)$, d'ordre $[G : Z(G)] = p$, est cyclique d'après la proposition. Le lemme 1 montre que $Z(G) = G$. Le cas $[Z(G) : 1] = p$ ne se présente donc pas. On a $[Z(G) : 1] = p^2$ et $Z(G) = G$ ∎.

Corollaire 2.

Soit G un groupe d'ordre p^m avec p premier et $m \geqslant 1$. Il existe dans le centre $Z(G)$ de G un élément d'ordre p.

Démonstration. D'après le lemme 2, le centre $Z(G)$ n'est pas réduit à $\{e\}$. D'après le th. de Lagrange, son ordre est une puissance de p. Le th. de Cauchy (voir 2-4) donne le résultat. ∎

3.6 Décomposition cyclique d'un groupe abélien fini

Lemme.

Soient G un groupe abélien fini et $a \in G$ d'ordre $o(a)$ maximum. Pour tout $y \in G/\langle a \rangle$ il existe $x \in G$ tel que $\overline{x} = y$ et tel que $o(x) = o(y)$.

Démonstration. Notons additivement la loi de composition de G. Soient φ l'homomorphisme canonique de G sur $G/\langle a \rangle$ et soit s l'ordre de $y \in G/\langle a \rangle$. Considérons $x \in G$ tel que $\varphi(x) = y$. On a $\varphi(sx) = sy = 0$ et donc $sx \in \mathrm{Ker}\,(\varphi) = \langle a \rangle$. Il existe donc $k \in \mathbb{N}$ tel que $0 \leqslant k < o(a)$ et $sx = ka$. Par division euclidienne,

$$k = sq + r \quad \text{avec} \quad 0 \leqslant r < s, \tag{1}$$

d'où $sx = ka = sqa + ra$. Posons $x' = x - qa$. On a

$$\varphi(x') = \varphi(x) = y \quad \text{d'où} \quad s = o(y) \,|\, o(x'). \tag{2}$$

Supposons $r \neq 0$. On a $sx' = sx - sqa = ra$. En utilisant 3-1, on obtient $o(sx') = \frac{o(x')}{o(x') \wedge s}$ soit $o(sx') = \frac{o(x')}{s}$ en tenant compte de (2). On en déduit,

$$o(x') \;=\; s\,o(sx') \;=\; s\,o(ra) \;=\; s\,\frac{o(a)}{o(a)\wedge r}\cdot$$

Du fait que $o(a)$ est maximum, on a $o(x') \leqslant o(a)$. La relation précédente donne alors $s \leqslant o(a)\wedge r \leqslant r$. Cela contredit (1) donc $r = 0$ et $sx' = ra = 0$. Cela prouve que $o(x') \mid s$ et donc que $o(x') = o(y)$ si on tient compte de (2). ∎

Proposition.

Soit G un groupe abélien fini d'ordre $n \geqslant 2$. Il existe des entiers q_1 supérieur ou égal à deux, q_2 multiple de $q_1, \ldots, q_k$ multiple de q_{k-1}, uniques, tels que G soit isomorphe à $(\mathbb{Z}/q_1\mathbb{Z}) \times \cdots \times (\mathbb{Z}/q_k\mathbb{Z})$.

Démonstration. 1°/ *Montrons l'existence* de cette suite, par récurrence sur l'ordre n de G. Pour $n = p$ premier, la propriété est vérifiée car G est isomorphe à $\mathbb{Z}/p\mathbb{Z}$ (3-5, prop.). Considérons G d'ordre $n \geqslant 2$. Supposons établie l'existence pour les groupes d'ordre strictement inférieur à n. Soit $a \in G$ d'ordre m maximum. On a $m > 1$ car $G \neq \{e\}$ donc $G/\langle a\rangle$ est d'ordre strictement inférieur à $[G : 1] = n$. D'après l'hypothèse de récurrence, il existe dans $G/\langle a\rangle$ des sous-groupes cycliques $G'_1 = \langle a'_1\rangle, \ldots, G'_{k-1} = \langle a'_{k-1}\rangle$ d'ordres $q_1, \ldots, q_{k-1}$ tels que $1 < q_1 | \cdots | q_{k-1}$ et tels que $G/\langle a\rangle = G'_1 \times \cdots \times G'_{k-1}$. D'après le lemme, il existe dans G des représentants $a_1, \ldots, a_{k-1}$ de $a'_1, \ldots, a'_{k-1}$ ayant les mêmes ordres. Vérifions que G est produit direct des sous-groupes cycliques $G_1 = \langle a_1\rangle, \ldots, G_{k-1} = \langle a_{k-1}\rangle, G_k = \langle a\rangle$.

Soit φ l'homomorphisme canonique de G sur $G/\langle a\rangle$. Pour tout $x \in G$, il existe $n_1, \ldots, n_{k-1}$, avec $0 \leqslant n_i < o(a_i)$ pour $i = 1, \ldots, k-1$, uniques, tels que

$$\varphi(x) \;=\; n_1a'_1 + \cdots + n_{k-1}a'_{k-1} \;=\; \varphi(n_1a_1 + \cdots + n_{k-1}a_{k-1})\,.$$

Il existe donc un élément n_ka de $\mathrm{Ker}\,(\varphi) = \langle a\rangle$ avec $0 \leqslant n_k < m = o(a)$ et tel que $x = (n_1a_1 + \cdots + n_{k-1}a_{k-1}) + n_ka$. Ainsi $G = G_1 + \cdots + G_k$.

Vérifions que cette expression de x est unique. Alors G sera le produit direct des sous-groupes $G_1, \ldots, G_k$. Soit $x = m_1a_1 + \cdots + m_ka$ une autre expression de x du type précédent. Alors $\varphi(x) = n_1a'_1 + \cdots + n_{k-1}a'_{k-1} = m_1a'_1 + \cdots + m_{k-1}a'_{k-1}$. Comme $G/\langle a\rangle$ est produit direct de $G'_1, \ldots, G'_{k-1}$, on a $n_1 = m_1, \ldots, n_{k-1} = m_{k-1}$. On en déduit ensuite $n_ka = m_ka$ d'où $n_k = m_k$ puisqu'on a $0 \leqslant n_k < o(a)$ et $0 \leqslant m_k < o(a)$.

D'après 1-14, cor. 2, l'ordre de $x_0 = (a_1, \ldots, a_{k-1}, a) \in G_1 \times \cdots \times G_k$ est le ppcm de $o(a_1), \ldots, o(a)$. On a donc $o(x_0) \geqslant o(a)$. Comme $o(a)$ est le maximum des ordres des éléments de G, on en déduit que $o(a) = o(x_0) = \text{ppcm}\,(o(a_1), \ldots, o(a_{k-1}), o(a))$ et donc que $o(a_1) \mid \ldots \mid o(a_{k-1}) \mid o(a)$.

2°/ *Montrons l'unicité* de la suite $q_1, \ldots, q_k$ par récurrence sur l'ordre n de G.

Si $n = p$ est premier, la suite (q_i) est unique, réduite à p. Supposons établie l'unicité pour les groupes d'ordre strictement inférieur à n. Considérons un groupe G d'ordre $n > 2$. Considérons deux décompositions

$$G \;=\; G_1 \times \cdots \times G_k \;=\; G'_1 \times \cdots \times G'_m\,,$$

avec $\quad G_i \simeq \mathbb{Z}/q_i\mathbb{Z} \quad , \quad G'_j \simeq \mathbb{Z}/q'_j\mathbb{Z} \quad , \quad 1 < q_1 \mid \cdots \mid q_k \quad , \quad 1 < q'_1 \mid \cdots \mid q'_m\,.$

Soit p un facteur premier de q_1 et donc de $q_2, \ldots, q_k$. Comme G est abélien, $f : x \mapsto px$ est un endomorphisme de G. Il laisse stable chacun des sous-groupes G_i. D'après 3-3, $f(G_1) \subset G_1$ est l'unique sous-groupe de G_1 d'ordre $\frac{q_1}{p}$. De même, $f(G_2) \subset G_2$, $\ldots$, $f(G_k) \subset G_k$ sont d'ordres $\frac{q_2}{p}, \ldots, \frac{q_k}{p}$. On a

$$[f(G_1) + \cdots + f(G_i)] \cap f(G_{i+1}) \subset [G_1 + \cdots + G_i] \cap G_{i+1} = \{0\}\,,$$

pour $i = 1, \dots, k-1$ donc $f(G)$ est produit direct de $f(G_1), \dots, f(G_k)$ et on a $[f(G) : 1] = \dfrac{q_1 \cdots q_k}{p^k} = \dfrac{[G : 1]}{p^k}$.

De même, on a $f(G'_j) \subset G'_j$ pour $j = 1 \dots, m$ et $f(G) = f(G'_1) \times \cdots \times f(G'_m)$. Puisque $q'_1 \mid \cdots \mid q'_m$, il existe r tel que p ne divise pas $q'_1, \dots, q'_r$ et p divise $q'_{r+1}, \dots, q'_m$. On a alors $f(G'_1) = G'_1$ car $f : x \mapsto px$ est alors un automorphisme de G'_1, d'après 3-2. De même, $f(G'_2) = G'_2, \dots, f(G'_r) = G'_r$. Par contre, les ordres de $f(G'_{r+1}), \dots, f(G'_m)$ sont $\dfrac{q'_{r+1}}{p}, \dots, \dfrac{q'_m}{p}$, donc $[f(G) : 1] = q'_1 \cdots q'_r \dfrac{q'_{r+1} \cdots q'_m}{p^{m-r}} = \dfrac{[G : 1]}{p^{m-r}}$.

En comparant les deux valeurs de $[f(G) : 1]$ obtenues, on voit que $k = m - r \leqslant m$. En échangeant les rôles, on obtient de même $m \leqslant k$ et donc $m = k$. On en déduit que $r = 0$ et que p divise $q'_1, \dots, q'_k$. D'après l'hypothèse de récurrence, la décomposition cyclique de $f(G)$ est unique. Les deux suites $\dfrac{q_1}{p}, \dots, \dfrac{q_k}{p}$ et $\dfrac{q'_1}{p}, \dots, \dfrac{q'_k}{p}$ sont donc égales et les suites $q_1, \dots, q_k$ et $q'_1, \dots, q'_k$ sont égales. ∎

Définition.

Cette suite $q_1, \dots, q_k$ telle que

$$G \simeq (\mathbb{Z}/q_1\mathbb{Z}) \times \cdots \times (\mathbb{Z}/q_k\mathbb{Z}) \qquad \text{et} \qquad 1 < q_1 \mid q_2 \dots \mid q_k,$$

qui caractérise G à isomorphisme près, est appelée la suite des invariants de G.

Corollaire 1.

Soit G un groupe abélien d'ordre p^m où p est premier. Il existe une suite $r_1 \leqslant \cdots \leqslant r_k$ dans $\mathbb{N}^*$, unique, telle que $G \simeq (\mathbb{Z}/p^{r_1}\mathbb{Z}) \times \cdots \times (\mathbb{Z}/p^{r_k}\mathbb{Z})$.

Corollaire 2.

Soit G un groupe abélien fini. Il existe un élément a de G dont l'ordre est le ppcm *des ordres des éléments de G.*

Démonstration. Posons $n = [G : 1]$. Si $n = 1$, le résultat est évident. Si $n \geqslant 2$, il existe dans G des sous-groupes cycliques $G_1, \dots, G_k$ tels que $G = G_1 \times \cdots \times G_k$ d'ordres $q_1, \dots, q_k$ tels que $2 \leqslant 2$ et $q_1 \mid q_2 \mid \cdots, \mid q_k$. Soit a un générateur de G_k. Pour tout $x = (x_1, \dots, x_k) \in G_1 \times \cdots \times G_k = G$ on a $o(x) = \text{ppcm}(o(x_1), \dots, o(x_k))$, avec $o(x_1) \mid q_1 \mid \cdots \mid q_k$, $o(x_2) \mid q_2 \mid \cdots, \mid q_k$, etc... Donc $o(x)$ divise $q_k = o(a)$ et $o(a)$ est le ppcm des ordres $o(x)$ des éléments x de G. ∎

Corollaire 3.

Soit G un groupe abélien d'ordre $n \geqslant 2$. Soit $n = p_1^{k_1} \cdots p_r^{k_r}$ la décomposition en facteurs premiers de n.

(i) *Pour tout diviseur d de l'ordre n de G, il existe un sous-groupe de G d'ordre d.*

(ii) *Pour chacun des diviseurs $p_i^{k_i}$ où $i = 1, \dots, k$, il existe un seul sous-groupe H_i d'ordre $p_i^{k_i}$ et $H_i = \{x \in G \mid \exists \alpha \quad o(x) = p_i^\alpha\}$. On a $G = H_1 \times \cdots \times H_r$.*

Démonstration. (i) D'après la proposition, G est produit direct $G_1 \times \cdots \times G_k$ de sous-groupes cycliques. On a $[G : 1] = [G_1 : 1] \times \cdots \times [G_k : 1]$. Si d divise $[G : 1]$, en répartissant autant de fois qu'on le peut chacun de ses facteurs premiers dans $[G_1 : 1]$, puis dans $[G_2 : 1]$, etc... on peut écrire d comme un produit $d = d_1 \cdots d_k$ où d_i divise $[G_i : 1]$ pour $i = 1, \dots, k$. Pour $i = 1, \dots, k$, il existe un sous-groupe K_i d'ordre d_i dans le groupe cyclique G_i. Alors $K_1 \times \cdots \times K_k \subset G_1 \times \cdots \times G_k = G$ est d'ordre d.

(ii) D'après (i), il existe dans G des sous-groupes $H_1, \dots, H_r$ d'ordres $p_1^{k_1}, \dots, p_r^{k_r}$. L'ordre de $H_1 \cap H_2$ est 1 car il divise les ordres $p_1^{k_1}$ et $p_2^{k_2}$ de H_1 et de H_2. On a donc $H_1 \cap H_2 = \{e\}$ et H_1H_2 est un sous-groupe de G isomorphe à $H_1 \times H_2$, d'ordre $p_1^{k_1}p_2^{k_2}$. De même, $(H_1H_2)H_3$, est isomorphe à $(H_1 \times H_2) \times H_3$, d'ordre $p_1^{k_1}p_2^{k_2}p_3^{k_3}$. Par récurrence finie, on voit que $H_1 \times \cdots \times H_r$ est un sous-groupe de G d'ordre $p_1^{k_1} \cdots p_r^{k_r}$. Il est donc égal à G. Soit $x = (x_1, \dots, x_r) \in H_1 \times \cdots \times H_r$. D'après le th. de Lagrange, il existe $\alpha_1, \dots, \alpha_r$, tels que $o(x_1) = p_1^{\alpha_1}, \dots, o(x_r) = p_r^{\alpha_r}$. On a $o(x) = \text{ppcm}(o(x_1), \dots, o(x_r)) = p_1^{\alpha_1} \cdots p_r^{\alpha_r}$. Si $o(x)$ est une puissance p_1^{α} de p_1, alors $\alpha_2 = 0, \dots, \alpha_r = 0$ et $x \in H_1$. Il résulte de cela deux choses. D'abord $H_1 = \{x \in G \mid \exists \alpha \quad o(x) = p_1^{\alpha}\}$. Ensuite, si H_1' est un autre sous-groupe de G d'ordre $p_1^{\alpha_1}$, l'ordre de tout élément de H_1' divisant $p_1^{\alpha_1}$ on a $H_1' \subset H_1$ et donc $H_1' = H_1$ car les ordres de ces sous-groupes sont égaux. Il existe donc un seul sous-groupe d'ordre $p_1^{k_1}$ dans G. Il en va de même pour les autres facteurs premiers de n. ∎

Définition.

Les sous-groupes $H_1, \dots, H_r$ de G d'ordres $p_1^{k_1}, \dots, p_r^{k_r}$, uniques avec cette propriété, sont appelés les composantes primaires du groupe commutatif G.

Exercice 1. Quelles sont les composantes primaires de $\mathbb{U}_{90}$?

Solution. On a $90 = 2 \times 3^2 \times 5$. Les composantes primaires de $\mathbb{U}_{90}$ sont des sous-groupes d'ordres 2, 3^2, 5. Ils sont uniques de ces ordres-là. Comme $\mathbb{U}_2 = \{1, -1\}$, $\mathbb{U}_9$, $\mathbb{U}_5$ sont des sous-groupes de $\mathbb{U}_{90}$, ce sont les composantes primaires. On a donc $\mathbb{U}_{90} = \mathbb{U}_2 \times \mathbb{U}_9 \times \mathbb{U}_5$.

Exercice 2. Donner la décomposition canonique de $G = (\mathbb{Z}/60\mathbb{Z}) \times (\mathbb{Z}/72\mathbb{Z})$.

Solution. On a $60 = 2^2 \times 3 \times 5$ et $72 = 2^3 \times 3^2$. Soit $H_1 \times H_2 \times H_3$ la décomposition primaire de $\mathbb{Z}/60\mathbb{Z}$. D'après 3-3, le sous-groupe H_1 est cyclique d'ordre 2^2 égal à $\langle \overline{15} \rangle$. On a $H_1 \simeq (\mathbb{Z}/2^2\mathbb{Z})$. De même, H_2 d'ordre 3 est $\langle \overline{20} \rangle \simeq \mathbb{Z}/3\mathbb{Z}$ et H_3 d'ordre 5 est $\langle \overline{12} \rangle \simeq \mathbb{Z}/5\mathbb{Z}$. On a donc $\mathbb{Z}/60\mathbb{Z} \simeq (\mathbb{Z}/2^2\mathbb{Z}) \times (\mathbb{Z}/3\mathbb{Z}) \times (\mathbb{Z}/5\mathbb{Z})$.

De même, $\mathbb{Z}/72\mathbb{Z} = K_1 \times K_2 \simeq (\mathbb{Z}/2^3\mathbb{Z}) \times (\mathbb{Z}/3^2\mathbb{Z})$, où $K_1 = \langle \overline{8} \rangle$ et $K_2 = \langle \overline{9} \rangle$.

De ces décompositions primaires on déduit celle de G :

$$\begin{aligned} G &\simeq (H_1 \times K_1) \times (H_2 \times K_2) \times H_3 \\ &\simeq [(\mathbb{Z}/2^2\mathbb{Z}) \times (\mathbb{Z}/2^3\mathbb{Z})] \times [(\mathbb{Z}/3\mathbb{Z}) \times (\mathbb{Z}/3^2\mathbb{Z})] \times [\mathbb{Z}/5\mathbb{Z}] \end{aligned}$$

Un produit de groupes cycliques d'ordres deux à deux premiers entre eux est cyclique donc $(\mathbb{Z}/2^3\mathbb{Z}) \times (\mathbb{Z}/3^2\mathbb{Z}) \times (\mathbb{Z}/5\mathbb{Z})$ est cyclique isomorphe à $(\mathbb{Z}/360\mathbb{Z})$. De même, $(\mathbb{Z}/2^2\mathbb{Z}) \times (\mathbb{Z}/3\mathbb{Z})$ est cyclique isomorphe à $\mathbb{Z}/12\mathbb{Z}$. Ainsi G est isomorphe à $(\mathbb{Z}/12\mathbb{Z}) \times (\mathbb{Z}/360\mathbb{Z})$. Ses invariants sont $q_1 = 12$ et $q_2 = 360$ (voir aussi Ex. 3-11).

Exercice 3. A isomorphisme près, quelles sont les structures possibles pour un groupe abélien d'ordre $600 = 2^3 \times 5^2 \times 3$?

Solution. La composante primaire H_1 de G relative au facteur premier 2 est un groupe d'ordre 2^3. D'après le cor. 1, les structures possibles sont données par la suite des invariants, soit par une suite d'entiers $r_1 \leqslant \cdots \leqslant r_k$ telle que $r_1 + \cdots + r_k = 3$. Donc H_1 est isomorphe à l'un des groupes $\mathbb{Z}/2^3\mathbb{Z}$, $(\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/2^2\mathbb{Z})$, $(\mathbb{Z}/2\mathbb{Z})^3$. L'unique sous-groupe H_2 de G d'ordre 5^2 est isomorphe à $\mathbb{Z}/5^2\mathbb{Z}$ ou a $(\mathbb{Z}/5\mathbb{Z})^2$.

L'unique sous-groupe H_3 d'ordre 3 est isomorphe à $\mathbb{Z}/3\mathbb{Z}$.
Il existe donc $3 \times 2 = 6$ structures possibles pour G qui sont

$(\mathbb{Z}/2^3\mathbb{Z}) \times (\mathbb{Z}/5^2\mathbb{Z}) \times (\mathbb{Z}/3\mathbb{Z}) \simeq \mathbb{Z}/600\mathbb{Z}$,
$(\mathbb{Z}/2^3\mathbb{Z}) \times (\mathbb{Z}/5\mathbb{Z}) \times (\mathbb{Z}/5\mathbb{Z}) \times (\mathbb{Z}/3\mathbb{Z}) \simeq (\mathbb{Z}/120\mathbb{Z}) \times (\mathbb{Z}/5\mathbb{Z})$,
$(\mathbb{Z}/2^2\mathbb{Z}) \times (\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/5^2\mathbb{Z}) \times (\mathbb{Z}/3\mathbb{Z}) \simeq (\mathbb{Z}/300\mathbb{Z}) \times (\mathbb{Z}/2\mathbb{Z})$,
$(\mathbb{Z}/2^2\mathbb{Z}) \times (\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/5\mathbb{Z}) \times (\mathbb{Z}/5\mathbb{Z}) \times (\mathbb{Z}/3\mathbb{Z}) \simeq (\mathbb{Z}/60\mathbb{Z}) \times (\mathbb{Z}/10\mathbb{Z})$,
$(\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/5^2\mathbb{Z}) \times (\mathbb{Z}/3\mathbb{Z}) \simeq (\mathbb{Z}/150\mathbb{Z}) \times (\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/2\mathbb{Z})$,
$(\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/5\mathbb{Z}) \times (\mathbb{Z}/5\mathbb{Z}) \times (\mathbb{Z}/3\mathbb{Z})$
$\simeq (\mathbb{Z}/30\mathbb{Z}) \times (\mathbb{Z}/10\mathbb{Z}) \times (\mathbb{Z}/2\mathbb{Z})$.

d'où les listes d'invariants possibles pour G :
(600) , $(5,120)$, $(2,300)$, $(10,60)$, $(2,2,150)$, $(2,10,30)$.

3.7 Groupes résolubles

Soit f un homomorphisme de G dans un autre groupe. L'image de f sera commutative si et seulement si pour tout $x \in G$ et pour tout $y \in G$, on a $f(x)f(y) = f(y)f(x)$, soit si $f(x)f(y)f(x)^{-1}f(y)^{-1} = e$ ou encore $xyx^{-1}y^{-1} \in \mathrm{Ker}\,(f)$. En particulier, si H est un sous-groupe distingué de G, le groupe G/H est abélien si et seulement si pour tout $x \in G$ et pour tout $y \in G$, l'élément $[x,y] = xyx^{-1}y^{-1}$ appartient à H.

Pour tout $\alpha \in \mathrm{Aut}\,(G)$, on a $\alpha([x,y]) = [\alpha(x), \alpha(y)]$. Le sous-groupe G' de G engendré par $C = \{\, [x,y]\,;\ \ x,y \in G \,\}$ est donc un sous-groupe caractéristique de G. Pour $k \in \mathbb{N}^*$, on définit par récurrence $G^{(k)}$ comme étant $(G^{(k-1)})'$. On convient que $G^{(0)} = G$. Les sous-groupes $G^{(k)}$ sont caractéristiques dans G.

Définitions.

L'élément $[x,y] = xyx^{-1}y^{-1}$ s'appelle le commutateur de x et y.

Le sous-groupe G' de G engendré par l'ensemble C des commutateurs s'appelle le sous-groupe dérivé du groupe G.

Le groupe G est dit résoluble, s'il possède une suite décroissante de sous-groupes,

$$(1) \qquad G = H_0 \supset H_1 \supset \cdots \supset H_{p-1} \supset H_p = \{e\}\,.$$

telle que $H_i \lhd H_{i-1}$ et telle que H_{i-1}/H_i soit abélien, pour $i = 1, \ldots, p$.

Proposition.

Soit G un groupe.

(i) *G est résoluble si et seulement s'il existe $p \in \mathbb{N}^*$ tel que $G^{(p)} = \{e\}$.*

(ii) *Si G est résoluble, tout sous-groupe K, tout quotient G/K (où $K \lhd G$) est résoluble.*

(iii) *Soit K un sous-groupe distingué de G. Pour que G soit résoluble, il faut et il suffit que K et G/K soient résolubles.*

Démonstration. (i) S'il existe $p \in \mathbb{N}$ tel que $G^{(p)} = \{e\}$, alors la définition précédente est vérifiée en prenant $H_i = G^{(i)}$ pour $i = 1, \ldots, p$.

Réciproquement, supposons G résoluble et considérons $(H_i)_{i=1,\ldots,p}$ ayant les propriétés de la définition. Montrons par récurrence que l'on a $G^{(k)} \subset H_k$ pour $k = 1, ..., p$.

On en déduira que $G^{(p)} = \{e\}$. Comme G/H_1 est abélien, on a $G' \subset H_1$. Supposons vérifié que $G^{(k-1)} \subset H_{k-1}$. L'homomorphisme $f : H_{k-1} \to H_{k-1}/H_k$ a une image commutative donc H_k contient $(H_{k-1})'$ et contient donc $(G^{(k-1)})' = G^{(k)}$.

(ii) Soit K un sous-groupe de G. On a $\{[x,y]\,;\ x \in K\,,\ y \in K\} \subset G'$ et donc $K' \subset G'$. Supposons établi que $K^{(i)} \subset G^{(i)}$, où $1 \leqslant i \leqslant p-1$. On en déduit $K^{(i+1)} = (K^{(i)})' \subset (G^{(i)})' = G^{(i+1)}$. Cela prouve par récurrence que $K^{(m)} \subset G^{(m)}$, pour tout $m \in \mathbb{N}$. D'après (i), si G est résoluble, il existe $p \in \mathbb{N}$ tel que $G^{(p)} = \{e\}$. On a alors $K^{(p)} = \{e\}$ et K est résoluble.

Supposons K distingué. L'homomorphisme canonique f de G sur G/K est surjectif. Soit $(H_i)_{i=0,\dots,p}$ une suite de sous-groupes de G ayant les propriétés de la définition. Dans G/K les sous-groupes $(f(H_i))_{i=0,\dots,p}$ vérifient (1). Pour $i = 1,\dots,p$, on a $f(H_i) \triangleleft f(H_{i-1})$ car f est surjective. En composant les homomorphismes surjectifs $H_{i-1} \to f(H_{i-1})$ et $f(H_{i-1}) \to f(H_{i-1})/\,f(H_i)$, on obtient un homomorphisme surjectif dont le noyau contient H_i. Il se factorise donc en un homomorphisme de même image et donc surjectif, de H_{i-1}/H_i sur $f(H_{i-1})/f(H_i)$. Comme H_{i-1}/H_i est commutatif, $f(H_{i-1})/f(H_i)$ est commutatif. Le groupe G/K est donc résoluble.

(iii) La condition est nécessaire d'après (ii). Montrons qu'elle est suffisante. Supposons G/K résoluble. Il existe une suite de sous-groupes $(H'_i)_{i=0,\dots,p}$ de G/K, vérifiant (1) telle que $H'_i \triangleleft H'_{i-1}$ et telle que H'_{i-1}/H'_i soit abélien pour tout i. Pour $i = 0,...,p$, posons $H_i = f^{-1}(H'_i)$, où $f : G \to G/K$ désigne l'homomorphisme canonique. On a $H_0 = G \supset H_1 \supset \cdots \supset H_p = K$ et $H_{i+1} \triangleleft H_i$ pour $i = 0,\dots,p-1$ (1-6, prop. (ii)). D'après 1-9, cor. 2, on a $H_i/H_{i+1} \simeq H'_i/H'_{i+1}$, abélien. Supposons de plus K résoluble. Il existe $K_0 = K \supset K_1 \supset \cdots \supset K_q = \{e\}$, vérifiant dans K les conditions de la définition des groupes résolubles. La suite $H_0 \supset H_1 \supset \cdots \supset H_p = K \supset K_1 \supset \cdots \supset K_q = \{e\}$ vérifie dans G toutes les conditions de cette définition. ∎

Corollaire 1.

Tout produit direct ou semi-direct de groupes résolubles est résoluble.

Démonstration. Cela résulte de (iii). En effet, si G est le produit semi-direct de deux sous-groupes H et K, on a $H \triangleleft (H \times_\alpha K)$ et $(H \times_\alpha K)/H \simeq K$ (2-6, rem.). ∎

Corollaire 2.

Soit G un groupe d'ordre p^m où p est premier et $m \in \mathbb{N}^*$. Alors G est résoluble. Plus précisément, il existe une suite finie $K_0 = \{e\} \subset K_1 \subset \cdots \subset K_m = G$ de sous-groupes distingués de G, telle que $[K_i/K_{i-1} : 1] = p$ pour $1 \leqslant i \leqslant m$.

Démonstration. Montrons cela par récurrence sur m. Si $m = 1$, alors $K_0 = \{e\}$, $K_1 = G$ conviennent. Considérons le cas où $m \geqslant 2$. Supposons démontrée la propriété pour les groupes d'ordre p^{m-1}. Soit G un groupe d'ordre p^m. D'après 2-5, cor. 3, il existe dans le centre Z de G un élément a d'ordre p. On a $K_1 = \langle a \rangle \triangleleft G$ et $G' = G/K_1$ est d'ordre p^{m-1}. D'après l'hypothèse de récurrence, il existe une suite

$$K'_1 = \{e\} \subset K'_2 \subset \cdots \subset K'_{m-1} \subset K'_m = G'\,,$$

de sous-groupes distingués de G' telle que $[K'_i/K'_{i-1} : 1] = p$ pour $2 \leqslant i \leqslant m$. Soit $\gamma : G \to G' = G/K_1$ l'homomorphisme canonique. Pour $i = 1, \dots, m$ les sous-groupes $K_i = \gamma^{-1}(K'_i)$ sont distingués dans G (1-6, prop. (ii)), d'ordre p car $K_i/K_{i-1} \simeq (K_i/K_1)/(K_{i-1}/K_1) \simeq K'_i/K'_{i-1}$ (1-9, cor. 2), d'où le résultat. ∎

Exercices du chapitre 3

Ex 3 - 1

Soit φ la fonction d'Euler.

a) Considérons un entier $n \geqslant 3$. Montrer que $\varphi(n)$ est pair.

b) Montrer que $\varphi(2n) = \varphi(n)$ si n est impair et que $\varphi(2n) = 2\varphi(n)$ si n est pair. Généraliser cette propriété.

Ex 3 - 2

Soient G et G' deux groupes cycliques d'ordres n, m. Combien existe-t-il d'homomorphismes de G dans G' ?

Donner l'expression de tous les homomorphismes de $\mathbb{Z}/21\mathbb{Z}$ dans $\mathbb{Z}/6\mathbb{Z}$, de $\mathbb{Z}/18\mathbb{Z}$ dans $\mathbb{Z}/6\mathbb{Z}$.

Ex 3 - 3

Montrer que le groupe $\mathrm{Aut}(\mathbb{Z}/5\mathbb{Z})$ des automorphismes du groupe additif $\mathbb{Z}/5\mathbb{Z}$ est cyclique. Expliciter ses éléments et donner ses générateurs.

Ex 3 - 4

Soient G un groupe cyclique multiplicatif d'ordre $n \geqslant 2$ et soit $k \in \mathbb{N}$. Montrer que $f_k : x \mapsto x^k$ est un endomorphisme de G. Déterminer son noyau, son image.

Ex 3 - 5

Pour $n \geqslant 3$, calculer le nombre k_n de polygones réguliers (convexes ou croisés) à n côtés, inscrits dans le cercle trigonométrique, tels que le point A_0 d'affixe 1 soit un sommet. Pour quelles valeurs de n a-t-on $k_n = 1$, $k_n = 2$?

Ex 3 - 6

a) Soit G est un sous-groupe fini de $\mathbb{C}^*$. Montrer que $G = \mathbb{U}_n$ où $n = [G : 1]$.

b) Soient $m, n \in \mathbb{N}^*$. Déterminer le sous-groupe de $\mathbb{C}^*$ engendré par $\mathbb{U}_m$ et $\mathbb{U}_n$.

c) Soient $n, p, q \in \mathbb{N}^*$. A quelle condition a-t-on $\mathbb{U}_n \simeq \mathbb{U}_p \times \mathbb{U}_q$?

d) Pour un tel choix, montrer que $\mathrm{Aut}(\mathbb{U}_n) \simeq \mathrm{Aut}(\mathbb{U}_p) \times \mathrm{Aut}(\mathbb{U}_q)$.

Ex 3 - 7

Donner la décomposition primaire du groupe abélien $\mathbb{Z}/n\mathbb{Z}$, où $n = 851$.
En déduire la structure du groupe A des automorphismes de $\mathbb{Z}/n\mathbb{Z}$. (On pourra utiliser l'exercice précédent.)

Ex 3 - 8

Caractériser les groupes finis G qui sont tels que $x^2 = e$ pour tout $x \in G$.

Ex 3 - 9

Soit G un groupe commutatif fini.
Supposons que pour tout diviseur d de l'ordre n de G, il existe un et un seul sous-groupe d'ordre d dans G. Montrer que G est cyclique.

Ex 3 - 10

Quelles sont toutes les structures possibles pour un groupe abélien G d'ordre 720 ?

Ex 3 - 11

Soient $k \geqslant 2$ et $n \geqslant 2$ des entiers. Posons $d = \mathrm{pgcd}(k, n)$, $m = \mathrm{ppcm}(k, n)$.
Montrer que $G = (\mathbb{Z}/k\mathbb{Z}) \times (\mathbb{Z}/n\mathbb{Z})$ est isomorphe à $(\mathbb{Z}/d\mathbb{Z}) \times (\mathbb{Z}/m\mathbb{Z})$ et que c'est, à isomorphisme près, la seule expression de G de la forme $(\mathbb{Z}/p\mathbb{Z}) \times (\mathbb{Z}/q\mathbb{Z})$ avec p diviseur de q.

Exemple $G = (\mathbb{Z}/18\mathbb{Z}) \times (\mathbb{Z}/45\mathbb{Z})$.

Ex 3 - 12

Soit G un groupe abélien infini. Montrer que l'ensemble T des éléments d'ordre fini de G est un sous-groupe de G.
Si $T = \{e\}$, on dit que G est sans torsion. Montrer que G/T est sans torsion.

Ex 3 - 13

Soient $G = H \times_\varphi K$ un produit semi-direct d'un groupe cyclique H par un groupe d'ordre p^m, où p est premier.
Montrer que G est résoluble et que pour tout diviseur d de $[G : 1]$, il existe un sous-groupe de G d'ordre d.

Ex 3 - 14

Soit G un groupe abélien fini. On appelle caractère de G, un homomorphisme de G dans $\mathbb{C}^*$. L'ensemble $\widehat{G}$ des caractères de G s'appelle le dual de G.

a) Soient $\chi \in \widehat{G}$ et $\chi' \in \widehat{G}$. Montrer que le produit $\chi\chi'$ des fonctions χ et χ' est un élément de $\widehat{G}$ et que $\widehat{G}$ muni de ce produit est un groupe.

b) Soit $\chi \in \widehat{G}$. Montrer que $|\chi(g)| = 1$ pour tout $g \in G$.

c) Si $G = \mathbb{U}_n$, montrer que $\widehat{G} \simeq G$.

d) Si G est le produit direct $G_1 \times G_2$ de deux groupes abéliens finis, montrer que $\widehat{G} \simeq \widehat{G}_1 \times \widehat{G}_2$.

e) Soit G un groupe abélien fini. Montrer que $G \simeq \widehat{G}$.

Indications

Ex 3 - 1

Utiliser l'expression de $\varphi(n)$.

Ex 3 - 2

Si $f \in \mathrm{Hom}(G, G')$, l'ordre k de $f(G)$ divise les ordres de G et de G'. Dans G' cyclique, la donnée de k détermine $f(G)$.

Ex 3 - 3

$\alpha \mapsto \alpha(\overline{1})$ est bijective, de $\mathrm{Aut}(\mathbb{Z}/5\mathbb{Z})$ sur l'ensemble des générateurs de $\mathbb{Z}/5\mathbb{Z}$. On en déduit $\mathrm{Aut}(\mathbb{Z}/5\mathbb{Z})$.

Ex 3 - 4

Utiliser la caractérisation des sous-groupes d'un groupe cyclique.

Ex 3 - 5

Tout générateur ζ de $\mathbb{U}_n$ détermine un polygone régulier. Mais ζ et $\zeta^{-1} = \overline{\zeta}$ définissent le même polygone.

Ex 3 - 6

Tout $\zeta \in G$ est racine du polynôme $X^n - 1$, d'où **a)**.
Pour les questions suivantes, on peut raisonner dans le groupe cyclique $\mathbb{U}_{nm}$.

Ex 3 - 7

$\mathbb{Z}/n\mathbb{Z}$ étant cyclique, ses composantes primaires sont bien identifiées.

Ex 3 - 8

Montrer que G est abélien, puis que 2 est le seul facteur premier de son ordre.

Ex 3 - 9

Utiliser la décomposition canonique et les invariants de G.

Ex 3 - 10

Rechercher les invariants possibles pour un tel groupe.

Ex 3 - 11

Effectuer la décomposition primaire des groupes

Ex 3 - 12

On peut s'appuyer sur la définition de l'ordre d'un élément.

Ex 3 - 13

Pour tout diviseur de $[H : 1]$ (resp. de $[K : 1]$) il existe un sous-groupe de H (resp. de K) de cet ordre.

Ex 3 - 14

a) Vérification facile.

b) Si $[G : 1] = n$, on a $g^n = e$ pour tout $g \in G$.

c) On connait $\mathrm{card}(\mathrm{Hom}(\mathbb{U}_n, \mathbb{U}_n)) = n$ (Ex. 3-2).

d) Considérer les restrictions aux sous-groupes G_1, G_2 de tout $\chi \in \widehat{G}$.

e) Utiliser la décomposition canonique d'un groupe abélien fini.

Solutions des exercices du chapitre 3

Ex 3 - 1

a) Si $n = 2^k$, avec $k \geqslant 2$, alors $\varphi(n) = 2^k - 2^{k-1} = 2^{k-1}$ est pair.

Si n a un facteur premier impair p, de multiplicité k, on a $n = p^k m$ avec $p^k \wedge m = 1$. Alors $\varphi(n) = \varphi(p^k)\varphi(m) = (p-1)p^{k-1}\varphi(m)$ est pair car $p-1$ est pair.

b) Si n est impair, comme $2 \wedge n = 1$ on a $\varphi(2n) = \varphi(2)\varphi(n) = (2-1)\varphi(n) = \varphi(n)$.

Si n est pair, il existe m impair et $k \geqslant 1$ tels que $n = 2^k m$. Comme 2^k et 2^{k+1} sont premiers avec m, on a

$\varphi(n) = \varphi(2^k m) = \varphi(2^k)\varphi(m) = (2^k - 2^{k-1})\varphi(m)$,
$\varphi(2n) = \varphi(2^{k+1}m) = \varphi(2^{k+1})\varphi(m) = (2^{k+1} - 2^k)\varphi(m) = 2\varphi(n)$.

Généralisation. On montre de même, que pour tout $s \in \mathbb{N}^*$ on a $\varphi(2^s n) = 2^{s-1}\varphi(n)$ pour n impair et $\varphi(2^s n) = 2^s\varphi(n)$ pour n pair.

Autre généralisation. Soit p un nombre premier. Si n n'est pas divisible par p, on a $\varphi(pn) = (p-1)\varphi(n)$. Si n est divisible par p, on a $\varphi(pn) = p\varphi(n)$.

Ex 3 - 2

Soit $f \in \mathrm{Hom}(G, G')$. Sans supposer les groupes cycliques, l'ordre k de $f(G)$ divise les ordres de G et de G' (1-9, cor. 1). Il divise donc $d = \mathrm{pgcd}(n, m)$. De plus, supposons G cyclique et soit a un générateur de G. Alors $f(a)$ engendre $f(G)$.

Réciproquement, considérons un diviseur k de d et supposons G et G' cycliques. Soit a un générateur de G. Puisque k divise m, il existe dans G' un unique sous-groupe H_k d'ordre k et il est cyclique. Puisque k divise n, pour tout choix b de l'un des $\varphi(k)$ générateurs de H_k, il existe un unique homomorphisme f de G sur H_k tel que $f(a) = b$ (3-2, prop.). On a donc exactement $\varphi(k)$ homomorphismes de G dans G' dont l'image est d'ordre k. Finalement, en utilisant 3-4, ex. 2, on voit que $\mathrm{card}\,(\mathrm{Hom}\,(G, G')) = \sum_{k|d} \varphi(k) = d$, où $d = \mathrm{pgcd}(n, m)$.

Comme $d = \mathrm{pgcd}(21, 6) = 3$ il existe 3 homomorphismes de $G = \mathbb{Z}/21\mathbb{Z}$ dans $G' = \mathbb{Z}/6\mathbb{Z}$. Comme $\overline{1}$ est un générateur de G, pour déterminer $f \in \mathrm{Hom}\,(G, G')$, on choisit un diviseur k de $d = 3$, un générateur b du sous-groupe H_k de $G' = \mathbb{Z}/6\mathbb{Z}$.
- Pour $k = 1$ on a $H_k = \{\overline{0}\}$ d'où un homomorphisme $f_1 : \overline{x} \mapsto \overline{0}$ trivial.
- Pour $k = 3$ on a $H_k = \langle \overline{2} \rangle$ qui a deux générateurs $\overline{2}, \overline{4}$. On obtient deux homomorphismes $f_2 : \overline{x} \mapsto x\overline{2}$ et $f_3 : \overline{x} \mapsto x\overline{4}$.

De même, $\mathrm{Hom}\,(\mathbb{Z}/18\mathbb{Z}, \mathbb{Z}/6\mathbb{Z})$ possède $d = 6$ éléments :

f_0 trivial d'image $H_1 = \{\overline{0}\}$,
f_1 d'image $H_2 = \langle \overline{3} \rangle = \{\overline{0}, \overline{3}\}$ tel que $f_1(\overline{1}) = \overline{3}$,
f_2, f_3 d'image $H_3 = \langle \overline{2} \rangle = \{\overline{0}, \overline{2}, \overline{4}\}$ tels que $f_2(\overline{1}) = \overline{2}$, $f_3(\overline{1}) = \overline{4}$,
f_4, f_5 d'image H_6 tels que $f_4(\overline{1}) = \overline{1}$, $f_5(\overline{1}) = \overline{5}$.

Ex 3 - 3

L'ensemble des générateurs du groupe $\mathbb{Z}/5\mathbb{Z}$ est

$$\Delta = \{\,\bar{k} \mid 0 \leqslant k \leqslant 4 \quad \text{et} \quad k \wedge 5 = 1\,\} = \{\,\bar{1},\bar{2},\bar{3},\bar{4}\,\}.$$

D'après 3-3, cor. 1, un automorphisme $\alpha \in \mathrm{Aut}\,(\mathbb{Z}/5\mathbb{Z})$ est déterminé par la donnée de $\alpha(\bar{1}) \in \Delta$. Donc $[\mathrm{Aut}\,(\mathbb{Z}/5\mathbb{Z}) : 1] = \mathrm{card}\,(\Delta) = \varphi(5) = 4$, où φ est la fonction d'Euler (voir 3-1). Les éléments de $\mathrm{Aut}\,(\mathbb{Z}/5\mathbb{Z})$ associés aux divers choix de $\alpha(\bar{1}) \in \Delta$ sont :

$$\begin{array}{llll} \alpha_1 : \overline{m} = m\bar{1} \mapsto m\bar{1} = \overline{m} & , & \alpha_2 : \overline{m} = m\bar{1} \mapsto m\bar{2} = \overline{2m}, \\ \alpha_3 : \overline{m} = m\bar{1} \mapsto m\bar{3} = \overline{3m} & , & \alpha_4 : \overline{m} = m\bar{1} \mapsto m\bar{4} = \overline{4m}. \end{array}$$

On a $\alpha_1 = \mathrm{Id}$. Posons $\alpha = \alpha_2$. On a $\alpha^2(\bar{1}) = \alpha(\alpha(\bar{1})) = \alpha(\bar{2}) = \bar{4} = \alpha_4(\bar{1})$. Donc $\alpha^2 = \alpha_4$ puisque $\bar{1}$ engendre $\mathbb{Z}/5\mathbb{Z}$. De même $\alpha^3(\bar{1}) = \alpha(\alpha^2(\bar{1})) = \alpha(\bar{4}) = \bar{8} = \bar{3} = \alpha_3(\bar{1})$ donc $\alpha^3 = \alpha_3$ et $\alpha^4 = \mathrm{Id}$. Ainsi, $\mathrm{Aut}\,(\mathbb{Z}/5\mathbb{Z}) = \{\,\mathrm{Id}, \alpha, \alpha^2, \alpha^3\,\}$ est cyclique, engendré par $\alpha = \alpha_2$. Comme $\varphi(4) = 2$ ce groupe cyclique a deux générateurs qui sont α et α^3 puisque 1 et 3 sont premiers avec l'ordre 4 de ce groupe. Plus généralement (3-2, rem.), si p est premier alors $\mathrm{Aut}\,(\mathbb{Z}/p\mathbb{Z})$ est cyclique.

Ex 3 - 4

Comme G est abélien, par récurrence sur k on obtient $(xy)^k = x^k y^k$ pour tous $x \in G$ et $y \in G$. Donc f_k est un homomorphisme. Si $x \in \mathrm{Ker}\,(f_k)$ on a $x^k = e$ donc l'ordre $o(x)$ de x divise k. Il divise n d'après le th. de Lagrange. Donc $o(x)$ divise $d = \mathrm{pgcd}(k,n)$. Réciproquement, si $o(x)$ divise d, alors $x^d = e$ et donc $x^k = e$. On voit donc que $\mathrm{Ker}\,(f_k) = \{x \in G \mid x^d = e\}$ est l'unique sous-groupe H_d de G d'ordre d (3-3, prop.). Par factorisation de f_k on obtient un isomorphisme de $G/\mathrm{Ker}\,(f_k)$ sur $f_k(G)$ donc $f_k(G)$ est l'unique sous-groupe $H_{\frac{n}{d}}$ de G dont l'ordre est $\frac{n}{d}$.

Ex 3 - 5

L'égalité des côtés $A_0A_1, \ldots, A_{n-1}A_0$ impose l'égalité des angles au centre correspondants $(\overrightarrow{OA}_0,\overrightarrow{OA}_1), \ldots, (\overrightarrow{OA}_{n-1},\overrightarrow{OA}_0)$. La somme de ces angles est 0 modulo 2π. L'affixe z de A_1 vérifie donc $z^n = 1$. C'est une racine $n^{\text{ième}}$ de 1. Elle est primitive, puisque n doit être le premier exposant pour lequel $z^n = 1$ (sinon le polygone aurait moins de n côtés). Réciproquement, tout choix d'un générateur du groupe $\mathbb{U}_n$ détermine un polygone solution. Toutefois, en raison de la symétrie du polygone par rapport à la droite (OA_0), le choix d'une racine primitive z et le choix de $\overline{z}$ conduisent au même polygone. Comme -1 n'est pas racine primitive, on a $\frac{1}{2}\varphi(n)$ polygones solutions (où φ est la fonction d'Euler).

Soit $n = 2^\alpha p^\beta q^\gamma \cdots$ la décomposition en facteurs premiers de n. On a :

$$k_n = 1 \quad \Leftrightarrow \quad 2 = \varphi(n) = 2^{\alpha-1}p^{\beta-1}(p-1)q^{\gamma-1}(q-1)\cdots$$

Un facteur de ce produit doit valoir 2 et les autres 1. Comme $p-1$, $q-1$, ... sont tous distincts, on ne peut avoir plus d'un facteur premier autre que 2 et ce ne peut être que 3, au degré un. Les seules possibilités sont $n = 2^2$, 3, $2 \times 3 = 6$.

On a $k_n = 2$ lorsque $\varphi(n) = 4 = 2^2$. On a au plus un facteur premier autre que 2 et ce ne peut être que 3, au degré un. Les seules possibilités sont $n = 2^3$, $2^2 \times 3 = 12$.

Ex 3 - 6

a) D'après le th. de Lagrange, on a $z^{[G:1]} = 1$ pour tout $z \in G$, ce qui prouve que $G \subset \mathbb{U}_n$. Comme $[G:1] = n = [\mathbb{U}_n : 1]$, on voit que $G = \mathbb{U}_n$.

b) Soit $M = \text{ppcm}(m,n)$. Puisque n divise M, la condition $z^n = 1$ implique $z^M = 1$. On a donc $\mathbb{U}_n \subset \mathbb{U}_M$ et de même $\mathbb{U}_m \subset \mathbb{U}_M$. Le sous-groupe $H = \mathbb{U}_m\mathbb{U}_n$ engendré par $\mathbb{U}_n$ et $\mathbb{U}_m$ est donc inclus dans $\mathbb{U}_M$ et fini. D'après le th. de Lagrange, les ordres n et m de $\mathbb{U}_n$ et $\mathbb{U}_m$ divisent $[H:1]$. Donc $M = \text{ppcm}(n,m)$ divise $[H:1]$. Comme on a $H \subset \mathbb{U}_M$, on a aussi $[H:1] \mid M$. Finalement, $[H:1] = M$ et $H = \mathbb{U}_M$. (3-3, cor. donne directement ce résultat, en examinant les sous-groupes de $\mathbb{U}_{mn}$.)

c) Il est nécessaire que $p \mid n$ et que $q \mid n$ et alors $\mathbb{U}_p$ et $\mathbb{U}_q$ sont des sous-groupes de $\mathbb{U}_n$, Comme $d \mapsto \mathbb{U}_d$ est un isomorphisme de l'ensembles ordonné des diviseurs de n sur l'ensemble ordonné des sous-groupes de $\mathbb{U}_n$ (3-3, cor.), les conditions $\mathbb{U}_p \cap \mathbb{U}_q = \{1\}$ et $\mathbb{U}_p\mathbb{U}_q = \mathbb{U}_n$ équivalent à $\text{pgcd}(p,q) = 1$ et $\text{ppcm}(p,q) = n$, d'où $n = pq$.

d) Soit $\alpha \in \text{Aut}(\mathbb{U}_n)$. Comme α est bijectif, $\alpha(\mathbb{U}_p)$ a le même ordre p que $\mathbb{U}_p$. Comme $\mathbb{U}_p$ est le seul sous-groupe de $\mathbb{U}_n$ d'ordre p, il est stable par α. (Autrement dit, tout sous-groupe d'un groupe cyclique est caractéristique). Par restriction, α induit un automorphisme β de $\mathbb{U}_p$. De même $\alpha(\mathbb{U}_q) = \mathbb{U}_q$ et par restriction α définit un élément γ de $\text{Aut}(\mathbb{U}_q)$. On a donc une application $\Phi : \alpha \mapsto (\beta,\gamma)$ de $\text{Aut}(\mathbb{U}_n)$ dans $\text{Aut}(\mathbb{U}_p) \times \text{Aut}(\mathbb{U}_q)$. L'application Φ est injective car tout élément de $\mathbb{U}_n$ est de la forme zz' avec $z \in \mathbb{U}_p$ et $z' \in \mathbb{U}_q$ et on a $\alpha(zz') = \beta(z)\gamma(z')$. L'application Φ est surjective car la donnée de deux automorphismes β et γ de $\mathbb{U}_p$ et $\mathbb{U}_q$ détermine un automorphisme α de $\mathbb{U}_p \times \mathbb{U}_q = \mathbb{U}_n$ en posant $\alpha(z,z') = (\beta(z),\gamma(z'))$ (facile à vérifier). On a alors $\Phi(\alpha) = (\beta,\gamma)$. Enfin Φ est un homomorphisme de groupes car la restriction de $\alpha_1 \circ \alpha_2$ au sous-groupe $\mathbb{U}_p$ est la composée $\beta_1 \circ \beta_2$ des restrictions de α_1 et α_2 et de même pour $\mathbb{U}_q$.

Ex 3 - 7

On a $851 = 23 \times 37$ et 23 et 37 sont premiers. Soit $H_1 \times H_2$ la décomposition primaire de $\mathbb{Z}/n\mathbb{Z}$. Alors H_1 est l'unique sous-groupe d'ordre 23 du groupe cyclique $\mathbb{Z}/n\mathbb{Z}$ et donc égal à $\langle 37 \rangle$ (3-3, prop.). De même, $H_2 = \langle 23 \rangle$.

D'après l'exercice précédent $A = \text{Aut}(\mathbb{Z}/n\mathbb{Z}) \simeq \text{Aut}(\mathbb{Z}/23\mathbb{Z}) \times \text{Aut}(\mathbb{Z}/37\mathbb{Z})$. D'après 3-2, rem. $\text{Aut}(\mathbb{Z}/n\mathbb{Z}) \simeq (\mathbb{Z}/22\,\mathbb{Z}) \times (\mathbb{Z}/36\,\mathbb{Z})$. En raisonnant comme dans 3-6, ex. 1, on obtient :

$$\begin{aligned} A &\simeq [(\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/11\mathbb{Z})] \times [(\mathbb{Z}/2^2\mathbb{Z}) \times (\mathbb{Z}/3^2\mathbb{Z})] \\ &\simeq (\mathbb{Z}/2\mathbb{Z}) \times [(\mathbb{Z}/2^2\mathbb{Z}) \times (\mathbb{Z}/3^2\mathbb{Z}) \times (\mathbb{Z}/11\mathbb{Z})] \simeq (\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/396\mathbb{Z}). \end{aligned}$$

Les invariants de A sont 2 , 396 .

Ex 3 - 8

Soient $x, y \in G$. Du fait que $(xy)(xy) = e$ on déduit $x(xy)(xy)y = xy$, puis $yx = xy$. Un tel groupe est donc abélien. De plus, tout élément distinct de e est d'ordre 2. D'après le th. de Cauchy (2-4, cor.) l'ordre de G est une puissance 2^k de 2. Alors G est isomorphe à un produit $(\mathbb{Z}/2^{r_1}\mathbb{Z}) \times \cdots \times (\mathbb{Z}/2^{r_s}\mathbb{Z})$. Comme tout élément de $G\backslash\{e\}$ est d'ordre 2, on a $r_1 = \cdots = r_s = 1$. Ainsi G est de la forme $(\mathbb{Z}/2\mathbb{Z})^k$. (Rappelons qu'un tel groupe est aussi isomorphe au groupe $\mathcal{P}(E)$ des parties de $E = \{1,\ldots,k\}$ muni de l'opération Δ de différence symétrique (voir 1-10, ex.).

Ex 3 - 9

Si G n'est pas cyclique, il est isomorphe à $(\mathbb{Z}/q_1\mathbb{Z}) \times \cdots \times (\mathbb{Z}/q_r\mathbb{Z})$, où $q_1 \mid \cdots \mid q_r$ sont les invariants de G et on a $r \geqslant 2$. Pour $d = r_1$, on trouve dans ce groupe au moins deux sous-groupes distincts d'ordre d : d'une part le facteur $\mathbb{Z}/q_1\mathbb{Z}$ et d'autre part l'unique sous-groupe d'ordre q_1 du facteur $\mathbb{Z}/q_2\mathbb{Z}$, associé au diviseur q_1 de q_2.

Ex 3 - 10

On a $720 = 2^4 \times 3^2 \times 5$. Les composantes primaires H, K, L de G sont des groupes abéliens d'ordres $2^4, 3^2, 5$. Le groupe H est isomorphe à $(\mathbb{Z}/2^{r_1}\mathbb{Z}) \times \cdots \times (\mathbb{Z}/2^{r_k}\mathbb{Z})$, avec $r_1 \leqslant \cdots \leqslant r_k$ et $r_1 + \cdots + r_k = 4$ puisque $[H : 1] = 2^4$, d'où les possibilités :

$$(1,1,1,1) \quad , \quad (1,1,2) \quad , \quad (2,2) \quad , \quad (1,3) \quad , \quad (4).$$

De même, K d'ordre 3^2 est isomorphe à $(\mathbb{Z}/3^2\mathbb{Z})$ ou à $(\mathbb{Z}/3\mathbb{Z}) \times (\mathbb{Z}/3\mathbb{Z})$ et $L \simeq \mathbb{Z}/5\mathbb{Z}$. On a donc 10 structures possibles pour G. En raisonnant comme dans 3-6, ex. 2, en posant $Z_k = \mathbb{Z}/k\mathbb{Z}$ le groupe G est isomorphe à l'un des 10 groupes suivants :

$$Z_2 \times Z_2 \times Z_6 \times Z_{30} \quad , \quad Z_2 \times Z_2 \times Z_2 \times Z_{90} \quad , \quad Z_2 \times Z_6 \times Z_{60} \quad , \quad Z_2 \times Z_2 \times Z_{180},$$

$$Z_{12} \times Z_{60} \quad , \quad Z_4 \times Z_{180} \quad , \quad Z_6 \times Z_{120} \quad , \quad Z_2 \times Z_3 \times Z_{120} \quad , \quad Z_3 \times Z_{240} \quad , \quad Z_{720}.$$

Ex 3 - 11

Considérons les décompositions en facteurs premiers de k et de n :

$$k = p_1^{\alpha_1} \cdots p_s^{\alpha_s} q_1^{\beta_1} \cdots q_t^{\beta_t} \qquad , \qquad n = p_1^{\gamma_1} \cdots p_s^{\gamma_s} r_1^{\delta_1} \cdots r_u^{\delta_u},$$

où $p_1, \ldots, p_s$ sont communs à k et n et où $q_1, \ldots, q_t$ (resp. $r_1, \ldots, r_u$) sont facteurs premiers de k et pas de n (resp. de n et pas de k). Pour $1 \leqslant i \leqslant s$, posons

$$\lambda_i = \min(\alpha_i, \gamma_i) \quad , \quad \mu_i = \max(\alpha_i, \gamma_i).$$

On a alors $d = p_1^{\lambda_1} \cdots p_s^{\lambda_s}$ et $m = p_1^{\mu_1} \cdots p_s^{\mu_s} q_1^{\beta_1} \cdots q_t^{\beta_t} r_1^{\delta_1} \cdots r_u^{\delta_u}$. Les composantes primaires de $\mathbb{Z}/k\mathbb{Z}, \mathbb{Z}/n\mathbb{Z}, \mathbb{Z}/d\mathbb{Z}, \mathbb{Z}/m\mathbb{Z}$ sont cycliques (3-3, prop.) donc

$$\mathbb{Z}/k\mathbb{Z} \simeq (\mathbb{Z}/p_1^{\alpha_1}\mathbb{Z}) \times \cdots \times (\mathbb{Z}/p_s^{\alpha_s}\mathbb{Z}) \times (\mathbb{Z}/q_1^{\beta_1}\mathbb{Z}) \times \cdots \times (\mathbb{Z}/q_t^{\beta_t}\mathbb{Z}),$$

$$\mathbb{Z}/n\mathbb{Z} \simeq (\mathbb{Z}/p_1^{\gamma_1}\mathbb{Z}) \times \cdots \times (\mathbb{Z}/p_s^{\gamma_s}\mathbb{Z}) \times (\mathbb{Z}/r_1^{\delta_1}\mathbb{Z}) \times \cdots \times (\mathbb{Z}/r_u^{\delta_u}\mathbb{Z}),$$

$$\mathbb{Z}/d\mathbb{Z} \simeq (\mathbb{Z}/p_1^{\lambda_1}\mathbb{Z}) \times \cdots \times (\mathbb{Z}/p_s^{\lambda_s}\mathbb{Z}),$$

$$\mathbb{Z}/m\mathbb{Z} \simeq (\mathbb{Z}/p_1^{\mu_1}\mathbb{Z}) \times \cdots \times (\mathbb{Z}/p_s^{\mu_s}\mathbb{Z}) \times (\mathbb{Z}/q_1^{\beta_1}\mathbb{Z}) \times \cdots \times (\mathbb{Z}/r_u^{\delta_u}\mathbb{Z}).$$

Pour $1 \leqslant i \leqslant s$, le produit $(\mathbb{Z}/p_i^{\alpha_i}\mathbb{Z}) \times (\mathbb{Z}/p_i^{\gamma_i}\mathbb{Z})$ est isomorphe à $(\mathbb{Z}/p_i^{\lambda_i}\mathbb{Z}) \times (\mathbb{Z}/p_i^{\mu_i}\mathbb{Z})$ car $\{\alpha_i, \gamma_i\} = \{\lambda_i, \mu_i\}$ donc $(\mathbb{Z}/k\mathbb{Z}) \times (\mathbb{Z}/n\mathbb{Z})$ et $(\mathbb{Z}/d\mathbb{Z}) \times (\mathbb{Z}/m\mathbb{Z})$ sont isomorphes.

En outre, $(\mathbb{Z}/d\mathbb{Z}) \times (\mathbb{Z}/m\mathbb{Z})$ est l'expression canonique du groupe G et d, m sont ses invariants car $d \mid m$, d'où l'unicité de cette expression de G.

Comme $\text{pgcd}(18,45) = 9$ et $\text{ppcm}(18,45) = 90$, les invariants de $(\mathbb{Z}/18\mathbb{Z}) \times (\mathbb{Z}/45\mathbb{Z})$ sont $9, 90$. (Cette méthode donne aussi la solution de 3-6, Ex. 1.)

Ex 3 - 12

Puisque $o(e) = 1$, on a $e \in T$. Soient $x, y \in T$ d'ordres k, $m \in \mathbb{N}^*$. On a $(xy)^{km} = (x^k)^m (y^m)^k = e$ donc $xy \in T$. Comme $o(x^{-1}) = o(x)$, on a $x^{-1} \in T$. Ainsi, T est un sous-groupe de G. Considérons l'application canonique $\varphi : G \to G/T$. Soit $a \in G/T$, d'ordre fini $s \in \mathbb{N}^*$. Il existe $x \in G$ tel que $a = \varphi(x)$. On a $\varphi(x^s) = a^s = e$ et donc $x^s \in T = \mathrm{Ker}\,(\varphi)$. Il existe donc $r \in \mathbb{N}^*$ tel que $x^{sr} = (x^s)^r = e$, ce qui prouve que $x \in T$ et donc que $a = \varphi(x) = e$. Cela montre que G/T est sans torsion.

Ex 3 - 13

D'après 3-7, cor. 2, K est résoluble. Il en est de même pour H abélien donc G est résoluble (3-7, cor. 1). On a $[G : 1] = \mathrm{card}\,(H \times K) = np^m$ où $n = [H : 1]$. Tout diviseur de $[G : 1]$ est de la forme dp^s, où d divise n et où $s \leqslant m$. Dans le groupe cyclique H, il existe un unique sous-groupe H_1 d'ordre d. Il est caractéristique (invariant par tout automorphisme de H) en raison de son unicité. Comme on a $H \triangleleft G$, on voit que $H_1 \triangleleft G$. Il existe dans K un sous-groupe (distingué) K_1 d'ordre p^s (3-7, cor. 2). D'après le th. de Noether H_1K_1 est un sous-groupe de G. Comme $(h, k) \mapsto hk$ est bijective de $H \times K$ sur G, l'ordre de H_1K_1 est dp^s.

Ex 3 - 14

a) L'ensemble $\mathcal{F}(G, \mathbb{C}^*)$ des applications de G dans $\mathbb{C}^*$ s'identifie avec le groupe $(\mathbb{C}^*)^G$. Le lecteur vérifiera que $\widehat{G}$ est un sous-groupe de $(\mathbb{C}^*)^G$.

b) Si $[G : 1] = n$, pour tout $g \in G$ on a $g^n = e$ (th. de Lagrange) et donc $\chi(g)^n = \chi(g^n) = 1$ pour tout $\chi \in \widehat{G}$. Ainsi $\chi(g) \in \mathbb{U}_n$ pour tout $g \in G$ et pour tout $\chi \in \widehat{G}$.

c) Si $G = \mathbb{U}_n$, il est engendré par $\zeta = \exp \frac{2i\pi}{n}$. Un caractère χ est déterminé par la donnée de $\alpha = \chi(\zeta) \in \mathbb{U}_n$. De plus, pour tout choix de $\alpha \in \mathbb{U}_n$, il existe $\chi \in \mathrm{Hom}\,(\mathbb{U}_n, \mathbb{U}_n)$ tel que $\chi(\zeta) = \alpha$ (3-2, cor. 1). Ainsi, $\widehat{\mathbb{U}}_n$ possède n éléments. (On a vu dans Ex. 3-2 que $\mathrm{card}\,(\mathrm{Hom}\,(\mathbb{U}_n, \mathbb{U}_n)) = n$). Si χ_0 est le caractère $\mathrm{Id} : z \mapsto z$, défini par $\chi_0(\zeta) = \zeta$, alors pour $k = 1, 2, \ldots, n-1$ le caractère χ_0^k est le caractère de G tel que $\chi_0^k(\zeta) = \zeta^k = \exp \frac{2ik\pi}{n}$. Ainsi, les puissances de χ_0 donnent tous les éléments de $\widehat{G}$. Ce groupe est donc cyclique, d'ordre n. Il est isomorphe à $\mathbb{U}_n$.

d) Identifions G_1 et G_2 avec les sous-groupes $G_1 \times \{e\}$ et $\{e\} \times G_2$ de G. Par restriction, tout $\chi \in \widehat{G}$ induit des caractères χ_1 et χ_2 de G_1 et G_2. L'application $f : \chi \mapsto (\chi_1, \chi_2)$ est injective car tout $g \in G$ s'écrit de manière unique $g = g_1g_2$ et donc $\chi(g) = \chi_1(g_1)\chi_2(g_2)$. Elle est surjective : pour tout $(\chi_1, \chi_2) \in \widehat{G}_1 \times \widehat{G}_2$, la formule $\chi(g) = \chi_1(g_1)\chi_2(g_2)$ définit un caractère sur G. Enfin f est un homomorphisme car pour tout $\chi \in \widehat{G}$ et pour tout $\chi' \in \widehat{G}$, la restriction de $\chi\chi'$ à G_1 (resp. G_2) est le produit des deux restrictions. Ainsi, f est un isomorphisme.

e) Soit G un groupe abélien fini et soient $q_1 \mid \cdots \mid q_k$ les invariants de G. Considérons sa décomposition cyclique canonique $G = G_1 \times \cdots \times G_k$, avec $G_1 \simeq \mathbb{Z}/q_1\mathbb{Z}$, …, $G_k \simeq \mathbb{Z}/q_k\mathbb{Z}$. En utilisant d) et c), on voit que $\widehat{G}$ est isomorphe à $\widehat{G}_1 \times \cdots \times \widehat{G}_k$ avec $\widehat{G}_1 \simeq \mathbb{Z}/q_1\mathbb{Z}, \ldots, G_k \simeq \mathbb{Z}/q_k\mathbb{Z}$. Donc $\widehat{G}$ est isomorphe à G (il a les mêmes invariants).

Chapitre 4

Le groupe symétrique

4.1 Décomposition d'une permutation en cycles

Soit E un ensemble fini ayant n éléments. Quitte à numéroter ses éléments, on peut supposer que $E = \{1, \dots, n\}$. Les bijections de E sur E sont appelées les *permutations* de E. Le groupe $\mathcal{S}_n$ des permutations de E est le *groupe symétrique*. Pour définir un élément s de $\mathcal{S}_n$, le plus simple est de donner le tableau de ses valeurs :

$$s = \begin{pmatrix} 1 & 2 & \dots & n \\ s(1) & s(2) & \dots & s(n) \end{pmatrix}.$$

On appelle *support* de s l'ensemble des éléments $k \in E$ tels que $s(k) \neq k$.

On appelle *cycle*, un élément c de $\mathcal{S}_n$ qui permute circulairement certains éléments $i_1, i_2, \dots, i_k$ de E et qui laisse fixes les autres éléments de E :

$$c(i_1) = i_2 \quad , \quad c(i_2) = i_3 \quad , \dots , \quad c(i_{k-1}) = i_k \quad , \quad c(i_k) = i_1 .$$

La partie $\{i_1, i_2, \dots, i_k\}$ de E est le support de ce cycle. Le cardinal k du support s'appelle la *longueur* du cycle. On note $(i_1, i_2, \dots, i_k)$ ce cycle. Cette notation de c n'est pas unique, puisqu'on peut commencer par n'importe quel élément de son support. On a $c^k(i_p) = i_p$ pour $1 \leqslant p \leqslant k$ et k est le plus petit entier strictement positif tel que $c^k = \mathrm{Id}_E$. L'ordre de c dans le groupe $\mathcal{S}_n$ est donc la longueur k du cycle.

Deux cycles c, c' sont dits *disjoints* si leurs supports sont des parties disjointes de E. Dans ce cas on a $c\,c' = c'\,c$.

Un cycle de longueur 2, de support $\{i, j\}$, est appelé une *transposition* et sera noté $[i, j]$. Nous appellerons *transpositions simples* les $n-1$ transpositions $t_i = [i, i+1]$, où $i = 1, \dots, n-1$, qui échangent deux entiers consécutifs.

Proposition.

Tout $s \in \mathcal{S}_n$ est de manière unique un produit $s = c_1 \cdots c_p$ de cycles disjoints. L'ordre de s est le ppcm *des ordres de $c_1, \dots, c_p$.*

Démonstration. Nous avons vu en 1-14 que $k \mapsto s^k$ est un homomorphisme du groupe additif $\mathbb{Z}$ dans $\mathcal{S}_n$. C'est une action de $\mathbb{Z}$ sur l'ensemble $E = \{1, \dots, n\}$. Soient $O_1, \dots, O_p$ les orbites qui ne sont pas réduites à un point, c'est-à-dire les orbites des éléments du support de s. Considérons $i_1 \in O_1$. Son stabilisateur est un sous-groupe de $\mathbb{Z}$ et donc de la forme $k\mathbb{Z}$. Les éléments de O_1 sont i_1, $i_2 = s(i_1)$, $i_3 = s(i_2) = s^2(i_1), \dots, i_k = s(i_{k-1}) = s^{k-1}(i_1)$. D'après 2-2, prop. (iii), ces éléments sont associés bijectivement aux classes de $\mathbb{Z}$ modulo le stabilisateur $k\mathbb{Z}$ et sont donc

distincts. On a $s^k(i_1) = i_1$. L'action de s sur l'orbite O_1 est la même que celle du cycle $c_1 = (i_1, \dots, i_k)$. Il existe de même des cycles $c_2, \dots, c_p$ ayant pour supports les orbites $O_2, \dots, O_p$ et ayant la même action que s sur ces orbites. Les cycles $c_1, \dots, c_p$ commutent car ils sont disjoints et $(c_1 \cdots c_p)(i) = s(i)$ pour tout point i du support $\bigcup_{m=1}^{p} O_m$ de s. Les autres éléments de E sont fixes par s et $c_1 \cdots c_p$ donc $s = c_1 \cdots c_p$.

Montrons l'unicité de l'expression $s = c_1 \cdots c_p$ par récurrence sur p. Si $p = 0$, c'est-à-dire si $s = \mathrm{Id}_E$, l'unicité est évidente. Soit $p \geqslant 1$. Supposons acquise l'unicité pour les permutations pouvant s'exprimer comme produit de moins de p cycles disjoints. Considérons le cas où s est le produit $s = c_1 \cdots c_p$ de p cycles disjoints. Soit $s = c'_1 \cdots c'_q$ une autre décomposition de s en cycles disjoints et soit i un élément du support O_1 de c_1. Il appartient au support d'un des cycles c'_j et à un seul. Quitte à changer la numérotation, on peut supposer que i appartient au support de c'_1. On a $s^r(i) = c_1^r(i) = {c'}_1^r(i)$ pour tout $r \in \mathbb{Z}$. On voit donc que $c_1 = c'_1$. Simplifions par c_1 la relation $c_1 c_2 \cdots c_p = c_1 c'_2 \cdots c'_q$. On obtient $c_2 \cdots c_p = c'_2 \cdots c'_q$. D'après l'hypothèse de récurrence, on a $q = p$ et $\{c_2, \dots, c_p\} = \{c'_2, \dots, c'_p\}$, d'où l'unicité de l'expression.

Puisque les cycles commutent, on a $s^n = c_1^n \cdots c_p^n$ pour tout $n \in \mathbb{N}$. Les supports étant disjoints, $s^n = \mathrm{Id}_E$ si et seulement si $c_1^n = \mathrm{Id}_E, \dots, c_p^n = \mathrm{Id}_E$, c'est-à-dire si n est multiple commun des ordres $k_1, \dots, k_p$ de $c_1, \dots, c_p$. Le plus petit entier strictement positif n tel que $s^n = \mathrm{Id}_E$ est donc $\mathrm{ppcm}(k_1, \dots, k_p)$. ∎

Exercice. Utiliser l'algorithme décrit dans la démonstration précédente pour décomposer en cycles disjoints $s = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 7 & 5 & 1 & 9 & 4 & 6 & 3 & 8 & 2 \end{pmatrix}$.

Solution. $s(1) = 7$, $s(7) = 3$, $s(3) = 1$ d'où un cycle $c_1 = (1,7,3)$.
$s(2) = 5$, $s(5) = 4$, $s(4) = 9$, $s(9) = 2$ d'où un cycle $c_2 = (2,5,4,9)$.
Comme $s(6) = 6$ et $s(8) = 8$, on a $s = c_1 c_2$. L'ordre de s est $\mathrm{ppcm}\,(3,4) = 12$.

4.2 Cycles conjugués

Proposition.

Soient $c = (i_1, \dots, i_k)$ un cycle de longueur k et $s \in \mathcal{S}_n$. Alors scs^{-1} est le cycle $c' = (s(i_1), \dots, s(i_k))$. Tout cycle de longueur k est un conjugué de c.

Démonstration. Soient $A = \{i_1, \dots, i_k\}$ le support de c et $p \in \{1, \dots, n\}$.
Si $p = s(i_j) \in s(A)$, on a $scs^{-1}(s(i_j)) = s(c(i_j)) = s(i_{j+1}) = c'(s(i_j))$.
Si $p \notin s(A)$, alors $s^{-1}(p) \notin A$ et $scs^{-1}(p) = s(c(s^{-1}(p))) = s(s^{-1}(p)) = p = c'(p)$.
Ainsi $scs^{-1} = c'$. Soit $c_1 = (j_1, \dots, j_k)$ un cycle de longueur k, de support A_1. Les complémentaires $\overline{A}, \overline{A_1}$ des supports de c et c_1 ayant le même cardinal $n - k$, il existe une bijection s de $\overline{A}$ sur $\overline{A_1}$. Posons $s(i_r) = j_r$ pour $r = 1, \dots, k$. On obtient une permutation $s \in \mathcal{S}_n$ et on a $scs^{-1} = c_1$ d'après ce qui précède. ∎

Corollaire 1.

Soient $[i,j]$ une transposition et $s \in \mathcal{S}_n$. On a $s[i,j]s^{-1} = [s(i), s(j)]$. Le groupe $\mathcal{S}_n$ agit transitivement par conjugaison sur l'ensemble des transpositions.

Démonstration. c'est ce que dit la proposition pour $k = 2$. ∎

Corollaire 2.

Toute transposition $[i,j]$, *où* $i<j$, *est conjuguée d'une transposition simple :*

$$[i,j] = c\,[j-1,j]\,c^{-1} \qquad \text{où} \qquad c = (i\,,i+1\,,\ldots,j-1)\,.$$

4.3 Générateurs du groupe symétrique

Proposition.

(i) *Toute permutation* $s\in\mathcal{S}_n$ *est produit de transpositions.*

(ii) *Les transpositions simples* $t_i=[i\,,i+1]$, *où* $1\leqslant i\leqslant n-1$, *engendrent* $\mathcal{S}_n$.

(iii) *Les deux permutations* $t_1=[1\,,2]$ *et* $c=(1,2,\ldots,n)$ *engendrent* $\mathcal{S}_n$.

Démonstration. (i) Compte tenu de 4-1, il suffit de montrer que tout cycle $(i_1,\ldots,i_p)$ est produit de transpositions. Vérifions par récurrence sur la longueur p du cycle, que

$$(1) \qquad (i_1,\ldots,i_p) = [i_1\,,i_2]\,[i_2\,,i_3]\cdots[i_{p-1}\,,i_p]\,.$$

Cette formule est vraie pour $p=2$. Considérons $p>2$. Admettons la formule à l'ordre $p-1$. On a alors $(i_1,\ldots,i_{p-1}) = [i_1\,,i_2]\,[i_2\,,i_3]\cdots[i_{p-2}\,,i_{p-1}]$, d'où

$$[i_1\,,i_2][i_2\,,i_3]\cdots[i_{p-1}\,,i_p] = (i_1,\ldots,i_{p-1})[i_{p-1}\,,i_p] = (i_1\,,\ldots,i_p)\,.$$

(ii) Compte tenu de (i), il suffit de démontrer que toute transposition $[i\,,j]$, où $i<j$, est un produit de transpositions simples. Or, d'après 4-2, cor. 2,

$$(2) \qquad [i\,,j] = c\,[j-1\,,j]\,c^{-1} \quad \text{avec} \quad c = (i,i+1,\ldots,j-1)\,.$$

D'après (1), $c = (i,i+1,\ldots,j-1) = [i\,,i+1]\,[i+1\,,i+2]\cdots[j-2\,,j-1]$ est un produit de transpositions simples et $c^{-1} = [j-2\,,j-1]\cdots[i\,,i+1]$ également.

(iii) Le sous-groupe $\langle t_1,c\rangle$ de $\mathcal{S}_n$ contient $c\,[1\,,2]\,c^{-1}=[2\,,3]=t_2$, $c\,t_2\,c^{-1}=t_3$, …, $c\,t_{n-2}\,c^{-1}=t_{n-1}$. D'après (ii), ce sous-groupe est égal à $\mathcal{S}_n$. ∎

4.4 Signature d'une permutation

Définitions

On dit que $s\in\mathcal{S}_n$, *présente une inversion en* (i,j), *où* $1\leqslant i<j\leqslant n$, *si on a* $s(i)>s(j)$. *Notons* N_s *le nombre d'inversions que présente* s. *L'entier* $\varepsilon(s)=(-1)^{N_s}$ *est appelé la signature de* s.

Si $\varepsilon(s)=+1$, *on dit que la permutation* s *est paire. Si* $\varepsilon(s)=-1$, *on dit que* s *est impaire. Nous allons voir que l'ensemble* A_n *des permutations paires est un sous-groupe distingué de* $\mathcal{S}_n$. *On l'appelle le groupe alterné.*

Proposition.

L'application $\varepsilon : s\mapsto\varepsilon(s)$ *est un homomorphisme surjectif du groupe* $\mathcal{S}_n$ *sur* $\{1,-1\}$ *et c'est le seul homomorphisme surjectif de* $\mathcal{S}_n$ *sur* $\{1,-1\}$. *Si* $s=t_1\cdots t_k$ *est produit de* k *transpositions, on a* $\varepsilon(s)=(-1)^k$.

Démonstration. Soient $s,t\in\mathcal{S}_n$. Montrons que $\varepsilon(st)=\varepsilon(s)\varepsilon(t)$. Répartissons les C_n^2 couples (i,j), où $1\leqslant i<j\leqslant n$, en quatre classes selon que :

- $t(i)<t(j)$ et $s(t(i))<s(t(j))$ (soit N_1 le nombre de couples (i,j) concernés),

- $t(i) < t(j)$ et $s(t(i)) > s(t(j))$ (soit N_2 le nombre de couples (i,j) concernés),
- $t(i) > t(j)$ et $s(t(i)) < s(t(j))$ (soit N_3 le nombre de couples (i,j) concernés),
- $t(i) > t(j)$ et $s(t(i)) > s(t(j))$ (soit N_4 le nombre de couples (i,j) concernés).

On a $N_{st} = N_2 + N_4$, $N_t = N_3 + N_4$, $N_s = N_2 + N_3$. Pour calculer N_s , on s'appuie sur le fait que t étant bijective, si $\{i,j\}$ décrit toutes les parties à deux éléments, alors $\{t(i),t(j)\}$ décrit toutes les parties à deux éléments. On en déduit

$$\varepsilon(s)\varepsilon(t) = (-1)^{N_2+N_3}(-1)^{N_3+N_4} = (-1)^{N_2+N_4} = \varepsilon(st)\,.$$

Ainsi ε est un homomorphisme de groupes.

Si $t = [i\,,i+1]$ est une transposition simple, alors $(i,i+1)$ est le seul couple qui présente une inversion. Donc $\varepsilon(t) = -1$ et ε est surjectif.

Toute transposition $[i\,,j]$ a pour signature -1 . En effet d'après 4-3, relation (2),

$$[i\,,j] = c\,[j-1\,,j]\,c^{-1}\,, \quad \text{donc} \quad \varepsilon([i\,,j]) = \varepsilon(c)\varepsilon([j-1\,,j])\varepsilon(c)^{-1} = \varepsilon([j-1\,,j]) = -1\,.$$

Si $s = t_1 \cdots t_k$ est produit de k transpositions, on a donc $\varepsilon(s) = \varepsilon(t_1)\cdots\varepsilon(t_k) = (-1)^k$.

Soit φ un homomorphisme surjectif de $\mathcal{S}_n$ sur $\{1,-1\}$. Montrons que $\varphi = \varepsilon$. Il existe une transposition t telle que $\varphi(t) = -1$, sinon on aurait $\varepsilon(t) = 1$ pour toute transposition t et ensuite pour tout $s \in \mathcal{S}_n$, puisque s est produit de transpositions, contredisant la surjectivité de φ . D'après 4-2, cor. 1, toute autre transposition est une conjuguée $t' = sts^{-1}$ de t . On a $\varphi(t') = \varphi(s)\varphi(t)\varphi(s)^{-1} = \varphi(t) = -1 = \varepsilon(t')$. Tout $s \in \mathcal{S}_n$ étant un produit $s = t_1 \cdots t_k$ de transpositions, il vient $\varphi(s) = (-1)^k = \varepsilon(s)$. ∎

Corollaire 1.

L'ensemble A_n des permutations paires est un sous-groupe caractéristique de $\mathcal{S}_n$, d'indice 2 . C'est le seul sous-groupe d'indice 2 de $\mathcal{S}_n$.

Démonstration. Considérons $\alpha \in \mathrm{Aut}\,(\mathcal{S}_n)$. Alors $\varepsilon \circ \alpha$ est un homomorphisme surjectif de $\mathcal{S}_n$ sur $\{1,-1\}$. D'après la proposition, il est égal à ε . On en déduit que $\alpha(s)$ et s ont la même signature, pour tout $s \in \mathcal{S}_n$ et donc que $\alpha(A_n) = A_n$. L'homomorphisme surjectif $\varepsilon : \mathcal{S}_n \mapsto \{1,-1\}$ a pour noyau A_n . Par factorisation, il définit un isomorphisme $\bar{\varepsilon}$ de $\mathcal{S}_n/\mathcal{A}_n$ sur $\{1,-1\}$ donc $[\mathcal{S}_n : A_n] = 2$.
Soit H un sous-groupe d'indice 2 de $\mathcal{S}_n$. Il est distingué (1-8, cor.). Soit $\varphi : \mathcal{S}_n \to \mathcal{S}_n/H$ l'homomorphisme canonique. Il existe un isomorphisme θ de $\mathcal{S}_n/H$ sur $\{1,-1\}$. D'après la proposition, $\theta \circ \varphi = \varepsilon$ donc $H = \mathrm{Ker}\,(\theta \circ \varphi) = \mathrm{Ker}\,(\varepsilon) = \mathcal{A}_n$. ∎

Corollaire 2.

Dans les diverses expressions $s = t_1 \cdots t_k$ d'une permutation $s \in \mathcal{S}_n$ comme produit de transpositions, l'entier k a toujours la même parité.

Démonstration. Si $s = t_1 \cdots t_k = t'_1 \cdots t'_m$ sont deux expressions de s , alors on a $\varepsilon(s) = (-1)^k = (-1)^m$. Donc k et m ont la même parité. ∎

Corollaire 3.

La signature d'un cycle $c = (i_1,\ldots,i_k)$ de longueur k est $(-1)^{k-1}$. La signature de tout $s \in \mathcal{S}_n$ se déduit de la décomposition de s en cycles disjoints.

Démonstration. D'après 4-3, relation (1), le cycle c est produit de $k-1$ transpositions donc $\varepsilon(c) = (-1)^{k-1}$. ∎

Exercice. Pour $n \geqslant 3$, montrer que les $n-2$ cycles $c_3 = (1,2,3)$, $c_4 = (1,2,4)$, $\ldots$, $c_n = (1,2,n)$ engendrent $\mathcal{A}_n$.

Solution. Les cycles $c_3, \ldots, c_n$ ont pour signature $(-1)^2 = 1$. Le sous-groupe H qu'ils engendrent est donc contenu dans $\mathcal{A}_n$. Montrons que $\mathcal{A}_n \subset H$ par récurrence sur n . Pour $n = 3$, on a $\mathcal{A}_3 = \{ \mathrm{Id}\, , c_3 , c_3^2 \} \subset H$.

Soit $n > 3$. Admettons le résultat pour le groupe $\mathcal{A}_{n-1}$. Considérons $s \in \mathcal{A}_n$.

1- Si $s(n) = n$, la restriction s' de s à $\{1, \ldots, n-1\}$ est un élément de $\mathcal{S}_{n-1}$ et c'est un élément de $\mathcal{A}_{n-1}$. D'après l'hypothèse de récurrence, s' (et donc s) s'exprime comme produit de cycles $c_3, \ldots, c_{n-1}$ et d'inverses de ces cycles.

2- Si $s(n) = k \neq n$, alors $c_n^2 c_k s \in \mathcal{A}_n$ et $c_n^2 c_k s(n) = n$. D'après le cas 1, $c_n^2 c_k s \in H$ et donc $s \in H$.

4.5 Non résolubilité du groupe des permutations

Le groupe $\mathcal{S}_2$ se compose de Id et $[1,2]$. Il est isomorphe à $\mathbb{Z}/2\mathbb{Z}$ abélien.

Le groupe $\mathcal{S}_3$ est d'ordre $3! = 6$. Le sous-groupe distingué $\mathcal{A}_3$, d'indice 2 , est d'ordre 3 premier. Il est cyclique, isomorphe à $\mathbb{Z}/3\mathbb{Z}$. Puisque $c = (1,2,3)$ et c^2 sont des permutations paires, on a $\mathcal{A}_3 = \{ \mathrm{Id}\, , c , c^2 \}$. Les 3 permutations impaires sont les trois transpositions $[1,2]$, $[2,3]$, $[1,3]$. Le quotient $\mathcal{S}_3/\mathcal{A}_3$ isomorphe à l'image $\{1,-1\}$ de ε , est abélien. Le groupe $\mathcal{S}_3$ est donc résoluble. Pour tout choix d'une transposition t l'application θ de $\{1,-1\}$ dans $\mathcal{S}_3$ définie par $\theta(1) = \mathrm{Id}$, $\theta(-1) = t$, est un isomorphisme de $\{1,-1\}$ sur le sous-groupe $K = \{ \mathrm{Id}, t\}$ de $\mathcal{S}_3$, avec $\varepsilon \circ \theta = \mathrm{Id}_{\{1,-1\}}$, donc $\mathcal{S}_3$ est un produit semi-direct de $\mathcal{A}_3 \simeq \mathbb{Z}/3\mathbb{Z}$ par $K \simeq \mathbb{Z}/2\mathbb{Z}$ (voir 2-7, ex. 1).

Le groupe $\mathcal{S}_4$ est d'ordre $4! = 24$. Le sous-groupe $\mathcal{A}_4$ d'indice 2 est d'ordre 12 . Il a un sous-groupe H d'ordre 4 évident, d'éléments Id , $[1,2]\,[3,4]$, $[1,3]\,[2,4]$, $[1,4]\,[2,3]$, isomorphe au groupe des 4 isométries du plan euclidien laissant stable un rectangle de sommets $\{1,2,3,4\}$ (petit groupe de Klein). D'après 4-2, cor. 1, pour tout $s \in \mathcal{S}_4$ et pour tout $s' \in H$, $ss's^{-1}$ est un autre élément de H . Donc, H est distingué dans $\mathcal{S}_4$ et dans $\mathcal{A}_4$. Les sous-groupes $\{ \mathrm{Id} \} \subset H \subset \mathcal{A}_4 \subset \mathcal{S}_4$, de $\mathcal{S}_4$ sont distingués, avec quotient d'ordre 4 ou premier et donc abélien. Le groupe $\mathcal{S}_4$ est résoluble.

Proposition.

Pour $n \geqslant 5$, le groupe $\mathcal{S}_n$ n'est pas résoluble. Pour $0 \leqslant n \leqslant 4$, il est résoluble.

Démonstration. Posons $\mathcal{S}_n = G$. Supposons $n \geqslant 5$. Considérons cinq éléments i,j,k,l,m de $\{1, \ldots, n\}$, les cycles $c_1 = (i,j,k)$ et $c_2 = (k,l,m)$. En examinant les images de i,j,k,l,m , on vérifie que $c_1 c_2 c_1^{-1} c_2^{-1} = (i,l,k)$. On voit que le sous-groupe dérivé G' , engendré par les commutateurs $ss's^{-1}s'^{-1}$, contiendra tout cycle (i,l,k) de longueur 3 . On en déduit ensuite que le groupe G'' dérivé de G' , contient tous les 3-cycles et par récurrence que tous les groupes dérivés $G^{(k)}$ de G contiennent tous les 3-cycles. Il n'existe donc pas d'entier k tel que $G^{(k)} = \{e\}$. ∎

Remarques. En fait (voir Ex. 4-11), pour $n \geqslant 5$, le groupe $\mathcal{A}_n$ est simple (sans autre sous-groupe distingué que $\mathcal{A}_n$ et $\{e\}$). De ce fait, $\mathcal{S}_n$ ne peut être résoluble, sinon le sous-groupe $\mathcal{A}_n$ serait résoluble. On aurait donc $(\mathcal{A}_n)' \neq \mathcal{A}_n$, d'où $(\mathcal{A}_n)' = \{e\}$ puisque $\mathcal{A}_n$ est simple. Cela signifierait que $\mathcal{A}_n$ est commutatif. C'est absurde.

Exercices du chapitre 4

Ex 4 - 1

Pour $n \geqslant 3$, déterminer le centre Z du groupe $\mathcal{S}_n$.

Ex 4 - 2

Montrer que $\mathrm{Aut}(\mathcal{S}_3) = \mathrm{Int}(\mathcal{S}_3)$ et que $\mathrm{Aut}(\mathcal{S}_3) \simeq \mathcal{S}_3$.

Ex 4 - 3

Montrer qu'il n'existe pas d'homomorphisme surjectif de $\mathcal{S}_3$ sur $\mathcal{A}_3$.

Ex 4 - 4

Dans le groupe $\mathcal{S}_n$, où $n \geqslant 3$, on note $t_1, \ldots, t_{n-1}$ les $n-1$ transpositions simples $[1,2], \ldots, [n-1,n]$.

a) Pour $i \neq j$, montrer que $t_i t_j = t_j t_i$ si et seulement si $|j-i| \geqslant 2$.

b) Montrer que $t_i t_{i+1} t_i = t_{i+1} t_i t_{i+1}$ pour $i = 1, \ldots, n-1$.

Ex 4 - 5

Dans $\mathcal{S}_n$, où $n \geqslant 2$, on considère un cycle c de longueur $k \geqslant 2$ et le sous-groupe $H = \langle c \rangle$ de $\mathcal{S}_n$ engendré par c.

a) Quel est le cardinal de l'ensemble des conjugués de c (orbite de c) dans $\mathcal{S}_n$.

b) Montrer qu'il y a trois classes de conjugaison dans $\mathcal{S}_3$ et cinq dans $\mathcal{S}_4$.

c) Calculer l'ordre du commutant H' de H dans $\mathcal{S}_n$.

d) Si $c = (1, \ldots, n)$, montrer que $H = \langle c \rangle$ est un sous-groupe abélien maximal de $\mathcal{S}_n$. Calculer le cardinal de l'ensemble des conjugués de H dans $\mathcal{S}_n$.

Ex 4 - 6

Déterminer la signature de

$$s = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 4 & 5 & 6 & 3 & 2 & 1 \end{pmatrix}$$

et donner une expression de s comme produit de transpositions simples.

Ex 4 - 7

Pour $n \geqslant 3$, montrer que $\mathcal{A}_n$ est le groupe dérivé de $\mathcal{S}_n$.

Ex 4 - 8

Montrer que les $n-1$ transpositions $\tau_i = [1,i]$, où $2 \leqslant i \leqslant n$, constituent un système de générateurs de $\mathcal{S}_n$.

Ex 4 - 9

a) Soit $n \geqslant 3$. Montrer que les $n-2$ cycles $c_i = (i, i+1, i+2)$, où $1 \leqslant i \leqslant n-2$, constituent un système de générateurs du groupe alterné $\mathcal{A}_n$.

b) Pour $i = 1, \ldots, n-1$, posons $t_i = [i, i+1]$. Calculer le commutateur $t_{i+1} t_i t_{i+1}^{-1} t_i^{-1}$. Retrouver ainsi le résultat de l'exercice 4-7.

Ex 4 - 10

Pour $n \geqslant 5$, montrer que les 3-cycles sont conjugués dans $\mathcal{A}_n$. Pour $n = 3$ ou 4, montrer que cette propriété est fausse.

Ex 4 - 11

On veut montrer que pour $n \geqslant 5$ le groupe $\mathcal{A}_n$ est simple (que ses seuls sous-groupes distingués sont $\{\mathrm{Id}\}$ et $\mathcal{A}_n$). Considérons $H \lhd \mathcal{A}_n$ tel que $H \neq \{\mathrm{Id}\}$.

a) Soit $s \in H$ avec $s \neq \mathrm{Id}$. On choisit $x \in E = \{1, \ldots, n\}$ tel que $y = s(x) \neq x$, puis $z \in E \setminus \{x, y, s(y)\}$. On considère le 3-cycle $c = (x, z, y)$ et le commutateur $\rho = [s, c]$. Montrer que $\rho \in H$, que $\rho \neq \mathrm{Id}$ et que ρ laisse fixes au moins $n-5$ éléments de E.

b) Si ρ n'est pas un 3-cycle, décomposer ρ en cycles disjoints. En considérant un commutateur de ρ avec une transposition $t = [\alpha, \beta]$ convenable, montrer que H contient un 3-cycle.

c) En déduire le résultat annoncé.

d) Pour $n \geqslant 5$, quels sont les sous-groupes distingués de $\mathcal{S}_n$?

Ex 4 - 12

Montrer que dans le groupe $\mathcal{A}_4$ il n'existe pas de sous-groupe d'ordre 6, bien que 6 divise l'ordre de $\mathcal{A}_4$.

Ex 4 - 13

a) Montrer que dans $\mathcal{A}_4$ il existe un unique sous-groupe H isomorphe à $(\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/2\mathbb{Z})$ et que H est un sous-groupe caractéristique de $\mathcal{S}_4$.

b) Montrer qu'il existe dans $\mathcal{S}_4$ deux sous-groupes d'ordre $2^2 = 4$ qui ne sont pas conjugués.

Indications

Ex 4 - 1

$Z = \{ \mathrm{Id} \}$ (raisonner par l'absurde).

Ex 4 - 2

Montrer que tout $\alpha \in \mathrm{Aut}(\mathcal{S}_3)$ permute les transpositions.

Ex 4 - 3

Si $f \in \mathrm{Hom}(\mathcal{S}_3, \mathcal{A}_3)$ examiner $f(t)$ lorsque t est une transposition.

Ex 4 - 4

Il est commode d'utiliser le fait que $t[i,j]t^{-1} = [t(i), t(j)]$ pour tout $t \in \mathcal{S}_n$.

Ex 4 - 5

a), b) Voir la 4-2, prop.

c) H' est le stabilisateur de c. Son ordre est fonction du cardinal de l'orbite de c.

d) Utiliser c). On a $sHs^{-1} = H$ si $scs^{-1} = c^k$ avec $k \wedge n = 1$.

Ex 4 - 6

Voir cours 4-1, ex., 4-2, cor. 2, 4-4, cor. 3.

Ex 4 - 7

Montrer qu'un produit tt' de deux transpositions est un commutateur.

Ex 4 - 8

Montrer que $\tau_k \cdots \tau_2$ est un cycle pour $2 \leqslant k \leqslant n$.

Ex 4 - 9

a) Raisonner par récurrence sur n.

b) On sait que $t_i t_{i+1} t_i = t_{i+1} t_i t_{i+1}$.

Ex 4 - 10

Tout 3-cycle c est conjugué de $(1,2,3)$ dans $\mathcal{S}_n$. Pour $n \geqslant 5$ il existe des transpositions qui commutent avec c.

Ex 4 - 11

Exercice assez difficile. Se laisser guider par l'énoncé, utiliser Ex. 4-1 et Ex. 4-9.

Ex 4 - 12

Raisonner par l'absurde et utiliser le th. de Cauchy.

Ex 4 - 13

Penser aux produits de 2 transpositions dont les supports sont disjoints.

Solutions des exercices du chapitre 4

Ex 4 - 1

Soit $s \in Z$. Supposons qu'il existe $i \in E = \{1, \ldots, n\}$ tel que $i \neq s(i) = j$. Choisissons $k \in E \backslash \{i, j\}$. Posons $t = [i, k]$. Comme $s \in Z$, on a $s(k) = s(t(i)) = t(s(i)) = t(j) = j$. C'est absurde car s étant bijective on ne peut avoir $s(i) = j$ et $s(k) = j$ avec $k \neq i$. On a donc $s(i) = i$ pour tout $i \in E$. Ainsi $Z = \{ \mathrm{Id} \}$.

Autre démonstration. Soit $s \in Z$. Considérons $i \in E = \{1, \ldots, n\}$ et une énumération $i_1, \ldots, i_{n-1}$ de $X = E \backslash \{i\}$. Le cycle $c = (i_1, \ldots, i_{n-1})$ commute avec s donc $scs^{-1} = c$. Les supports $s(X) = \{s(i_1), \ldots, s(i_{n-1})\}$ de scs^{-1} et X de c sont donc égaux, leurs complémentaires également. On a donc $s(i) = i$, pour tout $i \in E$, soit $s = \mathrm{Id}_E$.

Ex 4 - 2

Posons $t_1 = [1,2]$, $t_2 = [2,3]$, $t_3 = [1,3]$. Soit $\alpha \in \mathrm{Aut}(\mathcal{S}_3)$. Pour tout $i = 1, 2, 3$ on a $\alpha(t_i) \neq \mathrm{Id}$ et $\alpha(t_i)^2 = \alpha(t_i^2) = \alpha(\mathrm{Id}) = \mathrm{Id}$ donc $\alpha(t_i)$ est d'ordre 2. Or t_1, t_2, t_3 sont les seuls éléments d'ordre 2 de $\mathcal{S}_3$. Donc α permute t_1, t_2, t_3. L'application associant à $\alpha \in \mathrm{Aut}(\mathcal{S}_3)$ cette permutation φ_α de t_1, t_2, t_3 est injective. En effet, si deux automorphismes α, β sont tels que $\varphi_\alpha = \varphi_\beta$ alors $\alpha(s) = \beta(s)$ pour tout $s \in \mathcal{S}_3$ car s est produit de transpositions. On en déduit que $\mathrm{Aut}(\mathcal{S}_3)$ possède au plus 3 ! éléments. Par ailleurs, $\mathrm{Ad} : s \mapsto \mathrm{Ad}_s$ est un homomorphisme de $\mathcal{S}_3$ sur $\mathrm{Int}(\mathcal{S}_3)$. Son noyau est le centre Z du groupe $\mathcal{S}_3$, c'est-à-dire $\{ \mathrm{Id} \}$ d'après l'exercice précédent. Il est donc injectif et $\mathrm{Int}(\mathcal{S}_3)$ possède 3 ! éléments. On voit donc que $\mathrm{Aut}(\mathcal{S}_3) = \mathrm{Int}(\mathcal{S}_3) \simeq \mathcal{S}_3$.

Ex 4 - 3

Considérons $f \in \mathrm{Hom}(\mathcal{S}_3, \mathcal{A}_3)$. Pour toute transposition t on a $f(t)^2 = f(t^2) = f(\mathrm{Id}) = \mathrm{Id}$ donc $f(t)$ est d'ordre 1 ou 2. Comme $\mathcal{A}_3 = \{ \mathrm{Id}, c, c^2 \}$, où $c = (1,2,3)$, ne contient aucun élément d'ordre 2, on voit que $f(t) = \mathrm{Id}$ pour toute transposition t et donc pour tout $s \in \mathcal{S}_3$ car s est produit de transpositions. Ainsi f est l'homomorphisme trivial, qui n'est pas surjectif.

Ex 4 - 4

a) $t_i t_j = t_j t_i \Leftrightarrow t_i t_j t_i^{-1} = t_j \Leftrightarrow [t_i(j), t_i(j+1)] = [j, j+1]$
$\Leftrightarrow t_i(\{j, j+1\}) = \{j, j+1\}$.

- Si $i = j - 1$, on a $t_i(j) = j - 1 \notin \{j, j+1\}$, t_i et t_j ne commutent pas.
- Si $i = j + 1$, on a $t_i(j+1) = j + 2 \notin \{j, j+1\}$, t_i et t_j ne commutent pas.
- Si $|j - i| \geqslant 2$, les supports $\{i, i+1\}$ et $\{j, j+1\}$ de t_i et de t_j sont disjoints donc t_i et t_j commutent.

b) $t_i t_{i+1} t_i = t_i t_{i+1} t_i^{-1} = [t_i(i+1), t_i(i+2)] = [i, i+2]$.
$t_{i+1} t_i t_{i+1} = t_{i+1} t_i t_{i+1}^{-1} = [t_{i+1}(i), t_{i+1}(i+1)] = [i, i+2]$.

(On montre qu'un groupe engendré par $n-1$ éléments $t_1, \ldots, t_{n-1}$ vérifiant les relations a) et b) est isomorphe à $\mathcal{S}_n$.)

Ex 4 - 5

a) D'après 4-2, prop., l'orbite de c pour l'action par automorphismes intérieurs de $\mathcal{S}_n$ sur lui-même est l'ensemble $\mathcal{C}_k$ des cycles de longueur k. Pour déterminer $c' \in \mathcal{C}_k$, on choisit son support Δ parmi les C_n^k parties à k éléments, puis une liste numérotée $i_1, \dots, i_k$ des éléments du support Δ (on a $k!$ choix), d'où $c = (i_1, \dots, i_k)$. Toutefois, on a k listes qui donnent la même permutation, puisque $c = (i_2, \dots, i_k, i_1) = \cdots$ admet k expressions de ce type. Donc $\text{card}\,(\text{orb}(c)) = \frac{n!}{k!\,(n-k)!} k! \frac{1}{k} = \frac{n!}{(n-k)!\,k}$.

b) Soit $\sigma \in \mathcal{S}_n$ et soit $\sigma = c_1 \cdots c_k$ sa décomposition en cycles disjoints. Celle d'un de ses conjugués $s\sigma s^{-1} = sc_1s^{-1} \cdots sc_ks^{-1}$ a le même nombre de cycles, les cycles $c_1, \dots, c_k$ de s étant associés bijectivement à des cycles $sc_1s^{-1}, \dots, sc_ks^{-1}$ de $s\sigma s^{-1}$, de mêmes longueurs. On voit comme en 4-2, prop., que cette propriété caractérise les éléments de l'orbite de σ. Il y a donc autant d'orbites que de suites finies $(\alpha_1 \leqslant \cdots \leqslant \alpha_r)$, où $r \in \mathbb{N}^*$, telles que $n = \alpha_1 + \cdots + \alpha_r$. Pour $n = 3$, cela laisse 3 possibilités $(1,1,1)$, $(1,2)$, (3). Pour $\mathcal{S}_4$ on a 5 possibilités $(1,1,1,1)$, $(1,1,2)$, $(1,3)$, $(2,2)$, (4).

c) $s \in H' \;\Leftrightarrow\; sc^p = c^p s\,, \quad \forall\, p = 0, \dots, k-1$
$\Leftrightarrow\; sc^p s^{-1} = c^p\,, \quad \forall\, p = 0, \dots, k-1 \quad \Leftrightarrow \quad scs^{-1} = c\,,$

Le stabilisateur de c est H'. On a $\frac{[\mathcal{S}_n : 1]}{[H' : 1]} = \text{card}\,(\text{orb}(c))$, d'où $[H' : 1] = k(n-k)!$.

d) Si $k = n$, on obtient $[H' : 1] = n$. On a $H \subset H'$ car $H = \langle c \rangle$ est abélien et $[H : 1] = n$. On en déduit que $H = H'$. Si un sous-groupe abélien K de G contient H, alors tout $x \in K$ commute avec les éléments de H et donc $x \in H' = H$. Ainsi H est un sous-groupe abélien maximal de $\mathcal{S}_n$.

Si $s \in N_H$, on a $sHs^{-1} = H$ et donc $scs^{-1} \in H = \{\,\text{Id}\,, c\,, c^2, \dots, c^{n-1}\}$. Il existe donc $k \in \{0, \dots, n-1\}$ tel que $scs^{-1} = c^k$. De plus, $\text{Ad}_s(c) = scs^{-1}$ doit être un autre générateur de H donc $k \in \Delta = \{k \in \mathbb{N} \mid 0 \leqslant k \leqslant n-1 \text{ et } k \wedge n = 1\}$.

Réciproquement, si $scs^{-1} = c^k$ avec $k \in \Delta$, on a :

$$sHs^{-1} = s\langle c \rangle s^{-1} = \langle scs^{-1} \rangle = \langle c^k \rangle = H\,.$$

Ainsi, $s \in N_H$ si et seulement s'il existe $k \in \Delta$ tel que $scs^{-1} = (s(1), s(2), \dots, s(n))$ $= (1, 1+k, 1+2k, \dots, 1+(n-1)k)$, où les entiers sont réduits modulo n. Comme ce cycle admet n expressions $(l, k+l, 2k+l, \dots, (n-1)k+l)$ où $l = 1, \dots, n$, les éléments s de N_H sont donc définis par les données, indépendantes l'une de l'autre, de $k \in \Delta$ et de $l \in \{1, \dots, n\}$ et alors $s(i) = i + k + l$ pour tout $i \in \{1, \dots, n\}$. On a donc $[N_H : 1] = n\,\varphi(n)$, où φ est la fonction d'Euler. Le nombre de conjugués de H est donc $\frac{[\mathcal{S}_n : 1]}{[N_H : 1]} = \frac{(n-1)!}{\varphi(n)}$.

Ex 4 - 6

Ici s présente 12 inversions en $1 < 4$, $1 < 5$, …, $5 < 6$, donc $\varepsilon(s) = 1$.
$s(1) = 4$, $s(4) = 3$, $s(3) = 6$, $s(6) = 1$ d'où un cycle $c = (1,4,3,6)$.
$s(2) = 5$, $s(5) = 2$, d'où un cycle $c' = [2,5]$.

On a $s = cc' = c'c$. On retrouve ainsi que $\varepsilon(s) = \varepsilon(c)\varepsilon(c') = (-1)^3(-1) = 1$ (4-4, cor. 3). En utilisant 4-3, formules (1) et (2), on obtient

$c' = [2,5] = (2,3,4)[4,5](2,3,4)^{-1} = [2,3][3,4][4,5][3,4][2,3]$,
$c = (1,4,3,6) = [1,4][4,3][3,6]$, avec par exemple :

$[1,4] = (1,2,3)[3,4](1,2,3)^{-1} = [1,2][2,3][3,4][2,3][1,2]$,
$[3,6] = (3,4,5)[5,6](3,4,5)^{-1} = [3,4][4,5][5,6][4,5][3,4]$.

On obtient une expression de s (il n'y a pas d'unicité d'une telle expression) :

$$s = cc' = [1,2][2,3][3,4][2,3][1,2][4,5][5,6][4,5][3,4][2,3][3,4][4,5][3,4][2,3] .$$

Ex 4 - 7

D'après 4-2, cor. 1, deux transpositions t, t' sont conjuguées. Il existe donc $s \in \mathcal{S}_n$ telle que $t' = sts^{-1}$. On voit donc que $tt' = tst^{-1}s^{-1}$ est un commutateur. Tout $s \in \mathcal{A}_n$ est produit $s = t_1 t_2 \cdots t_{2k-1} t_{2k}$ d'un nombre pair de transpositions et donc produit de commutateurs. C'est un élément du groupe dérivé $\mathcal{S}'_n$ de $\mathcal{S}_n$. On a donc $\mathcal{A}_n \subset \mathcal{S}'_n$. Par ailleurs, le groupe dérivé $\mathcal{S}'_n$ est le plus petit sous-groupe distingué de $\mathcal{S}_n$ donnant un quotient abélien (voir 3-7). Puisque $\mathcal{S}_n/\mathcal{A}_n \simeq \{1,-1\}$ est abélien on a $\mathcal{S}'_n \subset \mathcal{A}_n$. Les deux sous-groupes sont égaux.

Ex 4 - 8

Pour tout $i \in \{2,\ldots,n\}$ on a $(1,2,\ldots,i) = [1,i][1,i-1]\cdots[1,2]$ (cela se vérifie par récurrence sur i). On voit donc que le sous-groupe engendré par $\tau_1,\ldots,\tau_n$ contient $\tau_1 = [1,2]$ et $c = (1,2,\ldots,n)$, d'où le résultat car τ_1 et c engendrent $\mathcal{S}_n$ (4-3, prop.).

Ex 4 - 9

a) On peut démontrer ce résultat par récurrence sur n , comme dans 4-4, ex. Donnons une autre démonstration. D'après 4-3, tout $s \in \mathcal{S}_n$ est produit de transpositions simples $s = [i,i+1][j,j+1][k,k+1][l,l+1]\cdots[m,m+1]$. On a $s \in \mathcal{A}_n$ si et seulement si le nombre de ces transpositions est pair. Il suffit donc de prouver que tout produit du type $\sigma = (i,i+1)(j,j+1)$ appartient au sous-groupe H de $\mathcal{S}_n$ engendré par les cycles c_i . Il revient au même de montrer que $\sigma^{-1} = (j,j+1)(i,i+1) \in H$. On peut donc supposer que $i \leqslant j$. Raisonnons par récurrence sur l'entier $k = j - i$.

- si $k = 0$, on a $[i,i+1][j,j+1] = [i,i+1][i,i+1] = \mathrm{Id} \in H$.
- si $k = 1$, on a $[i,i+1][j,j+1] = [i,i+1][i+1,i+2] = c_i \in H$.

Soit $k > 1$ et admettons la propriété pour $k-1$. Alors,

$$\sigma = [i,i+1][j,j+1] = [i,i+1][i+1,i+2][i+1,i+2][j,j+1] = c_i[i+1,i+2][j,j+1].$$

D'après l'hypothèse de récurrence, $[i+1,i+2][j,j+1] \in H$ donc $\sigma \in H$.

b) Dans Ex. 4-4, on a vu que $t_i t_{i+1} t_i = t_{i+1} t_i t_{i+1}$ donc $t_{i+1} t_i t_{i+1}^{-1} t_i^{-1} = t_i t_{i+1} = c_i$. Il en résulte que $c_i \in \mathcal{S}'_n$, pour tout i . D'après a), tout élément de $\mathcal{A}_n$ est produit de cycles c_i et d'inverses de cycles c_i . On a donc $\mathcal{A}_n \subset \mathcal{S}'_n$. D'autre part, tout commutateur $ss's^{-1}s'^{-1}$ est élément de $\mathcal{A}_n$ car $\varepsilon(ss's^{-1}s'^{-1}) = \varepsilon(s)\varepsilon(s')\varepsilon(s^{-1})\varepsilon(s'^{-1}) = 1$. On voit donc que $\mathcal{S}'n \subset \mathcal{A}_n$, d'où l'égalité de ces sous-groupes.

Ex 4 - 10

Soient $n \geqslant 2$ et $k \leqslant n$. D'après 4-2, prop., les cycles de longueur k constituent une classe de conjugaison dans $\mathcal{S}_n$. Pour tout 3-cycle $c = (i,j,k)$, il existe donc $s \in \mathcal{S}_n$ tel que $scs^{-1} = (1,2,3)$.
Si $s \notin \mathcal{A}_n$ et si $n \geqslant 5$, alors $([4,5]\,s\,)c\,([4,5]\,s)^{-1} = [4,5](1,2,3)[4,5] = (1,2,3)$, et $[4,5]s \in \mathcal{A}_n$. Pour $n \geqslant 5$, tout 3-cycle c est conjugué de $(1,2,3)$ dans $\mathcal{A}_n$.

Montrons que les cycles $\gamma = (1,2,3)$ et $\gamma^2 = (1,3,2)$ ne sont pas conjugués dans $\mathcal{A}_3$. Soit $s \in \mathcal{S}_3$ telle que $\gamma^2 = s\gamma s^{-1} = (s(1),s(2),s(3))$. Les images de $1,2,3$ par s sont $1,3,2$ ou $3,2,1$ ou $2,1,3$. Donc $s = [2,3]$ ou $s = [1,3]$ ou $s = [1,2]$. Ainsi $s \notin \mathcal{A}_3$.

Dans $\mathcal{S}_4$, considérons à nouveau $\gamma = (1,2,3)$ et $\gamma^2 = (1,3,2)$. Si $s \in \mathcal{S}_4$ est telle que $\gamma^2 = s\gamma s^{-1} = (s(1),s(2),s(3))$, alors nécessairement $s(4) = 4$. Le raisonnement précédent s'applique et montre que $s \notin \mathcal{A}_4$.

Ex 4 - 11

a) On a $s \in H$, $s^{-1} \in H$, $cs^{-1}c^{-1} \in H$ puisque $H \lhd \mathcal{A}_n$ et donc $\rho = scs^{-1}c^{-1} \in H$.

On a $sc(y) = s(x) = y$ et $cs(y) \neq y = c(z)$ car $s(y) \neq z$ et c est bijectif. Cela montre que $sc \neq cs$ et donc que $\rho \neq$ Id .

L'ensemble $X = \{x,y,z\} \cup \{s(x),s(y),s(z)\}$ a au plus 5 éléments car $y = s(x)$. Vérifions que tout $a \in E\backslash X$ est fixe par ρ. On a $c^{-1}(a) = a$. On ne peut avoir $s^{-1}(a) \in \{x,y,z\}$, sinon $a \in \{s(x),s(y),s(z)\} \subset X$ donc $cs^{-1}(a) = s^{-1}(a)$. Finalement, $\rho(a) = scs^{-1}c^{-1}(a) = scs^{-1}(a) = ss^{-1}(a) = a$.

b) Dans la décomposition de ρ en cycles disjoints, les cycles ont leurs supports dans X qui a au plus 5 éléments. On peut donc avoir $\rho = c_1$, cycle de longueur $|c_1| = 3$ ou 5 (ρ étant paire, la longueur ne peut être 2 ou 4) ou bien $\rho = c_1c_2$ avec $|c_1| = 2 = |c_2|$ (le cas $|c_1| = 2$ et $|c_2| = 3$ donnerait ρ impaire). Donc ρ a l'une des formes suivantes $\rho_1 = (i,j,k)$, $\rho_2 = (i,j,k,l,m)$, $\rho_3 = [i,j][k,l]$. Si $t = [\alpha,\beta]$, d'après 4-2, prop.

$$[t,\rho] \;=\; [\alpha,\beta]\rho[\alpha,\beta]\rho^{-1} \;=\; [\alpha,\beta][\rho(\alpha),\rho(\beta)]$$

Si on choisit $[\alpha,\beta]$ telle que $[\rho(\alpha),\rho(\beta)] = [\beta,\gamma]$, avec $\gamma \neq \alpha$ (et $\gamma \neq \beta$), on aura $[t,\rho] = [\alpha,\beta][\beta,\gamma] = (\alpha,\beta,\gamma)$. Dans le cas de ρ_1 et de ρ_2, on peut choisir $[\alpha,\beta] = [i,j]$. Dans le cas de ρ_3, considérons $m \notin \{i,j,k,l\}$. Alors $[\alpha,\beta] = [i,m]$ convient. Dans tous les cas H contient un 3-cycle.

c) Pour $n \geqslant 5$, les 3-cycles constituent une classe de conjugaison dans $\mathcal{A}_n$ (voir l'exercice précédent). Puisque H (distingué) contient un 3-cycle c, il contient tous les 3-cycles. Il contient donc le sous-groupe de $\mathcal{S}_n$ engendré par les 3-cycles, c'est-à-dire $\mathcal{A}_n$ (4-4, ex. ou Ex. 4-9). Ainsi, $\mathcal{A}_n$ est simple.

d) Soit H un sous-groupe distingué de $\mathcal{S}_n$. Si $H \subset \mathcal{A}_n$, alors $H = \{$ Id $\}$ ou $H = \mathcal{A}_n$. Supposons $H \not\subset \mathcal{A}_n$. Soit $h \in H\backslash\mathcal{A}_n$. Alors $H \cap \mathcal{A}_n$ est un sous-groupe distingué de $\mathcal{A}_n$. La partition $\mathcal{S}_n = \mathcal{A}_n \cup h\mathcal{A}_n$ en classes modulo $\mathcal{A}_n$ donne la partition de H

$$H \;=\; H \cap [\,\mathcal{A}_n \cup h\mathcal{A}_n\,] \;=\; (H \cap \mathcal{A}_n) \cup (H \cap h\mathcal{A}_n) \;=\; (H \cap \mathcal{A}_n) \cup h(H \cap \mathcal{A}_n)$$

en deux classes modulo $H \cap \mathcal{A}_n$. Comme $H \cap \mathcal{A}_n = \{ \mathrm{Id} \}$ ou $\mathcal{A}_n$, on a $H = \{ \mathrm{Id}, h\}$ ou $H = \mathcal{A}_n \cup h\mathcal{A}_n = \mathcal{S}_n$. Dans le premier cas, du fait que $H \lhd \mathcal{S}_n$ on a $shs^{-1} = h$ pour tout $s \in \mathcal{S}_n$ et donc $h = \mathrm{Id}$ car le centre de $\mathcal{S}_n$ est $\{ \mathrm{Id} \}$ (voir Ex. 4-1). C'est absurde car $h \notin \mathcal{A}_n$. Ainsi $H = \mathcal{S}_n$. Ainsi, $\{ \mathrm{Id} \}, \mathcal{A}_n$ et $\mathcal{S}_n$ sont les seuls sous-groupes distingués de $\mathcal{S}_n$.

Ex 4 - 12

Raisonnons par l'absurde. Supposons qu'il existe un sous-groupe H de $\mathcal{A}_4$ d'ordre 6. D'après le th. de Cauchy, il existe dans H des éléments c et s d'ordres 3 et 2. Dans $E = \{1,2,3,4\}$, les orbites sous l'action de $\langle c \rangle$ ont un cardinal diviseur de l'ordre 3 de $\langle c \rangle$. Ces orbites ont donc 1 ou 3 éléments. L'une au moins possède 3 éléments, sinon on aurait $c = \mathrm{Id}$, et une seule car E n'a que 4 éléments. Ainsi la décomposition en cycles disjoints de c, montre que c est un cycle d'ordre 3. Quitte à numéroter différemment les éléments de E, nous pouvons supposer que $c = (1,2,3)$. De même, l'action sur E de s et de ses puissances, a des orbites d'ordre 2 ou 1 et l'une des orbites au moins a deux éléments. Ainsi, s est soit une transposition t ou le produit tt' de deux transpositions disjointes. Comme $s \in H \subset \mathcal{A}_4$, le premier cas ne se présente pas. Donc $s = [i,j][k,l]$, avec $E = \{i,j\} \cup \{k,l\}$, réunion disjointe. L'une des parties, par exemple $\{i,j\}$, est contenue dans le support de c. Si $\{i,j\}$ est $\{2,3\}$ ou $\{3,1\}$, on peut écrire $c = (2,3,1)$ ou $c = (3,1,2)$. Quitte à changer une fois encore la notation des éléments de E, on peut supposer que $c = (1,2,3)$ et $s = [1,2][3,4]$. Dans le sous-groupe H on trouve les éléments Id, $s = [1,2][3,4]$, $csc^{-1} = [2,3][1,4]$, $c^2sc^{-2} = [3,1][2,4]$ qui constituent un sous-groupe de H d'ordre 4. D'après le th. de Lagrange, 4 doit alors diviser l'ordre 6 de H. C'est absurde.

Ex 4 - 13

a) Si H existe, tout $s \in H$, distinct de Id, est d'ordre 2. L'action du groupe $K = \{ \mathrm{Id}, s\}$ sur $E = \{1,2,3,4\}$ a des orbites dont le cardinal divise $[K : 1] = 2$. Si on a une orbite à deux éléments $\{i,j\}$, les autres points de E étant fixes, alors $s = [i,j]$. Ce cas est à écarter car on cherche H dans $\mathcal{A}_4$. Cette action a donc deux orbites à 2 éléments $\{i,j\}, \{k,l\}$ (disjointes). Posons $s_{ij} = [i,j][k,l]$. Ainsi, si H existe, ses éléments appartiennent à $\{ \mathrm{Id}, s_{12}, s_{13}, s_{14}\}$ et H ne peut être que cet ensemble. Or cet ensemble est effectivement un sous-groupe de $\mathcal{S}_4$, ayant la même table de multiplication que le petit groupe de Klein $(\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/2\mathbb{Z})$. En raison de l'unicité de ce sous-groupe H d'ordre 4, pour tout $\alpha \in \mathrm{Aut}(\mathcal{S}_4)$ on a $\alpha(H) = H$, autrement dit H est un sous-groupe caractéristique de $\mathcal{S}_4$.

b) Le cycle $c = (1,2,3,4)$ est d'ordre 4 donc $H' = \{ \mathrm{Id}, c, c^2, c^3\}$ est un sous-groupe d'ordre 4 de $\mathcal{S}_4$ isomorphe à $\mathbb{Z}/4\mathbb{Z}$. Comme $(\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/2\mathbb{Z})$ et $\mathbb{Z}/4\mathbb{Z}$ ne sont pas isomorphes (ils n'ont pas les mêmes invariants), H et H' ne peuvent pas être conjugués. (Les théorèmes de Sylow montreront que tous les sous-groupes d'ordre 2^3, puissance maximum de 2 dans l'ordre de $\mathcal{S}_4$, sont conjugués. Cet exercice montre donc qu'il n'en est pas de même pour les puissances inférieure à 3.)

Chapitre 5

Sous-groupes de Sylow

5.1 Théorèmes de Sylow

Soient G un groupe fini et $n = p_1^{k_1} \cdots p_s^{k_s}$ la décomposition en facteurs premiers de $n = [G : 1]$. D'après le th. de Lagrange, l'ordre de tout sous-groupe de G divise n.

Réciproquement soit d un diviseur de l'ordre de G. Si G est abélien, nous avons vu en 3-6, cor. 3, qu'il possède un sous-groupe d'ordre d. Ce sous-groupe n'est pas unique en général : par exemple, dans $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, il existe trois sous-groupes d'ordre 2. Si G est cyclique, ce sous-groupe d'ordre d est unique.

Si G n'est pas commutatif, si d divise l'ordre de G, il n'existe pas toujours de sous-groupe d'ordre d (Ex. 4-12 ou 5-2, ex.). S'il en existe un, il n'est en général pas unique.

Cependant, les théorèmes de Sylow donnent des réponses à ces questions pour les diviseurs particuliers $p_1^{k_1}, \ldots, p_s^{k_s}$ de l'ordre $n = p_1^{k_1} \cdots p_s^{k_s}$ de G.

Définitions.

Un groupe H d'ordre p^k, où p est un nombre premier, est appelé un p-groupe.

Si H d'ordre p^k, est un sous-groupe d'un groupe fini G (alors p est un facteur premier de $n = [G : 1]$), on dit que H un p-sous-groupe de G.

Si $n = [G : 1]$ a pour décomposition en facteurs premiers $n = p^k p_2^{k_2} \cdots p_s^{k_s}$ et si l'ordre de H est exactement p^k, on dit que H est un p-sous-groupe de Sylow de G.

Proposition. (théorèmes de Sylow)

Soit G un groupe fini, p un facteur premier de l'ordre n de G et soit $n = p^k p_2^{k_2} \cdots p_s^{k_s} = p^k q$ la décomposition en facteurs premiers de n.

(i) *Il existe dans G un p-sous-groupe de Sylow.*

(ii) *Tout p-sous-groupe de G est contenu dans un p-sous-groupe de Sylow de G.*

(iii) *Les p-sous-groupes de Sylow de G sont conjugués.*

(iv) *Le nombre n_p de p-sous-groupes de Sylow de G divise q et $n_p \equiv 1 \pmod{p}$.*

Démonstration. (i) Montrons (i) par récurrence sur n. Si n est premier, le résultat est évident. Supposons-le vrai pour les groupes d'ordre strictement inférieur à n.

Supposons qu'il existe dans G un sous-groupe $H \neq G$ tel que p^k divise $[H : 1]$. Comme $[G : 1] = [G : H][H : 1]$, il est équivalent de dire que p ne divise pas $[G : H]$. D'après l'hypothèse de récurrence, il existe dans H un sous-groupe d'ordre p^k.

Considérons le cas contraire où pour tout sous-groupe $H \neq G$, l'indice $[G : H]$ est divisible par p. Dans l'action de G sur G par automorphismes intérieurs, les orbites ponctuelles $\{x\}$ correspondent aux éléments du centre $Z(G)$. Soient $(O_{x_i})_{i\in I}$ les orbites non ponctuelles. Elles ont un stabilisateur G_{x_i} distinct de G. D'après l'hypothèse faite, $\text{card}\,(O_{x_i}) = [G : G_{x_i}]$ est divisible par p. La partition en orbites de G donne :

$$p^k q = \text{card}\,(G) = \text{card}\,(Z(G)) + \sum_{i\in I} \text{card}\,(O_{x_i}).$$

Donc $\text{card}\,(Z(G))$ est divisible par p, non nul car $e \in Z(G)$. D'après 3-5, cor. 2, il existe un sous-groupe K de $Z(G)$ d'ordre p. Etant contenu dans le centre de G, il est distingué dans G. D'après l'hypothèse de récurrence, le groupe G/K, dont l'ordre est $p^{k-1}q$, contient un sous-groupe L_1 d'ordre p^{k-1}. Soit φ l'homomorphisme canonique de G sur G/K et $L = \varphi^{-1}(L_1)$. On a $L_1 = \varphi(L) = L/K$, d'où $[L : 1] = [L : K][K : 1] = p^k$.

(ii) De l'action de G sur lui-même par automorphismes intérieurs, résulte une action de G sur les sous-groupes de G. Celle-ci laisse stable l'ensemble E des p-sous-groupes de Sylow de G car un sous-groupe isomorphe à un sous-groupe d'ordre p^k est encore un sous-groupe d'ordre p^k. Considérons $H \in E$ et son orbite $O_H = \{gHg^{-1}\,;\ g \in G\}$. Le stabilisateur G_H de H (normalisateur de H dans G) contient H donc

$$(1) \qquad \text{card}\,(O_H) = \frac{[G : 1]}{[G_H : 1]} = \frac{[G : 1]}{[G_H : H][H : 1]} = \frac{p^k q}{[G_H : H]p^k} = \frac{q}{[G_H : H]}$$

n'est pas divisible par p.

Soit K un p-sous-groupe de G d'ordre p^k. Restreignons l'action transitive de G sur O_H, au sous-groupe K. Soit $O_H = \bigcup_{i\in I} O_{H_i}$ la partition de O_H en orbites sous l'action de K. Pour tout $i \in I$, $\text{card}\,(O_{H_i}) = [K : K_{H_i}]$ divise $[K : 1] = p^k$. C'est une puissance p^{m_i} de p. Si on avait $m_i > 0$ pour tout $i \in I$, $\text{card}\,(O_H) = \sum_{i\in I} \text{card}\,(O_{H_i})$ serait divisible par p. Ce n'est pas le cas. Il existe donc $i \in I$ tel que $m_i = 0$ et donc tel que $O_{H_i} = \{H_i\}$. On a donc $kH_ik^{-1} = H_i$ pour tout $k \in K$.

Montrons que cette condition implique que $K \subset H_i$, ce qui prouvera (ii). Comme K normalise H_i, le th. de Noether montre que H_iK est un sous-groupe de G avec $H_i \lhd H_iK$, $H_i \cap K \lhd K$ et $H_iK/H_i \simeq K/(H_i \cap K)$. L'ordre de ce dernier groupe, qui divise $[K : 1]$, est une puissance p^α de p. Donc $[H_iK : 1] = [H_i : 1][K/(H_i \cap K) : 1] = p^k p^\alpha$ est une puissance de p. On a $H_i \subset H_iK$ et H_i est un sous-groupe de Sylow, d'ordre p^k maximum. On en déduit que $p^\alpha = 1$, d'où $H_i \cap K = K$ soit $K \subset H_i$.

(iii) Supposons de plus que K soit un sous-groupe de Sylow de G. On a $K \subset H_i$, avec $\text{card}\,(K) = p^k = \text{card}\,(H_i)$ et donc $K = H_i$, ce qui prouve que tout sous-groupe de Sylow K de G est l'un des conjugués H_i de H. Ainsi $E = O_H$.

(iv) Supposons toujours que K soit un sous-groupe de Sylow de G. D'après la fin de la démonstration de (ii), pour que l'action de K sur $O_H = E = O_K$, admette une orbite réduite à un élément, soit $O_{H_i} = \{H_i\}$, il faut et il suffit que $K \subset H_i$, ce qui signifie ici que $K = H_i$. Cela prouve que parmi les orbites sous l'action de K, une seule est de cardinal 1, les autres orbites O_{H_i} ont pour cardinal p^{α_i} avec $\alpha_i > 0$. Donc $\text{card}\,(E) = 1 + \sum_{i\in I} p^{\alpha_i}$ est congru à 1 modulo p.

Par ailleurs, la relation (1) ci-dessus montre que $\text{card}\,(E)$ divise q.

Corollaire.

Soient G un groupe fini, p un facteur premier de l'ordre de G et H un p-sous-groupe de Sylow de G. Si H est distingué, c'est le seul p-sous-groupe de Sylow de G. Réciproquement, s'il existe un seul p-sous-groupe de Sylow dans G, ce sous-groupe est caractéristique et donc distingué.

Démonstration. D'après la proposition, assertion (iii), les p-sous-groupes de Sylow de G sont les conjugués xHx^{-1} de H. Si H est distingué, ils sont tous égaux à H.

Réciproquement, si H est le seul sous-groupe de G d'ordre p^k, alors pour tout $\alpha \in \mathrm{Aut}(G)$, on a $\alpha(H)$ d'ordre p^k et donc $\alpha(H) = H$. ∎

Exercice 1. Quelle est la structure d'un groupe fini G d'ordre 153 ?

Solution. Puisque $1+5+3=9$ est divisible par 9, le nombre 153 est divisible par 9 (ch. 12, 1-1), d'où la décomposition en facteurs premiers $[G:1] = 3^2 \times 17$. D'après les th. de Sylow, il existe des sous-groupes H et K de G d'ordres $3^2 = 9$ et 17. Le nombre n_3 de 3-sous-groupes de Sylow divise 17 et vaut donc 1 ou 17. On a aussi, $n_3 \equiv 1 \pmod 3$. Comme $17 \equiv 2 \pmod 3$, on voit que $n_3 = 1$. D'après le corollaire, H est distingué. On vérifie de manière analogue que K est distingué.

D'après le th. de Lagrange, $[H \cap K : 1]$ divise $[H:1] = 9$ et $[K:1] = 17$. On a donc $[H \cap K : 1] = 1$ et $H \cap K = \{e\}$.

Comme les indices $[G:H] = 17$ et $[G:K] = 3^2$ sont premiers entre eux, on a $HK = G$ (Ex. 1-8, e)). On peut aussi démontrer que $HK = G$ en utilisant le th. de Noether (comme en 2-5, ex.).

Des propriétés $H \lhd G$, $K \lhd G$, $H \cap K = \{e\}$, $HK = G$, il résulte $G \simeq H \times K$ (prop. 1-11). Comme $[H:1] = p^2$, avec $p = 3$ premier, H est abélien (3-5, cor. 1). Comme $[K:1] = 17$ est premier, K est cyclique : on a $K \simeq \mathbb{Z}/17\mathbb{Z}$. Il en résulte que $G \simeq H \times K$ est abélien. D'après 3-6, on a $H \simeq \mathbb{Z}/9\mathbb{Z}$ ou $H \simeq (\mathbb{Z}/3\mathbb{Z}) \times (\mathbb{Z}/3\mathbb{Z})$. On en déduit deux décompositions cycliques canoniques possibles pour G, à savoir :

$(\mathbb{Z}/9\mathbb{Z}) \times (\mathbb{Z}/17\mathbb{Z}) \simeq \mathbb{Z}/153\mathbb{Z}$,

$[(\mathbb{Z}/3\mathbb{Z}) \times (\mathbb{Z}/3\mathbb{Z})] \times (\mathbb{Z}/17\mathbb{Z}) = (\mathbb{Z}/3\mathbb{Z}) \times (\mathbb{Z}/51\mathbb{Z})$ qui a pour invariants 3 et 51.

Exercice 2. Soient G un groupe fini, K un sous-groupe et p un facteur premier de $[K:1]$. Montrer que tout sous-groupe de Sylow de K est l'intersection de K avec un sous-groupe de Sylow de G. Si on a $K \lhd G$, montrer que réciproquement $H' \cap K$ est un p-sous-groupe de Sylow de K pour tout p-sous-groupe de Sylow H' de G. Montrer de plus que KH'/K est alors un p-sous-groupe de Sylow de G/K.

Solution. Soit p un facteur premier de l'ordre de K. D'après le premier th. de Sylow, il existe dans K un p-sous-groupe de Sylow H_0. Soit p^α son ordre. Alors H_0 est un p-sous-groupe de G. D'après le deuxième th. de Sylow, il existe un p-sous-groupe de Sylow H de G qui contient H_0. Soit p^β son ordre. Alors l'ordre du sous-groupe $H \cap K$ de H divise $[H:1] = p^\beta$. C'est donc un p-sous-groupe de K. Il contient H_0. Or H_0 est d'ordre p^α maximal. Il est donc maximal parmi les p-sous-groupes de K et $H \cap K = H_0$.

Supposons $K \lhd G$. Soit H' un p-sous-groupe de Sylow de G. D'après le troisième th. de Sylow, H' est un conjugué gHg^{-1} du p-sous-groupe de Sylow H précédent. On a :

$$H' \cap K = gHg^{-1} \cap gKg^{-1} = g(H \cap K)g^{-1} = gH_0g^{-1}.$$

Ainsi $[H' \cap K : 1] = [H_0 : 1] = p^\alpha$ est la puissance maximale de p dans $[K:1]$. C'est bien un p-sous-groupe de Sylow de K.

D'après le th. de Noether, $KH'/K \simeq H'/H' \cap K$. On en déduit que KH'/K est d'ordre $p^{\beta-\alpha}$ puissance de p dans l'ordre $[G/K:1] = \frac{[G:1]}{[K:1]} = \frac{p^\beta m'}{p^\alpha m}$ de G/K.

5.2 Structure de quelques groupes finis

Un groupe fini G, d'ordre p premier, est cyclique, isomorphe à $\mathbb{Z}/p\mathbb{Z}$. Pour $p = 2,3,5,7,11,13,\ldots$ il existe donc, à isomorphisme près, un seul groupe d'ordre p. Un tel groupe est isomorphe à $\mathbb{Z}/2\mathbb{Z}$, $\mathbb{Z}/3\mathbb{Z}$, $\mathbb{Z}/5\mathbb{Z}$, $\mathbb{Z}/7\mathbb{Z}$,..., ou encore $\mathbb{U}_2$, $\mathbb{U}_3$, $\mathbb{U}_5$, $\mathbb{U}_7$,... si on veut des groupes multiplicatifs.

Si G est d'ordre p^2 avec p premier, il est abélien (3-5, cor. 1). D'après 3-6, il est isomorphe à $\mathbb{Z}/p^2\mathbb{Z}$ ou à $(\mathbb{Z}/p\mathbb{Z}) \times (\mathbb{Z}/p\mathbb{Z})$. Un groupe fini d'ordre $4 = 2^2$ est donc commutatif, isomorphe à $\mathbb{Z}/4\mathbb{Z}$ s'il est cyclique ou isomorphe au petit groupe de Klein $(\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/2\mathbb{Z})$ s'il n'est pas cyclique.

Dans $\mathbb{Z}/4\mathbb{Z}$ il existe $\varphi(4) = 2$ éléments d'ordre 4 et un élément d'ordre 2. Le groupe $\mathrm{Aut}(\mathbb{Z}/4\mathbb{Z})$ est d'ordre $\varphi(4) = 2$ et donc constitué de Id et de $\overline{k} \mapsto -\overline{k}$.

Dans $G = (\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/2\mathbb{Z})$, il existe 3 éléments d'ordre 2. On peut vérifier que $\mathrm{Aut}(G)$ possède $3! = 6$ éléments correspondant aux 6 permutations des trois éléments d'ordre 2 de G (l'élément neutre est fixe par tout automorphisme)(voir Ex. 1-4). Il suffit d'ailleurs de vérifier que toute transposition est un automorphisme, puisque toute permutation est produit de transpositions.

De même, un groupe fini G d'ordre $9 = 3^2$ est commutatif, isomorphe à $\mathbb{Z}/9\mathbb{Z}$ ou à $(\mathbb{Z}/3\mathbb{Z}) \times (\mathbb{Z}/3\mathbb{Z})$. Si G est d'ordre 25 ou 49..., on conclut de manière analogue.

Nous nous proposons maintenant d'étudier les groupes d'ordre 6, 10, 14, 15,...

Proposition.

Soit G un groupe fini d'ordre pq où $p < q$ sont des nombres premiers.

(i) *Si q n'est pas congru à 1 modulo p, alors G est cyclique, isomorphe à $\mathbb{Z}/pq\mathbb{Z}$.*

(ii) *Si q est congru à 1 modulo p, à isomorphisme près G a deux structures possibles : ou bien G est abélien, cyclique, isomorphe à $\mathbb{Z}/pq\mathbb{Z}$, ou bien G n'est pas commutatif et alors G est isomorphe à $(\mathbb{Z}/q\mathbb{Z}) \times_\theta (\mathbb{Z}/p\mathbb{Z})$ où $\theta \in Hom(\mathbb{Z}/p\mathbb{Z}, Aut(\mathbb{Z}/q\mathbb{Z}))$ est tel que $\theta(\overline{1}) = \gamma$ est d'ordre p dans $Aut(\mathbb{Z}/q\mathbb{Z})$.*

Démonstration. D'après les th. de Sylow, il existe dans G un sous-groupe H d'ordre q et un sous-groupe K d'ordre p. Le nombre n_q de q-sous-groupes de Sylow est congru à 1 modulo q et divise p. Comme on a $p < q$, cela nécessite $n_q = 1$ donc H est distingué dans G.

D'après le th. de Lagrange, $[H \cap K : 1]$ divise $[H : 1] = q$ et $[K : 1] = p$. On a donc $[H \cap K : 1] = 1$ et $H \cap K = \{e\}$. Puisque $H \lhd G$, le th. de Noether montre que HK est un sous-groupe de G et que $HK/H \simeq K/(H \cap K) = K$. On en déduit que $[HK : 1] = [H : 1][K : 1] = pq = [G : 1]$ et donc que $HK = G$. D'après 2-6, G est un produit semi-direct de H et de K, isomorphe à $(\mathbb{Z}/q\mathbb{Z}) \times_\theta (\mathbb{Z}/p\mathbb{Z})$, où θ est un homomorphisme de $\mathbb{Z}/p\mathbb{Z}$ dans $\mathrm{Aut}(\mathbb{Z}/q\mathbb{Z})$.

Les p-sous-groupes de Sylow, sont les conjugués de K dans G. Leur nombre n_p est congru à 1 modulo p et divise q. Donc $n_p = 1$ ou $n_p = q$. Si $n_p = q$, alors q est congru à 1 modulo p d'après le quatrième th. de Sylow.

(i) *Supposons que q ne soit pas congru à 1 modulo p*. D'après ce qui précède, $n_p = 1$ et donc K est distingué dans G. Le produit semi-direct précédent est alors, d'après 2-6, un produit direct $H \times K$. Comme p et q sont premiers, H et K sont cycliques. Leurs ordres étant premiers entre eux, G est cyclique isomorphe à $\mathbb{Z}/pq\mathbb{Z}$.

(ii) *Supposons q congru à 1 modulo p* . L'ordre de l'image de $\theta : \mathbb{Z}/p\mathbb{Z} \to \mathrm{Aut}(\mathbb{Z}/q\mathbb{Z})$ divise l'ordre p de $\mathbb{Z}/p\mathbb{Z}$ et vaut p ou 1 (dans ce dernier cas, l'action est triviale).

Si θ est l'action triviale, alors le produit semi-direct $(\mathbb{Z}/q\mathbb{Z}) \times_\theta (\mathbb{Z}/p\mathbb{Z})$ est (d'après 2-6, cor.) un produit direct. Comme en (i), G est isomorphe à $\mathbb{Z}/pq\mathbb{Z}$.

Supposons maintenant que θ ne soit pas l'action triviale. On a vu en 3-2, rem., que $\mathrm{Aut}(\mathbb{Z}/q\mathbb{Z})$ est cyclique, d'ordre $\varphi(q) = q-1$ (ici divisible par p). D'après 3-3, il existe dans $\mathrm{Aut}(\mathbb{Z}/q\mathbb{Z})$ un unique sous-groupe Γ d'ordre p . On a donc $\Gamma = \mathrm{Im}(\theta)$. Puisque $\mathbb{Z}/p\mathbb{Z}$ et $\Gamma = \mathrm{Im}(\theta)$ ont le même ordre, θ est un isomorphisme de $\mathbb{Z}/p\mathbb{Z}$ sur Γ , déterminé par le choix de $\theta(\bar{1}) = \gamma$ parmi les $p-1$ générateurs de Γ . Vérifions que les $p-1$ choix possibles de $\theta(\bar{1})$ conduisent à des produits semi-directs isomorphes. Soit θ' un autre isomorphisme de $\mathbb{Z}/p\mathbb{Z}$ sur Γ . Alors $\alpha = \theta'^{-1} \circ \theta$ est un automorphisme de $\mathbb{Z}/p\mathbb{Z}$. Il existe alors un isomorphisme f de G_θ sur $G_{\theta'}$ d'après le lemme suivant. ∎

Lemme.

Avec ces données, $f : (\overset{\circ}{k}, \bar{l}) \mapsto (\overset{\circ}{k}, \alpha(\bar{l}))$ de $G_\theta = (\mathbb{Z}/q\mathbb{Z}) \times_\theta (\mathbb{Z}/p\mathbb{Z})$ sur $G_{\theta'} = (\mathbb{Z}/q\mathbb{Z}) \times_{\theta'} (\mathbb{Z}/p\mathbb{Z})$ est un isomorphisme.

Démonstration. Vérifions que f est un homomorphisme. Soient $x = (\overset{\circ}{k}, \bar{l})$ et $y = (\overset{\circ}{m}, \bar{n})$ deux éléments de G_θ . On a :

$$f(xy) = f[(\overset{\circ}{k}, \bar{l})(\overset{\circ}{m}, \bar{n})] = f(\overset{\circ}{k}\ [\theta(\bar{l})(\overset{\circ}{m})], \bar{l}\,\bar{n}) = (\overset{\circ}{k}\ [\theta(\bar{l})(\overset{\circ}{m})], \alpha(\bar{l}\,\bar{n})),$$

$$f(x)f(y) = (\overset{\circ}{k}, \alpha(\bar{l}))(\overset{\circ}{m}, \alpha(\bar{n})) = (\overset{\circ}{k}\ [\theta'(\alpha(\bar{l}))(\overset{\circ}{m})], \alpha(\bar{l})\alpha(\bar{n})) = (\overset{\circ}{k}\ [\theta(\bar{l})(\overset{\circ}{m})], \alpha(\bar{l}\,\bar{n})),$$

d'où le lemme car f est visiblement une bijection de $(\mathbb{Z}/q\mathbb{Z}) \times (\mathbb{Z}/p\mathbb{Z})$ sur lui-même. ∎

Corollaire.

Si $p = 2$ et si $q > 2$ est premier, un groupe G d'ordre $2q$ est soit isomorphe à $\mathbb{Z}/2q\mathbb{Z}$, soit isomorphe au groupe diédral D_p .

Démonstration. D'après la proposition, (ii), G n'a que deux structures possibles : l'une abélienne et $G \simeq \mathbb{Z}/2q\mathbb{Z}$, l'autre non abélienne. Comme D_q est d'ordre $2q$ et non abélien, il représente l'autre alternative. (voir 3-7, ex. 2 pour une étude directe) ∎

Remarque. Le corollaire montre qu'un groupe G d'ordre 6 est isomorphe à un produit semi-direct $\mathbb{Z}/3\mathbb{Z} \times_\theta \mathbb{Z}/2\mathbb{Z}$. Il a donc deux structures possibles : l'une (abélienne) lorsque θ est triviale, l'autre non abélienne. Si l'action θ est triviale, G est isomorphe au produit direct $(\mathbb{Z}/3\mathbb{Z}) \times (\mathbb{Z}/2\mathbb{Z})$ et donc à $\mathbb{Z}/6\mathbb{Z}$. Si θ n'est pas triviale, on a $\theta(\bar{0}) = \mathrm{Id}$ et $\theta(\bar{1}) = \alpha$, avec $\alpha : \bar{x} \mapsto -\bar{x}$. Alors $G \simeq (\mathbb{Z}/3\mathbb{Z}) \times_\theta (\mathbb{Z}/2\mathbb{Z})$ est non commutatif (sinon ce serait le produit direct et l'action serait triviale).

En résumé un groupe G d'ordre 6 ne peut avoir, à isomorphisme près, que deux structures : l'une commutative et alors $G \simeq \mathbb{Z}/6\mathbb{Z}$, l'autre non commutative. Or, nous connaissons un groupe d'ordre 6 non commutatif, à savoir le groupe $\mathcal{S}_3$ des permutations de 3 éléments. C'est donc $\mathcal{S}_3$ qui correspond au second cas (voir 4-5).

En géométrie, le groupe diédral D_3 des isométries du plan laissant invariant un triangle équilatéral $A_1A_2A_3$, est d'ordre 6, non commutatif. Il est donc isomorphe au groupe $\mathcal{S}_3$. Géométriquement, c'est visible car tout élément de D_3 permute les trois sommets et toute permutation des trois sommets correspond à un élément de D_3 .

Exercice. Montrer que dans le groupe symétrique $\mathcal{S}_5$ il n'existe aucun sous-groupe d'ordre 15, bien que 15 divise l'ordre de $\mathcal{S}_5$.

Solution. Comme $15 = pq$, avec $p = 3, q = 5$ premiers et q non congru à 1 modulo p, la proposition montre qu'un groupe H d'ordre 15 est cyclique isomorphe à $\mathbb{Z}/15\mathbb{Z}$. Supposons que H soit un sous-groupe de $\mathcal{S}_5$. Considérons un générateur s de H et sa décomposition en cycles disjoints $s = c_1 \cdots c_k$. L'ordre de s étant $\mathrm{ppcm}(o(c_1), \ldots, o(c_k))$, ces ordres $o(c_i)$ ne peuvent être que 3, 5 ou 15. La valeur 15 est exclue car dans $E = \{1, 2, 3, 4, 5\}$ on ne peut former des cycles de longueur 15. Les cycles c_i ont donc pour longueur 3 ou 5 et les deux valeurs doivent apparaître pour que le ppcm soit 15. On voit que c'est impossible car dans E on ne peut loger deux cycles disjoints, l'un d'ordre 3, l'autre d'ordre 5.

5.3 Groupes d'ordre 8

Parmi les groupes d'ordre petit, le cas d'un groupe G d'ordre $[G : 1] = 2^3 = 8$, échappe aux diverses remarques précédentes. Nous allons maintenant l'étudier.

D'après 3-6, cor. 1, si G est abélien, il est isomorphe à $\mathbb{Z}/8\mathbb{Z}$ ou $(\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/4\mathbb{Z})$ ou $(\mathbb{Z}/2\mathbb{Z})^3$. Ecartons ce cas et considérons un groupe G non commutatif, d'ordre 8. Il n'existe dans G aucun élément d'ordre 8, sinon G serait abélien cyclique. De même, si tout élément était d'ordre 2, alors G serait commutatif car pour tous $x, y \in G$, on aurait $x^2 = e$, $y^2 = e$, $xyxy = e$ et donc $yx = x(xyxy)y = xy$. Il existe donc dans G au moins un élément a d'ordre 4. Posons $A = \langle a \rangle$. Choisissons $b \notin A$. Alors, la classe à droite Ab est disjointe de A, de cardinal 4. On a donc $G = A \cup Ab$. Nécessairement $b^2 \in A$ car si on avait $b^2 \in Ab$, on en déduirait que $b \in A$. De plus, si on avait $b^2 = a$ ou $b^2 = a^3$, qui sont d'ordre 4, on vérifie facilement que b serait d'ordre 8, ce qui est exclu. Ainsi $b^2 = e$ ou $b^2 = a^2$. De plus, A d'indice 2 dans G est un sous-groupe distingué, d'après 1-7, cor. On a donc $b^{-1}ab \in A$ et comme l'ordre de $b^{-1}ab = \mathrm{Ad}_{b^{-1}}(a)$ est égal à l'ordre 4 de a, on a $b^{-1}ab = a$ ou $b^{-1}ab = a^3$. Or, $b^{-1}ab = a$ est exclu car cela impliquerait que $ab = ba$ et le groupe G engendré par a et b serait abélien. Ainsi, G est engendré par deux éléments a, b vérifiant :

$$a^4 = e \quad , \quad b^2 = e \quad , \quad b^{-1}ab = a^3 , \tag{1}$$

ou bien

$$a^4 = e \quad , \quad b^2 = a^2 \quad , \quad b^{-1}ab = a^3 . \tag{2}$$

Le cas (1) se présente pour le groupe diédral D_4 constitué des isométries du plan euclidien qui laissent globalement invariant un carré de centre O. Ce groupe possède 8 éléments, il est engendré par la rotation a de centre O et d'angle $\pi/4$ et par la symétrie b par rapport à une diagonale du carré et a, b vérifient les relations (1). Le groupe D_4 est, à isomorphisme près, le seul groupe engendré par deux éléments vérifiant les relations (1) (voir Ex. 8-3).

Le cas (2) se présente également. Le sous-groupe de $\mathrm{GL}(2, \mathbb{C})$ engendré par les matrices $a = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}$ et $b = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$, appelé le groupe des quaternions, possède 8 éléments. Il n'est pas isomorphe à D_4 et ses générateurs a, b vérifient (2). A isomorphisme près, c'est le seul groupe engendré par deux éléments vérifiant les relations (2). Nous laissons au lecteur le soin de le vérifier.

Exercices du chapitre 5

Ex 5 - 1

Donner les structures possibles, à isomorphisme près, pour un groupe G dont l'ordre est 1225.

Ex 5 - 2

On considère un groupe fini G, un diviseur premier p de $[G : 1]$, un p-sous-groupe de Sylow H de G et le normalisateur $N(H)$ de H.

a) Montrer que le nombre de p-sous-groupes de Sylow de G est $[G : N(H)]$.

b) Montrer que $N(N(H)) = N(H)$.

Ex 5 - 3

Soit G un groupe fini possédant la propriété suivante :
(P) tout sous-groupe de Sylow de G est cyclique.

a) Montrer que tout sous-groupe H de G possède la propriété (P).

b) Soient K_1 et K_2 des sous-groupes de G d'ordre p^m avec p premier et $m \in \mathbb{N}^*$. Montrer que K_1 et K_2 sont conjugués.

c) Si G est abélien, montrer que G est cyclique.

Ex 5 - 4

Soient G un groupe fini, H un sous-groupe distingué de G et $\varphi : G \to G/H$ l'homomorphisme canonique. Montrer que tout sous-groupe de Sylow de G/H est de la forme $HK/H = \varphi(K)$, où K est un sous-groupe de Sylow de G (réciproque de 5-1, ex. 2).

Ex 5 - 5

Montrer qu'un groupe G d'ordre 56 n'est pas simple.

Ex 5 - 6

Soit G un groupe d'ordre 130.

a) Soit K un groupe d'ordre 65. Montrer que K est cyclique. Montrer que dans le groupe $\mathrm{Aut}(K)$, il existe 3 éléments d'ordre 2.

b) Montrer qu'il existe dans G des sous-groupes P, Q d'ordres 2 et 5 et un sous-groupe distingué R d'ordre 13.

c) Montrer que $K = QR$ est un sous-groupe distingué de G, d'ordre 65. En déduire que Q est un sous-groupe distingué de G.

d) Montrer que G est un produit semi-direct $K \times_\varphi P$.

e) Montrer que G est isomorphe à l'un des groupes $\mathbb{Z}/130\mathbb{Z}$, D_{65}, $D_5 \times (\mathbb{Z}/13\mathbb{Z})$, $D_{13} \times (\mathbb{Z}/5\mathbb{Z})$.

Ex 5 - 7

Soit G un groupe d'ordre 12. Montrer que si G contient 4 sous-groupes d'ordre 3 alors il existe un seul sous-groupe d'ordre 4. En déduire que G n'est pas simple. Montrer qu'à isomorphisme près il existe 5 groupes d'ordre 12.

Indications

Ex 5 - 1

En utilisant les th. de Sylow, montrer que G est produit direct de ses sous-groupes de Sylow, puis que G est abélien.

Ex 5 - 2

b) Montrer que H est le seul p-sous-groupe de Sylow de $N(H)$.

Ex 5 - 3

Utiliser les th. de Sylow et les particularités des groupes cycliques.

Ex 5 - 4

Utiliser les th. de Sylow. Exprimer l'ordre des sous-groupes considérés.

Ex 5 - 5

Si G est d'ordre 56, montrer que s'il possède plusieurs sous-groupes d'ordre 7, alors leur complémentaire est un sous-groupe d'ordre 8 qui sera distingué.

Ex 5 - 6

a) D'après les th. de Sylow, K est produit direct de ses sous-groupes de Sylow.

c) K est d'indice 2.

e) Montrer qu'il n'existe que quatre actions de P sur $K \simeq (\mathbb{Z}/5\mathbb{Z}) \times (\mathbb{Z}/13\,\mathbb{Z})$ et utiliser Ex. 2-11.

Ex 5 - 7

Utiliser les th. de Sylow et raisonner comme dans Ex. 5-5 et Ex. 5-6.

Solutions des exercices du chapitre 5

Ex 5 - 1

D'après les th. de Sylow, G d'ordre $1225 = 5^2 \times 7^2$, possède un 5-sous-groupe de Sylow H d'ordre 5^2 et un 7-sous-groupe de Sylow K d'ordre 7^2. Le nombre n_5 des 5-sous-groupes de Sylow divise 7^2 et il est congru à 1 modulo 5 donc $n_5 = 1$. Puisque H est le seul sous-groupe de G d'ordre 5^2, pour tout automorphisme α de G, on a $\alpha(H) = H$. Ainsi $H \lhd G$. Le nombre n_7 des 7-sous-groupes de Sylow divise 5^2 et il est congru à 1 modulo 7 donc $n_7 = 1$. De cette unicité on déduit que $K \lhd G$.

L'ordre de $H \cap K$ divise $[H : 1] = 5^2$ et $[K : 1] = 7^2$. Donc $[H \cap K : 1] = 1$ et $H \cap K = \{e\}$. Puisque $H \lhd G$, le th. de Noether s'applique. On a $H \cap K \lhd K$ et $HK/H \simeq K/H \cap K$, d'où $[HK : 1] = [HK : H][H : 1] = [K : H \cap K][H : 1] = 5^2 \times 7^2 = [G : 1]$. Ainsi $HK = G$ (On peut aussi utiliser Ex. 1-8, e)).

On a $H \lhd G$, $K \lhd G$, $H \cap K = \{e\}$, $HK = G$ et donc $G \simeq H \times K$ (1-11, prop.). Or H (resp. K) d'ordre p^2, avec p premier, est abélien (3-5, cor. 1). Ainsi G est abélien et $G \simeq H \times K$ est la décomposition primaire de G.

Pour un groupe abélien d'ordre p^2, deux structures sont possibles : il est isomorphe à $\mathbb{Z}/p^2\mathbb{Z}$ ou à $(\mathbb{Z}/p\mathbb{Z}) \times (\mathbb{Z}/p\mathbb{Z})$ (3-6, cor. 1). Un produit de groupes cycliques d'ordres premiers entre eux étant cyclique (3-4, prop.), G est isomorphe à l'un des groupes :

$$
\begin{array}{lcl}
(\mathbb{Z}/5^2\mathbb{Z}) \times (\mathbb{Z}/7^2\mathbb{Z}) & \simeq & \mathbb{Z}/1225\mathbb{Z}\,, \\
(\mathbb{Z}/5^2\mathbb{Z}) \times \big((\mathbb{Z}/7\mathbb{Z}) \times (\mathbb{Z}/7\mathbb{Z})\big) & \simeq & (\mathbb{Z}/7\mathbb{Z}) \times (\mathbb{Z}/175\mathbb{Z})\,, \\
\big((\mathbb{Z}/5\mathbb{Z}) \times (\mathbb{Z}/5\mathbb{Z})\big) \times (\mathbb{Z}/7^2\mathbb{Z}) & \simeq & (\mathbb{Z}/5\mathbb{Z}) \times (\mathbb{Z}/245\mathbb{Z})\,, \\
\big((\mathbb{Z}/5\mathbb{Z}) \times (\mathbb{Z}/5\mathbb{Z})\big) \times \big((\mathbb{Z}/7\mathbb{Z}) \times (\mathbb{Z}/7\mathbb{Z})\big) & \simeq & (\mathbb{Z}/35\mathbb{Z}) \times (\mathbb{Z}/35\mathbb{Z}).
\end{array}
$$

Ex 5 - 2

a) On fait agir G sur lui-même par automorphismes intérieurs, d'où une action de G sur l'ensemble Ω des p-sous-groupes de Sylow de G, transitive d'après les th. de Sylow. Le stabilisateur de H est $N(H)$ donc $\text{card}\,(\Omega) = \frac{[G:1]}{[N(H):1]} = [G : N(H)]$.

b) D'après la définition du normalisateur de H, on a $H \lhd N(H)$. Les inclusions $H \subset N(H) \subset G$ et le th. de Lagrange, montrent que $[H : 1] = p^\alpha$ est la puissance de p maximum dans $[G : 1]$ et dans $[N(H) : 1]$. Ainsi, H est un p-sous-groupe de Sylow de $N(H)$. C'est le seul car il est distingué dans $N(H)$. Pour tout $g \in N(N(H))$, on a $gN(H)g^{-1} = N(H)$. Par restriction, l'automorphisme Ad_g induit un automorphisme de $N(H)$ qui laisse stable H car H est le seul sous-groupe d'ordre p^α de $N(H)$. On a donc $g \in N(H)$, ce qui prouve que $N(N(H)) \subset N(H)$. Comme on a $K \subset N(K)$ pour tout sous-groupe K, on obtient $N(N(H)) = N(H)$.

Ex 5 - 3

a) Soit p un facteur premier de $[H : 1]$ et soit K un sous-groupe de Sylow de H. Puisque $[H : 1]$ divise $[G : 1]$, p est un facteur premier de $[G : 1]$. Puisque K est un p-sous-groupe de G, il existe (d'après le deuxième th. de Sylow) un p-sous-groupe de Sylow K' de G qui contient K. Or K' est cyclique d'après (P). Le sous-groupe K de K' est donc cyclique (3-3, prop.) et H a la propriété (P).

b) K_1 et K_2 étant des p-sous-groupes de G, il existe (d'après les th. de Sylow) des p-sous-groupes de Sylow K_1' et K_2' de G tels que $K_1 \subset K_1'$ et $K_2 \subset K_2'$. D'après les th. de Sylow, K_1' et K_2' sont conjugués. Il existe $x \in G$ tel que $xK_1'x^{-1} = K_2'$. Alors, xK_1x^{-1} est un sous-groupe de K_2' d'ordre p^m. Comme K_2' est cyclique, il existe un seul groupe d'ordre p^m dans K_2' (3-3, prop.) donc $xK_1x^{-1} = K_2$.

c) Si G est abélien, il est le produit $G = H_1 \times \cdots \times H_k$ de ses sous-groupes de Sylow (composantes primaires de G), lesquels sont cycliques d'après la propriété (P). Donc G est cyclique car les ordres de $H_1, \ldots, H_k$ sont deux à deux premiers entre eux.

Ex 5 - 4

Puisque $[G/H : 1] = \frac{[G:1]}{[H:1]}$ divise $[G : 1]$, tout facteur premier p de $[G/H : 1]$ est facteur premier de $[G : 1]$. Considérons alors les puissances p^α et p^β de p dans $[G : 1]$ et $[H : 1]$ respectivement. Dans $[G/H : 1] = \frac{[G:1]}{[H:1]}$, la puissance de p est $p^{\alpha-\beta}$. Soit L un p-sous-groupe de Sylow de G/H. Il est d'ordre $p^{\alpha-\beta}$. Le sous-groupe $\varphi^{-1}(L) = M$ de G contient $H = \text{Ker}\,(\varphi)$. En factorisant la restriction de φ à M, on voit que $M/H \simeq L$ et donc que $[M : 1] = [H : 1][L : 1] = [H : 1]p^{\alpha-\beta}$ est divisible par p^α. C'est la puissance de p dans $[M : 1]$. D'après les th. de Sylow, il existe dans H un sous-groupe K_1 d'ordre p^β. D'après 5-1, ex. 2, il existe un p-sous-groupe de Sylow K de M tel que $K \cap H = K_1$. D'après le th. de Noether, KH est un sous-groupe de G et on a $KH/H \simeq K/K \cap H = K/K_1$. Alors, $\varphi(K) = \varphi(KH) = KH/H \simeq K/K_1$ est d'ordre $\frac{[K:1]}{[K_1:1]} = \frac{p^\alpha}{p^\beta} = p^{\alpha-\beta}$, avec $\varphi(K) \subset \varphi(M) = L$. Comme $[L : 1] = p^{\alpha-\beta}$, on en déduit que $\varphi(K) = L$. (Cet exercice complète 5-1, ex. 2.)

Ex 5 - 5

D'après les th. de Sylow, dans G d'ordre $56 = 2^3 \times 7$, il existe un sous-groupe H_1 d'ordre 7. Le nombre n_7 de sous-groupes d'ordre 7, est congru à 1 modulo 7 et divise $2^3 = 8$. Il vaut donc 1 ou 8. Si $n_7 = 1$, alors H_1 est distingué et G n'est pas simple. Si $n_7 = 8$, soient $H_1, \ldots, H_8$ les sous-groupes d'ordre 7. Pour $i \neq j$, on a $H_i \cap H_j = \{e\}$ car $[H_i \cap H_j : 1]$ divise $[H_i : 1] = 7$ et ne peut valoir que 1 ou 7. Or, la valeur 7 est exclue sinon $H_i = H_j$. Ainsi, $\cup H_i$ a pour éléments, e commun à tous les sous-groupes et 8 fois 6 éléments, d'où 49 éléments en tout. D'après les th. de Sylow, il existe dans G un sous-groupe K d'ordre 8. Pour tout i on a $K \cap H_i = \{e\}$ car $[K \cap H_i : 1]$ qui divise $[K : 1] = 8$ et $[H_i : 1] = 7$ ne peut valoir que 1. Donc les éléments de K ne peuvent être que e et les 7 éléments de $G \backslash (\cup H_i)$. Il en résulte que K est le seul sous-groupe d'ordre 8 de G. Il est donc distingué. Ainsi, dans un groupe d'ordre $56 = 2^3 \times 7$ ou bien il n'existe qu'un seul sous-groupe de Sylow d'ordre 8 qui est alors distingué ou bien il n'existe qu'un seul sous-groupe de Sylow d'ordre 7 qui est distingué.

Ex 5 - 6

a) On a $[K : 1] = 5 \times 13$. D'après les th. de Sylow, il existe dans K des sous-groupes H et L d'ordres 5 et 13. Le nombre n_5 de 5-sous-groupes de Sylow de K divise 13 et il est congru à 1 modulo 5 donc $n_5 = 1$. De ce fait, $\alpha(H) = H$ pour tout $\alpha \in \mathrm{Aut}(K)$ et H est caractéristique dans K. De même, L est caractéristique. D'après le th. de Lagrange, $[H \cap L : 1]$ divise $[H : 1] = 5$ et $[L : 1] = 13$ donc $[H \cap L : 1] = 1$ et $H \cap L = \{e\}$. D'après le th. de Noether, HL est un sous-groupe de K, d'ordre divisible par $[H : 1] = 5$, par $[L : 1] = 13$ et donc par 65. Il est nécessairement égal K. On a $H \lhd K$, $L \lhd K$, $H \cap L = \{e\}$, $HL = K$. Ainsi $(h, k) \mapsto hk$ est un isomorphisme $H \times L$ sur K (1-11, prop.). Or H et L d'ordres premiers sont cycliques. Leurs ordres étant premiers entre eux, $H \times L$ est cyclique.

Comme H et L sont des sous-groupes caractéristiques, tout automorphisme α de K les laisse invariants et induit par restrictions des automorphismes β et γ de ces groupes. L'application $\Phi : \alpha \mapsto (\beta, \gamma)$, de $\mathrm{Aut}(K)$ dans $\mathrm{Aut}(H) \times \mathrm{Aut}(L)$, est injective. En effet, puisque $K = HL$ la connaissance de β et γ détermine $\alpha(hl) = \beta(h)\gamma(l)$ pour tout élément hl de HL. Elle est surjective car la donnée de $\beta \in \mathrm{Aut}(H)$ et de $\gamma \in \mathrm{Aut}(L)$ détermine un automorphisme $(h, l) \mapsto (\beta(h), \gamma(l))$ de $H \times L$ et donc un automorphisme $hk \mapsto \alpha(h)\beta(k)$ de HL. L'application Φ est un isomorphisme de groupes : si α, α' sont éléments de $\mathrm{Aut}(K)$, alors on a
$\Phi(\alpha \circ \alpha') = (\alpha \circ \alpha'|_H , \alpha \circ \alpha'|_L) = (\alpha|_H \circ \alpha'|_H , \alpha|_L \circ \alpha'|_L) = \Phi(\alpha)\Phi(\alpha')$.
Pour p premier, $\mathrm{Aut}(\mathbb{Z}/p\mathbb{Z})$ est cyclique, d'ordre $p - 1$ donc
$\mathrm{Aut}(K) \simeq (\mathbb{Z}/4\mathbb{Z}) \times (\mathbb{Z}/12\mathbb{Z})$.

L'ordre de $(\bar{r}, \bar{s}) \in (\mathbb{Z}/4\mathbb{Z}) \times (\mathbb{Z}/12\mathbb{Z})$ est $\mathrm{ppcm}(o(\bar{r}), o(\bar{s}))$. Il existe un seul élément d'ordre 2 dans un groupe cyclique d'ordre pair. Dans $\mathbb{Z}/4\mathbb{Z}$, c'est $\bar{2}$. Dans $\mathbb{Z}/12\mathbb{Z}$, c'est $\bar{6}$. Dans $(\mathbb{Z}/4\mathbb{Z}) \times (\mathbb{Z}/12\mathbb{Z})$ les éléments d'ordre 2 sont : $(\bar{2}, \bar{0})$, $(\bar{0}, \bar{6})$, $(\bar{2}, \bar{6})$.

b) $[G : 1] = 2 \times 5 \times 13$. D'après les th. de Sylow, il existe des sous-groupes P, Q, R de G d'ordres $2, 5, 13$. Le nombre k de 13-sous-groupes de Sylow de G divise 2×5 et il est congru à 1 modulo 13. On a donc $k = 1$ et de ce fait R est distingué.

c) Puisque $[R \cap Q : 1]$ divise $[R : 1] = 13$ et $[Q : 1] = 5$, on voit que $[R \cap Q : 1] = 1$. On a $R \lhd G$. Appliquons le th. de Noether : QR est un sous-groupe de G, on a $R \lhd QR$, $R \cap Q \lhd Q$, $QR/R \simeq Q/R \cap Q$. On en déduit $[RQ : 1] = [R : 1][Q : 1] = 65$. Ainsi $RQ = K$ est d'indice 2 dans G et donc distingué (1-8, cor.).

Considérons $g \in G$ et le sous-groupe gQg^{-1}. On a $gRg^{-1} = R$ car R est distingué, d'où $(gQg^{-1})R = gQRg^{-1} = gKg^{-1} = K$ car K est distingué. Cela prouve que $gQg^{-1} \subset K$. Or dans K il n'existe, d'après a), qu'un seul sous-groupe d'ordre 5. Donc $gQg^{-1} = Q$ et Q est distingué dans G.

d) On a $K \cap P = \{e\}$ car l'ordre de $K \cap R$ divise $[P : 1] = 2$ et $[K : 1] = 65$ qui sont premiers entre eux. Puisque $K \lhd G$, le th. de Noether s'applique et permet de montrer, comme précédemment, que $KP = G$. On sait alors (voir 2-7, prop.) que $(k, p) \mapsto kp$ est un isomorphisme du produit semi-direct $K \times_\varphi P$ sur $KP = G$, où $\varphi \in \mathrm{Hom}(P, \mathrm{Aut}(K))$ désigne l'action $p \mapsto \mathrm{Ad}_p|_K$ de P sur K.

e) Si $P = \{e, p\}$, on a $\varphi(e) = \mathrm{Id}_K$ donc l'action φ est déterminée par la connaissance de $\varphi(p) \in \mathrm{Aut}(K)$. Puisque $p^2 = 2$, l'ordre de $\varphi(p)$ est 1 ou 2. Si l'ordre est 1, alors $\varphi(p) = \mathrm{Id}_K$ et φ est l'action triviale. Le produit semi-direct $K \times_\varphi P$ est alors le produit direct $K \times P$ qui est isomorphe à $\mathbb{Z}/130\,\mathbb{Z}$ puisque K et P sont cycliques d'ordres premiers entre eux. Si l'ordre est 2, alors $\varphi(p)$ est un des trois éléments d'ordre 2 de $\mathrm{Aut}(K)$ suivants (en identifiant K avec $(\mathbb{Z}/5\mathbb{Z}) \times (\mathbb{Z}/13\mathbb{Z})$) :

$\alpha_1 : (\bar{r}, \bar{s}) \mapsto (-\bar{r}, \bar{s})$ qui agit sur le premier facteur et induit l'identité sur le second,
$\alpha_2 : (\bar{r}, \bar{s}) \mapsto (\bar{r}, -\bar{s})$ qui induit l'identité sur le premier facteur,
$\alpha_3 : (\bar{r}, \bar{s}) \mapsto (-\bar{r}, -\bar{s}) = -(\bar{r}, \bar{s})$.

Si $\varphi(p) = \alpha_1$, l'action φ, est triviale sur le facteur $\mathbb{Z}/13\mathbb{Z}$ de $(\mathbb{Z}/5\mathbb{Z}) \times (\mathbb{Z}/13\mathbb{Z})$ et induit sur $\mathbb{Z}/5\mathbb{Z}$ une action ψ telle que $\psi(\bar{0}) = \mathrm{Id}$, $\psi(\bar{1})(\bar{k}) = -\bar{k}$. On a alors $[(\mathbb{Z}/5\mathbb{Z}) \times (\mathbb{Z}/13\mathbb{Z})] \times_\varphi (\mathbb{Z}/2\mathbb{Z}) \simeq [(\mathbb{Z}/5\mathbb{Z}) \times_\psi (\mathbb{Z}/2\mathbb{Z})] \times (\mathbb{Z}/13\mathbb{Z})$ (Ex. 2-11), avec $(\mathbb{Z}/5\mathbb{Z}) \times_\psi (\mathbb{Z}/2\mathbb{Z}) \simeq D_5$. Si $\varphi(p) = \alpha_2$, on a une situation analogue. Finalement,

si $\varphi(p) = \alpha_1$, on obtient $[(\mathbb{Z}/5\mathbb{Z}) \times (\mathbb{Z}/13\mathbb{Z})] \times_\varphi (\mathbb{Z}/2\mathbb{Z}) \simeq D_5 \times (\mathbb{Z}/13\mathbb{Z})$,
si $\varphi(p) = \alpha_2$, on obtient $[(\mathbb{Z}/5\mathbb{Z}) \times (\mathbb{Z}/13\mathbb{Z})] \times_\varphi (\mathbb{Z}/2\mathbb{Z}) \simeq (\mathbb{Z}/5\mathbb{Z}) \times D_{13}$,
si $\varphi(p) = \alpha_3$, on obtient $[(\mathbb{Z}/5\mathbb{Z}) \times (\mathbb{Z}/13\mathbb{Z})] \times_\varphi (\mathbb{Z}/2\mathbb{Z}) \simeq (\mathbb{Z}/65\mathbb{Z}) \times_\varphi (\mathbb{Z}/2\mathbb{Z}) \simeq D_{65}$.

Ex 5 - 7

Soit G un groupe d'ordre $12 = 2^2 \times 3$. D'après les th. de Sylow, il existe un sous-groupe H de G d'ordre 2^2 et un sous-groupe K d'ordre 3. Le nombre n_3 de 3-sous-groupes de Sylow divise 4 et on a $n_3 \equiv 1 \pmod 3$ donc $n_3 = 1$ ou 4.

Supposons que $n_3 = 4$. Notons $K_1, \ldots, K_4$ les quatre 3-sous-groupes de Sylow. D'après le th. de Lagrange, pour $i \neq j$, $[K_i \cap K_j : 1]$ divise $[K_i : 1] = 3$ et vaut donc 1 ou 3. Il est exclu que $[K_i \cap K_j : 1] = 3$ car cela imposerait $K_i = K_i \cap K_j = K_j$. Donc $K_i \cap K_j = \{e\}$. Si $x \in G$ est d'ordre 3, d'après le deuxième th. de Sylow $\langle x \rangle$ est, inclus dans l'un des 3-sous-groupes de Sylow K_i. Il existe donc $2 \times 4 = 8$ éléments d'ordre 3 dans G. Comme aucun élément du groupe H n'est d'ordre 3 (car $[H : 1] = 4$), on voit que H est le complémentaire de l'ensemble X des éléments d'ordre 3 de G. Tout $\alpha \in \mathrm{Aut}(G)$ laisse stable X. Donc $\alpha(H) = H$. Ainsi, on a $H \lhd G$.

D'après le th. de Lagrange, $[H \cap K : 1]$ divise $[H : 1] = 4$ et $[K : 1] = 3$ donc $[H \cap K : 1] = 1$ et $H \cap K = \{e\}$. D'après le th. de Noether, HK est un sous-groupe et $HK/H \simeq K/(K \cap H) \simeq K$ donc $[HK : 1] = [H : 1] \times [K : 1] = 12$ et $HK = G$. Ainsi, G est un produit semi-direct $H \times_\varphi K$, avec $K \simeq \mathbb{Z}/3\mathbb{Z}$ et $H \simeq \mathbb{Z}/4\mathbb{Z}$ ou $(\mathbb{Z}/2\mathbb{Z})^2$.

Si $H \simeq \mathbb{Z}/4\mathbb{Z}$ alors $[\mathrm{Aut}(H) : 1] = 2$ (3-2, cor. 2). Comme $3 \wedge 2 = 1$, d'après 1-9, cor. 1, le seul homomorphisme φ de $\mathbb{Z}/3\mathbb{Z}$ dans $\mathrm{Aut}(H)$ est l'homomorphisme trivial. Le produit semi-direct $H \times_\varphi K$ est un produit direct et G est isomorphe à $(\mathbb{Z}/4\mathbb{Z}) \times (\mathbb{Z}/3\mathbb{Z}) \simeq \mathbb{Z}/12\mathbb{Z}$.

Si $H \simeq (\mathbb{Z}/2\mathbb{Z})^2$, alors $\mathrm{Aut}(H)$ est d'ordre 6, isomorphe à $\mathcal{S}_3$ (voir Ex. 1-4). Un homomorphisme φ de $\mathbb{Z}/3\mathbb{Z}$ dans $\mathcal{S}_3$, est déterminé par la donnée de l'image $\varphi(\overline{1})$ du générateur $\overline{1}$ de $\mathbb{Z}/3\mathbb{Z}$. L'ordre $o(\varphi(\overline{1}))$ de $\varphi(\overline{1})$ divise $o(\overline{1})$. Il vaut 1 ou 3.
Si $o(\varphi(\overline{1})) = 1$, alors φ est trivial et $G \simeq (\mathbb{Z}/2\mathbb{Z})^2 \times (\mathbb{Z}/3\mathbb{Z}) \simeq (\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/6\mathbb{Z})$.
Si $o(\varphi(\overline{1})) = 3$, alors $\varphi(\overline{1})$ est l'un des éléments $c = (1,2,3)$ ou $c^2 = (1,3,2)$ d'ordre 3 de $\mathcal{S}_3$. Il existe donc deux homomorphismes φ_1 et φ_2 de $\mathbb{Z}/3\mathbb{Z}$ dans $\mathrm{Aut}(\mathcal{S}_3)$ (voir 3-2, cor. 1). Comme $\alpha : \overline{k} \mapsto -\overline{k}$ est un automorphisme de $\mathbb{Z}/3\mathbb{Z}$ tel que $\varphi_2 = \varphi_1 \circ \alpha$, les produits semi-directs $(\mathbb{Z}/2\mathbb{Z})^2 \times_{\varphi_i} (\mathbb{Z}/3\mathbb{Z})$, où $i = 1,2$, sont isomorphes (5-2, lemme). Par exemple, le groupe alterné $\mathcal{A}_4$ et le groupe des déplacements de l'espace euclidien conservant un tétraèdre régulier, sont d'ordre 12, non commutatifs et ont 4 sous-groupes d'ordre 3. Ils sont isomorphes et ont la structure que nous venons de caractériser.

Supposons que $n_3 = 1$. Alors K est distingué. On voit comme précédemment, que G est isomorphe à un produit semi-direct $K \times_\psi H$, où $\psi \in \mathrm{Hom}(H, \mathrm{Aut}(K))$. Ici, $\mathrm{Aut}(K)$ d'ordre $\varphi(3) = 2$ est isomorphe à $\mathbb{Z}/2\mathbb{Z} = \{\overline{0}, \overline{1}\}$.

Si $H = \mathbb{Z}/4\mathbb{Z}$, alors $\psi \in \mathrm{Hom}(\mathbb{Z}/4\mathbb{Z}, \mathbb{Z}/2\mathbb{Z})$ applique $\overline{1} \in \mathbb{Z}/4\mathbb{Z}$ sur $\overline{0}$ ou $\overline{1}$.
Si $\psi(\overline{1}) = \overline{0}$, alors ψ est trivial, $G \simeq (\mathbb{Z}/3\mathbb{Z}) \times (\mathbb{Z}/4\mathbb{Z}) \simeq \mathbb{Z}/12\mathbb{Z}$.
Si $\psi(\overline{1}) = \overline{1}$, alors $\psi(\overline{2}) = \overline{0}$, $\psi(\overline{3}) = \overline{1}$, $\psi(\overline{0}) = \overline{0}$ et $G \simeq (\mathbb{Z}/3\mathbb{Z}) \times_\psi (\mathbb{Z}/4\mathbb{Z})$.

Si $H = (\mathbb{Z}/2\mathbb{Z})^2$, ψ peut être triviale et alors $G \simeq (\mathbb{Z}/3\mathbb{Z}) \times (\mathbb{Z}/2\mathbb{Z})^2 \simeq (\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/6\mathbb{Z})$. Si ψ n'est pas trivial, alors $\psi(H) = \mathrm{Aut}(K)$ étant d'ordre 2, le noyau de ψ est un sous-groupe d'ordre 2 de $(\mathbb{Z}/2\mathbb{Z})^2$. On a donc trois choix ψ_1, ψ_2, ψ_3 selon le choix du noyau de ψ. Comme $\mathrm{Aut}(H) = \mathcal{S}_3$ permute les éléments d'ordre 2 de H, on voit que pour tous $i \neq j$, il existe $\alpha \in \mathrm{Aut}(H)$ tel que $\psi_i \circ \alpha = \psi_j$. Les produits semi-directs $K \times_{\psi_i} H$ et $K \times_{\psi_j} H$ sont isomorphes (5-2, lemme). Dans ce cas, G est isomorphe à un produit semi-direct $(\mathbb{Z}/3\mathbb{Z}) \times_\psi (\mathbb{Z}/4\mathbb{Z})$ qui est engendré par $a = (\overline{1}, \overline{0})$ et $b = (\overline{0}, \overline{1})$ d'ordres 3 et 4 tels que $bab^{-1} = \psi_b(a) = a^2$.

Finalement, à isomorphisme près, il existe cinq groupes d'ordre 12 parmi lesquels deux groupes abéliens $\mathbb{Z}/12\,\mathbb{Z}$, $(\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/6\mathbb{Z})$, trois groupes non abéliens :
- $\mathcal{A}_4$ qui a 8 éléments d'ordre 3 et qui n'a aucun élément d'ordre 4,
- le groupe diédral D_6 qui a deux éléments d'ordre 3 et aucun élément d'ordre 4,
- un autre groupe $(\mathbb{Z}/3\mathbb{Z}) \times_\psi (\mathbb{Z}/4\mathbb{Z})$ qui a des éléments d'ordre 4.

Ces cinq groupes sont deux à deux non isomorphes et tout groupe d'ordre 12 est isomorphe à l'un d'eux.

Deuxième partie

GEOMETRIE

Chapitre 6

Géométrie affine

6.1 Espace affine associé à un espace vectoriel

Définition.

On appelle espace affine, un ensemble $\mathcal{E}$ sur lequel le groupe additif $(E,+)$ d'un espace vectoriel agit à droite, transitivement et librement.

Les éléments de $\mathcal{E}$ sont appelés les points, ceux de E les vecteurs.

Si E est de dimension finie, $\dim(E)$ est appelée la dimension de l'espace affine $\mathcal{E}$.

Le groupe additif E est commutatif. Toute action à gauche de E est aussi une action à droite. Dans l'étude des espaces affines, elle est vue comme une action à droite. Elle ne se note pas $(M, \overrightarrow{x}) \mapsto M\cdot\overrightarrow{x}$ comme nous l'avions fait précédemment mais

$$(M, \overrightarrow{x}) \mapsto M+\overrightarrow{x}\,.$$

Ce signe $+$ ne désigne donc pas une loi de composition interne puisque M est un élément de $\mathcal{E}$ et $\overrightarrow{x}$ est un élément de E. C'est le résultat de l'action de $\overrightarrow{x}\in E$ sur $M\in\mathcal{E}$. Puisqu'il s'agit d'une action, on a :

a) $\forall\, M\in\mathcal{E}\quad \forall\,\overrightarrow{x}\in E\quad \forall\,\overrightarrow{y}\in E\qquad (M+\overrightarrow{x})+\overrightarrow{y} = M+(\overrightarrow{x}+\overrightarrow{y})$,

b) $\forall\, M\in\mathcal{E}\qquad M+\overrightarrow{0} = M$.

Dans l'expression $M+(\overrightarrow{x}+\overrightarrow{y})$, les deux signes "plus" n'ont pas du tout la même signification : le premier exprime l'action sur $M\in\mathcal{E}$ d'un vecteur $\overrightarrow{z}=\overrightarrow{x}+\overrightarrow{y}$, le deuxième est la loi de composition interne du groupe additif $(E,+)$.

Puisque l'action est ici transitive, pour tout couple de points (M,N) de $\mathcal{E}$ il existe $\overrightarrow{x}\in E$ tel que $N=M+\overrightarrow{x}$. L'action étant libre, ce vecteur $\overrightarrow{x}$ est unique. Il existe donc une application bien définie associant à tout couple (M,N) de points de $\mathcal{E}$ le vecteur $\overrightarrow{x}\in E$ tel que $N=M+\overrightarrow{x}$. On note $\overrightarrow{MN}$ ce vecteur $\overrightarrow{x}$. Il vérifie la condition suivante, qui le caractérise :

$$M+\overrightarrow{MN} = N\,. \tag{1}$$

Proposition.

Quels que soient les points A,B,C de l'espace affine $\mathcal{E}$, on a la relation de Chasles

$$\overrightarrow{AB}+\overrightarrow{BC} = \overrightarrow{AC}\,.$$

On a $\overrightarrow{AA}=\overrightarrow{0}$ pour tout $A\in\mathcal{E}$ et $\overrightarrow{BA}=-\overrightarrow{AB}$ pour tout $A\in\mathcal{E}$, tout $B\in\mathcal{E}$.

Démonstration. En utilisant (1) et la condition a), on obtient

$$A + \overrightarrow{AC} = C \quad \text{et} \quad A + (\overrightarrow{AB} + \overrightarrow{BC}) = (A + \overrightarrow{AB}) + \overrightarrow{BC} = B + \overrightarrow{BC} = C .$$

L'unique vecteur $\overrightarrow{x}$ tel que $A + \overrightarrow{x} = C$, est donc $\overrightarrow{AB} + \overrightarrow{BC} = \overrightarrow{AC}$. Avec $A = B = C$ on voit que $\overrightarrow{AA} = \overrightarrow{0}$. En prenant $C = A$ il vient $\overrightarrow{AB} + \overrightarrow{BA} = \overrightarrow{AA} = \overrightarrow{0}$. ∎

Corollaire.

Les translations $t_{\vec{x}} : M \mapsto M + \overrightarrow{x}$, où $\overrightarrow{x} \in E$, constituent un sous-groupe du groupe $\mathcal{S}_{\mathcal{E}}$ des bijections de $\mathcal{E}$ sur $\mathcal{E}$, isomorphe à E.

Démonstration. Comme pour toute action de groupe, $t_{\vec{x}} : M \mapsto M + \overrightarrow{x}$ est, pour tout $\overrightarrow{x} \in E$, une bijection de $\mathcal{E}$ sur $\mathcal{E}$ (d'application réciproque $t_{-\vec{x}}$) et $t : \overrightarrow{x} \mapsto t_{\vec{x}}$, est un homomorphisme du groupe additif $(E, +)$ dans $\mathcal{S}_{\mathcal{E}}$. Si $\overrightarrow{x} \in \mathrm{Ker}\,(t)$, on a $t_{\vec{x}} = \mathrm{Id}_{\mathcal{E}}$, soit $M + \overrightarrow{x} = M$ pour tout $M \in \mathcal{E}$. On en déduit que $\overrightarrow{x} = \overrightarrow{MM} = \overrightarrow{0}$. L'homomorphisme t est injectif (une action libre est toujours fidèle) et $t(E)$ est isomorphe à E. ∎

Exercice. On considère un ensemble $\mathcal{E}$, un espace vectoriel E et une application $(A, B) \mapsto \overrightarrow{AB}$ de $\mathcal{E} \times \mathcal{E}$ dans E, telle que :

1) $\forall A \in \mathcal{E} \quad \forall B \in \mathcal{E} \quad \forall C \in \mathcal{E} \qquad \overrightarrow{AB} + \overrightarrow{BC} = \overrightarrow{AC}$,

2) pour tout $A \in \mathcal{E}$, l'application $\varphi_A : N \mapsto \overrightarrow{AN}$ est bijective de $\mathcal{E}$ sur E.

Montrer que $\mathcal{E}$ est de manière naturelle un espace affine sur E.

Solution. Soient $M \in \mathcal{E}$ et $\overrightarrow{x} \in E$. D'après 2), il existe $N \in \mathcal{E}$ unique, tel que $\overrightarrow{MN} = \overrightarrow{x}$. Posons $M + \overrightarrow{x} = N$. Montrons que l'on définit ainsi une action de $(E, +)$ sur $\mathcal{E}$.

Soient $M \in \mathcal{E}$, $\overrightarrow{x} \in E$, $\overrightarrow{y} \in E$. Alors $N = M + \overrightarrow{x}$, est l'unique point de $\mathcal{E}$ tel que $\overrightarrow{MN} = \overrightarrow{x}$. De même $P = N + \overrightarrow{y}$ est l'unique point tel que $\overrightarrow{NP} = \overrightarrow{y}$. D'après 1), $\overrightarrow{x} + \overrightarrow{y} = \overrightarrow{MN} + \overrightarrow{NP} = \overrightarrow{MP}$. Ainsi $P = M + (\overrightarrow{x} + \overrightarrow{y})$, ce qui prouve que :

$$(M + \overrightarrow{x}) + \overrightarrow{y} = N + \overrightarrow{y} = P = M + (\overrightarrow{x} + \overrightarrow{y}) .$$

Pour tout $M \in \mathcal{E}$, on a $\overrightarrow{MM} + \overrightarrow{MM} = \overrightarrow{MM}$ et donc $\overrightarrow{MM} = \overrightarrow{0}$. L'unique vecteur $\overrightarrow{x}$ tel que $M = M + \overrightarrow{x}$ est $\overrightarrow{x} = \overrightarrow{0}$. Pour tout $M \in \mathcal{E}$, on a donc $M + \overrightarrow{0} = M$.

On a donc bien une action. Cette action est transitive et libre, d'après 2).

Exemple. Tout groupe G agit par translations à droite sur lui-même : en posant $X = G$, cette action est $(x, g) \mapsto xg$. Cette action est libre et transitive : pour tout $x \in X$ et pour tout $x' \in X$, il existe $g \in G$ unique tel que $xg = x'$, à savoir $g = x^{-1}x'$.

Cela s'applique en particulier au groupe additif $(E, +)$ d'un espace vectoriel E. Il existe donc un espace affine $\mathcal{E}_E$ dont l'ensemble des points est $\mathcal{E}_E = E$ et pour lequel l'action d'un vecteur $\overrightarrow{y} \in E$ sur $\mathcal{E}_E$ est l'action par la translation $t_{\vec{y}} : \overrightarrow{x} \mapsto \overrightarrow{x} + \overrightarrow{y}$ habituelle. Nous l'appellerons l'*espace affine canonique* sur E.

Si $E = K^n$, nous noterons $\mathcal{E}_n(K)$ l'espace affine canonique de K^n.

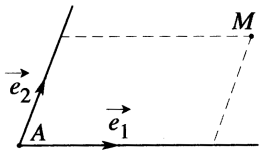
6.2 Repères cartésiens

Fixons une origine $A \in \mathcal{E}$. L'application de E sur $\mathcal{E}$

$$\varphi_A : \overrightarrow{x} \mapsto A + \overrightarrow{x}$$

est bijective car l'action est libre et transitive. Elle permet de paramétrer $\mathcal{E}$ à l'aide de E. L'application réciproque de φ_A est $M \mapsto \overrightarrow{AM}$ car $\varphi_A(\overrightarrow{AM}) = M$.
Supposons l'espace vectoriel E de dimension finie n sur le corps K. Soit $\mathcal{B} = (\overrightarrow{e_1}, \ldots, \overrightarrow{e_n})$ une base de E. Tout vecteur $\overrightarrow{x} = x_1\overrightarrow{e_1} + \cdots + x_n\overrightarrow{e_n}$ de E est caractérisé par ses coordonnées $x_1, \ldots, x_n$ dans cette base. On obtient donc une bijection de K^n sur $\mathcal{E}$, associant à $(x_1, \ldots, x_n)$ le point

$$M = A + x_1\overrightarrow{e_1} + \cdots + x_n\overrightarrow{e_n}. \quad (1)$$



cas où $n = 2$

Définition.

Un tel système $R = (A, \overrightarrow{e_1}, \ldots, \overrightarrow{e_n})$ formé d'une origine A de $\mathcal{E}$ et d'une base de E est appelé un repère cartésien de $\mathcal{E}$. Les scalaires $x_1, \ldots, x_n$ caractérisés par la relation (1) *s'appellent les coordonnées du point M de $\mathcal{E}$ dans ce repère.*

Soient $R' = (A', \overrightarrow{e'_1}, \ldots, \overrightarrow{e'_n})$ un autre repère, $P = (a_{ij})$ la matrice de passage de la base $\mathcal{B} = (\overrightarrow{e_1}, \ldots, \overrightarrow{e_n})$ à la base $\mathcal{B}' = (\overrightarrow{e'_1}, \ldots, \overrightarrow{e'_n})$, c'est-à-dire la matrice de $\mathrm{Id}_E : (E, \mathcal{B}') \mapsto (E, \mathcal{B})$ dont les colonnes sont formées des coordonnées de $\overrightarrow{e'_1}, \ldots, \overrightarrow{e'_n}$ dans la base $\mathcal{B}$. Les coordonnées d'un vecteur dans la base $\mathcal{B}$ sont données en fonction de ses coordonnées dans la base $\mathcal{B}'$ par la formule $X = AX'$. Si on note $a'_1, \ldots, a'_n$ les coordonnées de A' dans le repère R, la relation

$$\overrightarrow{AM} = \overrightarrow{AA'} + \overrightarrow{A'M}$$

donne les formules de changement de repère

$$(1) \qquad \begin{cases} x_1 &= a'_1 + a_{11}x'_1 + \cdots + a_{1n}x'_n \\ \ldots & \ldots \quad \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ x_n &= a'_n + a_{n1}x'_1 + \cdots + a_{nn}x'_n \end{cases}.$$

Considérons une variété (C) d'équation $F(x_1, \ldots, x_n) = 0$ dans le repère R, où F est un polynôme de n variables à coefficients dans le corps K des scalaires de E, de degré total k. En substituant à $x_1, \ldots, x_n$ leur expression (1) en fonction des coordonnées $x'_1, \ldots, x'_n$, on obtient l'équation de (C) dans le repère R'. C'est encore un polynôme de degré total k car la matrice $(a_{ij}$ est inversible. On voit qu'en géométrie affine la notion de *variété algébrique de degré k*, a un sens indépendamment du repère dans lequel on se place pour la définir.

Dans le plan affine $\mathcal{E}_2(K)$, les courbes de degré 2 sont appelées les *coniques*. Les courbes de degré $3, 4, \ldots$ sont appelées les *cubiques*, les *quartiques*, ... Elles furent très étudiées, dans le plan euclidien, aux 17$^{\mathrm{e}}$ et 18$^{\mathrm{e}}$ siècles. Les plus connues comme la strophoïde, la cissoïde, la lemniscate de Bernoulli, les limaçons de Pascal dont la cardioïde, se déduisent par inversion de coniques, ce qui fournit des paramétrages rationnels et des caractérisations géométriques de ces courbes (voir Ex. 8-1).

Les surfaces de degré 2 de l'espace affine $\mathcal{E}_3(K)$ sont appelées *quadriques*. Les variétés algébriques de degré 2 de $\mathcal{E}_n(K)$ sont appelées *hyperquadriques* de cet espace.

Rappelons le principe de la classification affine des coniques (celle des quadriques se fait de manière analogue). Considérons l'équation générale d'une conique (C) :

$$f(x,y) \;=\; ax^2 + 2bxy + cy^2 + 2dx + 2ey + f \;=\; 0$$

dans un repère R. La signature de la forme quadratique $q(x,y) = ax^2 + 2bxy + cy^2$, donnant les signes de sa décomposition comme somme de carrés de formes linéaires indépendantes, ne dépend pas de la base de E choisie. Comme on peut multiplier le premier membre de l'équation de (C) par un réel non nul sans changer (C), trois cas se présentent :

$q(x,y) \;=\; (\alpha x + \beta y)^2 + (\gamma x + \delta y)^2$, genre ellipse (on a q de rang 2),
$q(x,y) = (\alpha x + \beta y)^2 - (\gamma x + \delta y)^2$, genre hyperbole (on a q de rang 2),
$q(x,y) = (\alpha x + \beta y)^2$, genre parabole (on a q de rang 1).

Pour savoir si $I(x_0, y_0)$ est centre de symétrie de (C), on place l'origine en I. Les nouvelles coordonnées X, Y, vérifient $x = x_0 + X$, $y = y_0 + Y$, d'où l'équation de (C) :

$$q(X,Y) + 2(ax_0 + by_0 + d)X + 2(bx_0 + cy_0 + e)Y + f(x_0, y_0) \;=\; 0\,.$$

Ainsi, I est centre de symétrie si et seulement si $\left\{ \begin{array}{lcl} ax_0 + by_0 & = & -d \\ bx_0 + cy_0 & = & -e \end{array} \right.$.

Si le déterminant $\delta = ac - b^2$ du système est non nul, la conique a un unique centre de symétrie. La matrice M du système est la matrice de la forme quadratique q donc $\delta \neq 0$ lorsque q est de rang 2, c'est-à-dire si (C) est du genre ellipse ou du genre hyperbole. On appelle ces coniques les *coniques à centre*.

Dans le cas du genre parabole, on a $\delta = 0$. Le système précédent est de rang 1, les colonnes de la matrice M du système sont proportionnelles, engendrent une droite dans K^2. Si le second membre appartient à cette droite, le système est équivalent à la première de ses équations. On a une droite de centres de symétrie. La conique est constituée de deux droites parallèles. Si le second membre n'appartient pas à cette droite de K^2, le système n'a pas de solution. La conique est une parabole.

Si (C) est à centre, $q(x,y)$ est somme ou différence de carrés de formes linéaires indépendantes. Le changement de base indiqué par ces formes conduit à l'équation

$X^2 + Y^2 - 1 = 0$ (genre ellipse) ou $X^2 - Y^2 - 1 = 0$ (genre hyperbole).

Si (C) est une parabole, en prenant pour origine un point de (C) et en choisissant la forme linéaire apparaissant au carré dans $q(x,y)$ et les termes de degré 1 (contenant une forme indépendante de la précédente), on obtient l'équation $X^2 - Y = 0$.

Exercice. Dans $\mathcal{E}_2(\mathbb{R})$, muni d'un repère $R = (O, \overrightarrow{\imath}, \overrightarrow{\jmath})$, étudier la conique (C) ayant pour équation $f(x,y) \;=\; x^2 + 2xy - y^2 - 6x + 2y - 1 \;=\; 0$.

Solution. La forme quadratique $q(x,y) \;=\; x^2 + 2xy - y^2 \;=\; (x+y)^2 - 2y^2$ a pour signature $(1,1)$. Donc (C) est une conique à centre, du genre hyperbole. Déterminons son centre A. En posant $x = a + X$, $y = b + Y$, l'équation devient

$$q(X,Y) + (2a + 2b - 6)X + (2a - 2b + 2)Y + f(a,b) = 0\,.$$

Les coordonnées de A sont solutions du système de Cramer $\left\{ \begin{array}{lcl} 2a + 2b & = & 6 \\ 2a - 2b & = & -2 \end{array} \right.$,

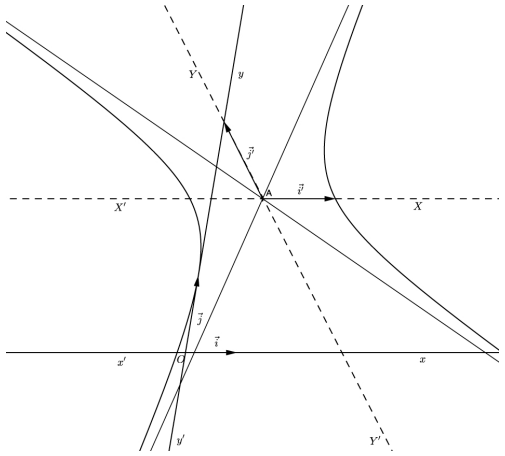
soit $a = 1$ et $b = 2$. Dans le repère $(A, \overrightarrow{\imath}, \overrightarrow{\jmath})$, l'équation de (C) est

$$\begin{aligned} 0 &= X^2 + 2XY - Y^2 - 2 \\ &= (X+Y)^2 - 2Y^2 - 2 \end{aligned}$$

soit $\frac{1}{2}(X+Y)^2 - Y^2 - 1 = 0$.

Posons $X' = \frac{1}{\sqrt{2}}(X+Y)$, $Y' = Y$, c'est-à-dire prenons comme nouveaux vecteurs de base $\overrightarrow{\imath'}(\sqrt{2}, 0)$, $\overrightarrow{\jmath'}(-1, 1)$.

L'équation de (C) est $X'^2 - Y'^2 - 1 = 0$.



6.3 Applications affines

Considérons une action d'un groupe G sur un ensemble X, c'est-à-dire un homomorphisme t du groupe G dans le groupe $\mathcal{S}_X$ des bijections de X. Que peut être une action (X', G', t') isomorphe à (X, G, t) ? Si $G = G'$, la notion naturelle sera la donnée d'une bijection $f : X \mapsto X'$ qui échange les deux actions, c'est-à-dire telle que $f(x.g) = f(x).g$ pour tout $x \in X$ et pour tout $g \in G$. Cela signifie que f entrelace les homomorphismes de groupes $t : G \to \mathcal{S}_X$ et $t' : G' \to \mathcal{S}'_X$ dans le sens suivant :

$$\forall\, g \in G \quad f \circ t(g) = t'(g) \circ f\,.$$

Si G et G' sont distincts, pour avoir des objets isomorphes, on donnera en outre un isomorphisme de groupes h de G sur G' tel que :

$$\forall\, g \in G \quad f \circ t(g) = t'[h(g)] \circ f\,.$$

Cette condition peut encore s'écrire :

$$\forall\, x \in X \quad \forall\, g \in G \quad f(x \cdot g) = f(x) \cdot h(g)\,.$$

Pour définir une notion d'homomorphisme de (X, G, t) dans (X', G', t'), on considèrera un homomorphisme de groupes h de G dans G', une application f de X dans X', qui vérifient la condition ci-dessus. C'est ce type de notion que l'on considère en géométrie affine, où les morphismes sont appelés applications affines.

Définition 1.

Considérons deux espaces vectoriels E et E' sur le même corps K et deux espaces affines $\mathcal{E}$ et $\mathcal{E}'$ sur E et E' respectivement. Une application f de $\mathcal{E}$ dans $\mathcal{E}'$ est dite affine, s'il existe une application linéaire v de E dans E' telle que

(1) $$\forall\, M \in \mathcal{E} \quad \forall\, \overrightarrow{x} \in E \quad f(M + \overrightarrow{x}) = f(M) + v(\overrightarrow{x})\,,$$

c'est-à-dire telle que

(2) $$\forall\, \overrightarrow{x} \in E \quad f \circ t_{\vec{x}} = t_{v(\vec{x})} \circ f\,.$$

Nous noterons $\mathcal{A}(\mathcal{E}, \mathcal{E}')$ l'ensemble des applications affines de $\mathcal{E}$ dans $\mathcal{E}'$. Si $\mathcal{E} = \mathcal{E}'$ nous noterons $\mathcal{A}(\mathcal{E})$ cet ensemble.

On peut encore exprimer la condition (1) de la manière suivante : une application f de $\mathcal{E}$ dans $\mathcal{E}'$ est affine si et seulement s'il existe $v \in \mathcal{L}(E, E')$ telle que :

$$\forall M \in \mathcal{E} \quad \forall N \in \mathcal{E} \qquad \overrightarrow{M'N'} = v(\overrightarrow{MN}) \quad \text{où} \quad M' = f(M) \quad \text{et} \quad N' = f(N).$$

Proposition 1.

Dans la définition ci-dessus, l'application linéaire v est unique. Elle est injective (resp. surjective) si et seulement si f est injective (resp. surjective).
Si $\mathcal{E}$ et $\mathcal{E}'$ sont de dimension finie et de même dimension, alors f est injective si et seulement si f est surjective (et alors f est bijective).

Démonstration. Fixons une origine A de $\mathcal{E}$ et posons $A' = f(A)$. A l'aide des bijections $\varphi_A : \overrightarrow{x} \mapsto A + \overrightarrow{x}$ et $\varphi_{A'} : \overrightarrow{y} \mapsto A' + \overrightarrow{y}$, la condition (1) appliquée avec $M = A$, donne $\varphi_{A'}(v(\overrightarrow{x})) = f(\varphi_A(\overrightarrow{x}))$ pour tout $\overrightarrow{x} \in E$. On a donc nécessairement,

$$(3) \qquad v = \varphi_{A'}^{-1} \circ f \circ \varphi_A \qquad \text{et} \qquad f = \varphi_{A'} \circ v \circ \varphi_A^{-1}.$$

Donc v est unique. Les relations ci-dessus montrent que f est injective (resp. surjective) si et seulement si v est injective (resp. surjective).

Si les dimensions des espaces $\mathcal{E}$ et $\mathcal{E}'$ sont finies et égales, la formule du rang, $\dim(\mathrm{Im}(v)) = \dim(E) - \dim(\mathrm{Ker}(v))$ montre que v est surjective si et seulement si elle est injective. ∎

Définition 2.

L'application linéaire v est appelée l'application linéaire associée à f. Nous la noterons v_f.

Proposition 2.

Considérons des espaces vectoriels E, E', E'' sur un même corps K, des espaces affines $\mathcal{E}, \mathcal{E}', \mathcal{E}''$ sur E, E', E'' respectivement, $f \in \mathcal{A}(\mathcal{E}, \mathcal{E}')$, $g \in \mathcal{A}(\mathcal{E}', \mathcal{E}'')$. Alors l'application $g \circ f$ est affine et $v_{g\circ f} = v_g \circ v_f$.

Démonstration. Pour tout $M \in \mathcal{E}$ et pour tout $\overrightarrow{x} \in E$ on a

$$(g \circ f)(M + \overrightarrow{x}) = g(f(M) + v_f(\overrightarrow{x})) = g(f(M)) + v_g(v_f(\overrightarrow{x})),$$

donc $g \circ f$ est affine et l'application linéaire associée est $v_g \circ v_f$. ∎

Considérons des espaces affines $\mathcal{E}$ et $\mathcal{E}'$ de dimensions finies p et q, munis de repères cartésiens $(O, \mathcal{B})$ et $O', \mathcal{B}')$. Considérons une application affine f de $\mathcal{E}$ dans $\mathcal{E}'$. Notons (a_{ij}) la matrice de l'application linéaire v_f dans les bases $\mathcal{B}$ et $\mathcal{B}'$ de E et E'. Introduisons aussi les coordonnées $b_1, \ldots, b_q$ du point $I = f(O)$ dans le repère $(O', \mathcal{B}')$. Alors, tout point $M = O + x_1\overrightarrow{e_1} + \ldots + x_p\overrightarrow{e_p}$ de $\mathcal{E}$ a pour image

$$f(M) = f(O) + v_f(x_1\overrightarrow{e_1} + \ldots + x_p\overrightarrow{e_p}) = O' + \overrightarrow{O'I} + v_f(x_1\overrightarrow{e_1} + \ldots + x_p\overrightarrow{e_p}),$$

de coordonnées :

$$(4) \qquad \begin{cases} x'_1 &= a_{11}x_1 + \ldots + a_{1p}x_p + b_1 \\ \ldots & \ldots \quad \ldots\ldots\ldots\ldots\ldots\ldots \\ x'_q &= a_{q1}x_1 + \ldots + a_{qp}x_p + b_q \end{cases}.$$

Réciproquement, nous allons voir au paragraphe suivant qu'une application qui a une expression de ce type est affine.

6.4 Existence d'applications affines

Proposition.

Soient E, E' des espaces vectoriels sur le même corps K et $\mathcal{E}, \mathcal{E}'$ des espaces affines sur E et E' respectivement. L'application $f \mapsto v_f$ est surjective de $\mathcal{A}(\mathcal{E}, \mathcal{E}')$ sur $\mathcal{L}(E, E')$. Plus précisément, pour tout $A \in \mathcal{E}$, tout $A' \in \mathcal{E}'$ et tout $v \in \mathcal{L}(E, E')$, il existe une application affine f et une seule telle que $f(A) = A'$ et $v_f = v$. Elle est définie par :

$$(1) \qquad \forall M \in \mathcal{E} \qquad f(M) = A' + v(\overrightarrow{AM}).$$

Démonstration. S'il existe $f \in \mathcal{A}(\mathcal{E}, \mathcal{E}')$ telle que $f(A) = A'$ et $v_f = v$, alors d'après 6-3, formules (3), on a $f = \varphi_{A'} \circ v_f \circ \varphi_A^{-1}$, ce qui montre que f est unique. Réciproquement, définissons f en posant $f = \varphi_{A'} \circ v \circ \varphi_A^{-1}$. Alors f est définie par la relation (1) ci-dessus. Vérifions qu'elle est affine. Soient $M \in \mathcal{E}$ et $\overrightarrow{x} \in E$. Posons $N = M + \overrightarrow{x}$. D'après la relation de Chasles on a :

$$\begin{aligned} f(M + \overrightarrow{x}) &= f(N) = A' + v(\overrightarrow{AN}) = A' + v(\overrightarrow{AM} + \overrightarrow{MN}) \\ &= A' + [v(\overrightarrow{AM}) + v(\overrightarrow{MN})] = [A' + v(\overrightarrow{AM})] + v(\overrightarrow{MN}) \\ &= f(M) + v(\overrightarrow{MN}) = f(M) + v(\overrightarrow{x}). \end{aligned}$$

∎

Remarque. Soient $f : \mathcal{E} \to \mathcal{E}'$, $A \in \mathcal{E}$ et $A' = f(A)$. Pour savoir si $f : \mathcal{E} \to \mathcal{E}'$ est affine, il suffit de considérer $M = A + \overrightarrow{x}$ et $M' = f(M)$, pour tout $\overrightarrow{x} \in E$. Si l'application $v : \overrightarrow{x} \mapsto \overrightarrow{x'} = \overrightarrow{A'M'}$ est linéaire de E dans E', alors f est affine.

Corollaire 1.

Soient $\mathcal{E}, \mathcal{E}'$ des espaces affines sur le même corps K de dimensions finies égales. Il existe des applications affines bijectives de $\mathcal{E}$ sur $\mathcal{E}'$.

Démonstration. Puisque $\dim(E) = \dim(E')$, il existe $v \in \mathcal{L}(E, E')$ bijective. Choisissons des origines A et A' de $\mathcal{E}$ et $\mathcal{E}'$. Alors $f = \varphi_{A'} \circ v \circ \varphi_A^{-1}$ est affine de $\mathcal{E}$ dans $\mathcal{E}'$. D'après 6-3, prop. 1, elle est bijective. ∎

Corollaire 2.

Soit $\mathcal{E}$ un espace affine. Pour tout $A \in \mathcal{E}$, tout scalaire λ non nul, l'homothétie $h : M \mapsto A + \lambda \overrightarrow{AM}$, de centre A de rapport λ, est affine et $v_h = \lambda \ Id_E$.

Démonstration. La proposition s'applique en prenant $A' = A$ et $v = \lambda \ \mathrm{Id}_E$. ∎

Corollaire 3.

Supposons $\mathcal{E}$ et $\mathcal{E}'$ de dimensions finies p et q sur le corps K, munis de repères cartésiens $R = (O, \mathcal{B})$ et $R' = (O', \mathcal{B}')$. Une application f de $\mathcal{E}$ dans $\mathcal{E}'$ est affine si et seulement s'il existe une matrice $M = (a_{ij}) \in \mathcal{M}_{p,q}(K)$ et $b_1, \ldots, b_q \in K$ tels que f ait l'expression (4) *obtenue en* 6-3. *Elle est bijective si et seulement si la matrice M est inversible, ce qui nécessite $p = q$.*

Démonstration. Nous avons vu en 6-3 que si f est affine, son expression est donnée par (4). Réciproquement supposons f définie par (4). Appliquons la proposition en prenant $A = O$. Alors, $f(A) = A'$ a pour coordonnées $b_1, \ldots, b_q$. Soit v l'application linéaire

de matrice $M = (a_{ij})$ dans les bases $\mathcal{B}$ et $\mathcal{B}'$. On a $f = \varphi_{A'} \circ v \circ \varphi_A^{-1}$ donc f est affine d'après la proposition. Elle est bijective si et seulement si v_f est bijective, c'est-à-dire si M est inversible. La résolution du système de Cramer (4) exprimera alors $x_1, \ldots, x_p$ en fonction de $x'_1, \ldots, x'_p$, d'où l'expression de f^{-1}. ∎

Exercice. On considère un espace affine $\mathcal{E}$ de dimension 3 sur un corps K, un repère $R = (O, \overrightarrow{\imath}, \overrightarrow{\jmath}, \overrightarrow{k})$ de $\mathcal{E}$, le plan $\mathcal{P}$ d'équation $x - y + z + 2 = 0$ et le vecteur $\overrightarrow{v} = \overrightarrow{\imath} + \overrightarrow{\jmath} + \overrightarrow{k}$. Montrer que la projection f sur $\mathcal{P}$ parallèlement à $\overrightarrow{v}$, la symétrie g par rapport à $\mathcal{P}$ parallèlement à $\overrightarrow{v}$, sont affines.

Solution. Soit $M(x, y, z) \in \mathcal{E}$. La droite $\mathcal{D}$ issue de M dirigée par $\overrightarrow{v}$ est l'ensemble des points $N \in \mathcal{E}$ tels qu'il existe $t \in K$ tel que $\overrightarrow{MN} = t\,\overrightarrow{v}$. On a le paramétrage $N = M + t\,\overrightarrow{v}$ des points de $\mathcal{D}$, soit :

$$(1) \qquad x_N = x + t \quad , \quad y_N = y + t \quad , \quad z_N = z + t\,.$$

Les coordonnées d'un point N commun à $\mathcal{D}$ et $\mathcal{P}$ auront la forme ci-dessus et vérifieront l'équation du plan $\mathcal{P}$. On obtient l'équation au paramètre t,

$$(x + t) - (y + t) + (z + t) + 2 = 0\,,$$

d'où $t = -x + y - z - 2$, puis les coordonnées du projeté $N = f(M) = M + t\,\overrightarrow{v}$ et du symétrique $N' = g(M) = M + 2t\,\overrightarrow{v}$ c'est-à-dire les expressions analytiques de f et de g dans le repère R, qui montrent que f et g sont affines :

$$\begin{cases} x_N = y - z - 2 \\ y_N = -x + 2y - z - 2 \\ z_N = -x + y - 2 \end{cases} \quad , \quad \begin{cases} x_{N'} = -x + 2y - 2z - 4 \\ y_{N'} = -2x + 3y - 2z - 4 \\ z_{N'} = -2x + 2y - z - 4 \end{cases}$$

6.5 Isomorphismes affines

Dans une catégorie mathématique, dont on a défini les objets et les morphismes, on appelle isomorphisme d'un objet X sur un autre X', un homomorphisme $f : X \to X'$ tel qu'il existe un homomorphisme g de X' dans X vérifiant $g \circ f = \mathrm{Id}_X$ et $f \circ g = \mathrm{Id}_{X'}$.

Proposition.

Soit $f : \mathcal{E} \to \mathcal{E}'$ une application affine. Si f est bijective, c'est un isomorphisme affine. Plus précisément, f^{-1} est affine et l'application linéaire associée est v_f^{-1}.

Démonstration. Considérons $M \in \mathcal{E}'$, $\overrightarrow{x} \in E'$ et montrons que $f^{-1}(M + \overrightarrow{x})$ et $f^{-1}(M) + v_f^{-1}(\overrightarrow{x})$ sont égaux. Pour cela, il suffit que leurs images par f soient égales car f est bijective. Or f étant affine, on a

$$f[f^{-1}(M) + v_f^{-1}(\overrightarrow{x})] = f[f^{-1}(M)] + v_f(v_f^{-1}(\overrightarrow{x})) = M + \overrightarrow{x} = f[f^{-1}(M + \overrightarrow{x})]\,.$$ ∎

Corollaire 1.

Soient $f : \mathcal{E} \to \mathcal{E}'$ et $g : \mathcal{E}' \to \mathcal{E}''$ des isomorphismes. Alors $g \circ f$ est un isomorphisme affine de $\mathcal{E}$ sur $\mathcal{E}''$.

Démonstration. Si f et g sont affines bijectives, il en est de même pour $g \circ f$. ∎

Corollaire 2.

Soit $\mathcal{E}$ un espace affine sur l'espace vectoriel E. Fixons une origine A dans $\mathcal{E}$. Alors $\varphi_A : \overrightarrow{x} \mapsto A + \overrightarrow{x}$ est un isomorphisme affine de l'espace affine $\mathcal{E}_E$ sur $\mathcal{E}$.

Démonstration. On sait que φ_A est bijective. Elle est affine car pour tous $\overrightarrow{x}, \overrightarrow{y} \in E$ on a $\varphi_A(\overrightarrow{x} + \overrightarrow{y}) = A + (\overrightarrow{x} + \overrightarrow{y}) = (A + \overrightarrow{x}) + \overrightarrow{y} = \varphi_A(\overrightarrow{x}) + \mathrm{Id}_E(\overrightarrow{y})$. ∎

Corollaire 3.

Soit $\mathcal{E}$ un espace affine de dimension finie n sur le corps K. Alors $\mathcal{E}$ est isomorphe à l'espace affine canonique $\mathcal{E}_n(K)$.

Démonstration. Fixons une base $\mathcal{B} = (\overrightarrow{e_1}, \ldots, \overrightarrow{e_n})$ de E, une origine A de $\mathcal{E}$. Alors $\varphi : (x_1, \ldots, x_n) \mapsto A + x_1\overrightarrow{e_1} + \cdots + x_n\overrightarrow{e_n}$ est un isomorphisme de $\mathcal{E}_n(K)$ sur $\mathcal{E}$. ∎

Remarque. En raison de l'unicité, à isomorphisme près, de l'espace affine de dimension n sur K, on parle de l'espace affine $\mathcal{E}_n(K)$. En géométrie plane on dit "le plan affine" $\mathcal{E}_2(\mathbb{R})$. En géométrie dans l'espace, on dit "l'espace affine" $\mathcal{E}_3(\mathbb{R})$. Toutefois, l'isomorphisme φ du corollaire n'a rien de canonique. Il dépend des choix de l'origine A et de la base $\mathcal{B}$.

Evidemment, cela démystifie la notion d'espace affine. La définition des espaces affines s'exprime dans un formalisme qui paraît savant et compliqué. En fait, nous constatons maintenant que c'est un objet familier : il est isomorphe à un espace vectoriel E que l'on fait agir sur lui-même par translations. Mieux, en dimension finie n, une fois choisie une origine A dans $\mathcal{E}$ et une base $\mathcal{B}$ de E, on peut considérer que l'on est dans K^n avec le vecteur nul pour origine. C'est ce que l'on fait souvent, pour ne pas s'encombrer d'un formalisme qui se révèle un peu excessif. Toutefois, il ne faut pas perdre de vue que dans $\mathcal{E}_n(K)$ l'origine $\overrightarrow{0}$ n'a rien de particulier. Ce n'est qu'un élément parmi les autres, ce qui n'est pas le cas dans l'espace vectoriel E.

Exercice. Dans le plan affine $\mathcal{E}_2(\mathbb{R})$, étudier l'ensemble G des applications affines qui laissent globalement invariant un parallélogramme $P = ABCD$ (non aplati).

Solution. Munissons $\mathbb{R}^2$ d'un produit scalaire et donc $\mathcal{E}_2(\mathbb{R})$ d'une structure euclidienne (voir §3). Soit $(O, \overrightarrow{\imath}, \overrightarrow{\jmath})$ un repère orthonormé. Considérons le carré $C = OIKJ$, où $I = O + \overrightarrow{\imath}$, $J = O + \overrightarrow{\jmath}$. D'après 6-4, il existe une application affine unique g telle que $g(A) = O$, $v_g(\overrightarrow{AB}) = \overrightarrow{\imath}$, $v_g(\overrightarrow{AD}) = \overrightarrow{\jmath}$. Comme v_g applique une base $(\overrightarrow{AB}, \overrightarrow{AD})$ de $\mathbb{R}^2$ sur une autre base $(\overrightarrow{\imath}, \overrightarrow{\jmath})$ de $\mathbb{R}^2$, c'est un automorphisme de l'espace vectoriel $\mathbb{R}^2$. D'après 6-3, g est bijective. C'est un isomorphisme de l'espace affine $\mathcal{E}_2(\mathbb{R})$ sur lui-même. On voit alors qu'une application affine f laisse globalement invariant le parallélogramme P, si et seulement si $g \circ f \circ g^{-1}$ laisse invariant le carré C. Or nous verrons (Ex. 8-2) que les applications affines qui conservent C sont des isométries, qu'elles constituent un groupe fini D_4 ayant 8 éléments. Alors $\varphi : f' \mapsto g^{-1} \circ f' \circ g$ applique D_4 sur G qui est donc un groupe isomorphe à D_4. Bien sûr, transportées par φ les symétries orthogonales du carré deviennent des symétries obliques pour P. En géométrie affine, on n'a pas de produit scalaire et donc pas d'orthogonalité. Il n'y a pas davantage de rotations. On pourra toujours voir la transformation conservant P associée à une rotation conservant C comme composée de symétries obliques, puisqu'en géométrie euclidienne une rotation est la composée de symétries orthogonales convenables.

6.6 Sous-espaces affines

Soient $\mathcal{E}$ un espace affine et E l'espace vectoriel associé. Considérons un sous-espace vectoriel F de E. On peut restreindre à F l'homomorphisme $t : \overrightarrow{x} \mapsto t_{\vec{x}}$ du groupe additif E dans $\mathcal{S}_{\mathcal{E}}$. On obtient ainsi une action du sous-groupe F de E sur $\mathcal{E}$. Cette action de F est libre car l'action de E est libre. Mais si $F \neq E$, elle n'est pas transitive. Les orbites sous cette action de F constituent une partition de $\mathcal{E}$. Par définition d'une orbite, F agit transitivement, et ici librement, sur chacune de ces orbites. Toute orbite pour l'action de F est donc un espace affine sur l'espace vectoriel F.

Définition 1.

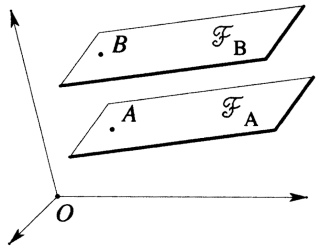
Les orbites pour l'action du sous-espace vectoriel F sur $\mathcal{E}$ sont appelées les sous-espaces affines de $\mathcal{E}$ de direction F.

Ces orbites constituent une partition de $\mathcal{E}$. Par tout point $A \in \mathcal{E}$ il passe donc un sous-espace affine de direction F et un seul : c'est l'orbite de A sous l'action de F,

$$\mathcal{F}_A = \{ A + \overrightarrow{x} ; \ \overrightarrow{x} \in F \}.$$

L'injection naturelle $M \mapsto M$ de $\mathcal{F}_A$ dans $\mathcal{E}$ est affine, l'application linéaire associée est l'injection $\overrightarrow{x} \mapsto \overrightarrow{x}$ de F dans E.

Soit $\mathcal{F}$ un sous-ensemble de $\mathcal{E}$ et soit $A \in \mathcal{F}$. Pour que $\mathcal{F}$ soit un sous-espace affine de $\mathcal{E}$, il faut et il suffit que $F = \{\overrightarrow{AM} ; \ M \in \mathcal{F}\}$ soit un sous-espace vectoriel de E. Alors F est la direction de $\mathcal{F}$.



Si $\mathcal{F}_A$ et $\mathcal{F}_B$ sont les sous-espaces affines de $\mathcal{E}$ de direction F issus de A et B, alors $\mathcal{F}_B$ se déduit de $\mathcal{F}_A$ par la translation de vecteur $\overrightarrow{a} = \overrightarrow{AB}$ car

$$\mathcal{F}_B = \{ B + \overrightarrow{x} ; \ \overrightarrow{x} \in F \} = \{ A + \overrightarrow{AB} + \overrightarrow{x} ; \ \overrightarrow{x} \in F \} = \{ t_{\vec{a}}(A + \overrightarrow{x}) ; \ \overrightarrow{x} \in F \}.$$

Dans le cas de l'espace affine $\mathcal{E}_E$ canonique sur l'espace vectoriel E, les sous-espaces affines de direction F, où F est un sous-espace vectoriel de E, sont aussi les classes du groupe additif E modulo le sous-groupe F.

Les sous-espaces affines de dimension 1 sont appelés les *droites affines de $\mathcal{E}$*, ceux de dimension 2 sont les *plans affines*.

Soient $\mathcal{F}$ et $\mathcal{G}$ des sous-espaces affines de $\mathcal{E}$, de directions F et G. On dit que $\mathcal{F}$ est *parallèle* à $\mathcal{G}$, si on a $F \subset G$. Cette relation binaire est un préordre sur l'ensemble des sous-espaces affines de $\mathcal{E}$. La relation d'équivalence associée (soit $F \subset G$ et $G \subset F$), exprime que $\mathcal{F}$ et $\mathcal{G}$ ont la même direction $F = G$. On la note souvent $\mathcal{F} // \mathcal{G}$.

Proposition.

Soit $(\mathcal{F}_i)_{i\in I}$ une famille de sous-espaces affines de l'espace affine $\mathcal{E}$. Pour $i \in I$, notons F_i la direction de $\mathcal{F}_i$. Si $\bigcap_{i\in I} \mathcal{F}_i$ n'est pas vide, c'est un sous-espace affine de $\mathcal{E}$ de direction $\bigcap_{i\in I} F_i$.

Démonstration. Prenons pour origine de $\mathcal{E}$ un point A de $\bigcap_{i\in I} \mathcal{F}_i$. On a

$$M \in \bigcap_{i\in I} \mathcal{F}_i \quad \Leftrightarrow \quad \forall i \in I \quad M \in \mathcal{F}_i \quad \Leftrightarrow \quad \forall i \in I \quad \overrightarrow{AM} \in F_i \quad \Leftrightarrow \quad \overrightarrow{AM} \in \bigcap_{i\in I} F_i .$$

Cela montre que $\bigcap_{i\in I} \mathcal{F}_i = \{A + \overrightarrow{x}\ ;\quad \overrightarrow{x} \in \bigcap_{i\in I} F_i\}$ est le sous-espace affine de $\mathcal{E}$, passant par A, ayant pour direction le sous-espace vectoriel $\bigcap_{i\in I} F_i$ de E. ∎

Corollaire.

Soit X une partie non vide de l'espace affine $\mathcal{E}$. Il existe un plus petit sous-espace affine $\mathcal{F}$ de $\mathcal{E}$ contenant X, à savoir l'intersection de tous les sous-espaces affines de $\mathcal{E}$ contenant X. Si A est un point de X, alors la direction de $\mathcal{F}$ est le sous-espace vectoriel $F = \mathrm{Vect}\{\overrightarrow{AM}\ ;\ M \in X\}$ de E.

Démonstration. D'après la proposition, l'intersection $\mathcal{F}$ des sous-espaces affines de $\mathcal{E}$ contenant X est un sous-espace affine de $\mathcal{E}$, contenant X. Il est inclus dans tout autre sous-espace affine de $\mathcal{E}$ contenant X, ce qui justifie la première assertion.

Soit A un point de X. La direction F de $\mathcal{F}$ est un sous-espace vectoriel de E qui contient $\overrightarrow{AM}$ pour tout $M \in X$. Il contient donc le sous-espace vectoriel $V = \mathrm{Vect}\{\overrightarrow{AM}\ ;\quad M \in X\}$. Par ailleurs, $A + V$ est un sous-espace affine de $\mathcal{E}$ qui contient tout point $M = A + \overrightarrow{AM}$ de X. Il contient donc $\mathcal{F}$. Ainsi, $V = F$ et $\mathcal{F} = A + V$. ∎

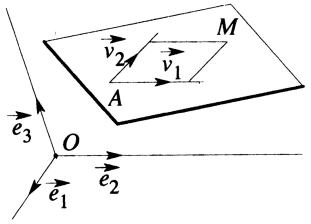
Définition 2.

Ce plus petit sous-espace affine de $\mathcal{E}$ contenant la partie non vide X de $\mathcal{E}$, est appelé le sous-espace affine de $\mathcal{E}$ engendré par X.

Par exemple, si X est constituée de deux points distincts $A, B \in \mathcal{E}$, le sous-espace affine engendré par X est le sous-espace affine issu de A ayant pour direction la droite vectorielle $\{\lambda\,\overrightarrow{AB}\ ;\ \lambda \in K\}$ dirigée par $\overrightarrow{AB}$. C'est la droite (AB).

6.7 Sous-espaces affines en dimension finie

Soit $\mathcal{E}$ un espace affine de dimension finie n, muni d'un repère $R = (O, \overrightarrow{e_1}, \ldots, \overrightarrow{e_n})$. Soient $\mathcal{F}$ un sous-espace affine, F sa direction, $A \in \mathcal{F}$ et $(\overrightarrow{v_1}, \ldots, \overrightarrow{v_k})$ une base de F. Alors, $(A, \overrightarrow{v_1}, \ldots, \overrightarrow{v_k})$ est un repère cartésien de l'espace affine $\mathcal{F}$. Si on connaît les coordonnées des vecteurs $\overrightarrow{OA}, \overrightarrow{v_1}, \ldots, \overrightarrow{v_k}$ dans la base $\mathcal{B} = (\overrightarrow{e_1}, \ldots, \overrightarrow{e_n})$ de E, on a la représentation paramétrique des points M de $\mathcal{F}$:



exemple pour $n = 3$ et $k = 2$

$$\overrightarrow{OM} = \overrightarrow{OA} + t_1\overrightarrow{v_1} + \cdots + t_k\overrightarrow{v_k},$$

où $t_1, \ldots, t_k$ sont les coordonnées de $M \in \mathcal{F}$ dans le repère $(A, \overrightarrow{v_1}, \ldots, \overrightarrow{v_k})$ de $\mathcal{F}$. Dans le repère R de $\mathcal{E}$, les coordonnées de M s'expriment en fonction des coordonnées $a_1, \ldots, a_n$ de A et des coordonnées $b_{1j}, \ldots, b_{nj}$ des vecteurs $\overrightarrow{v_j}$:

$$(1)\qquad \begin{cases} x_1 &= a_1 + b_{11}t_1 + \ldots + b_{1k}t_k \\ \ldots & \ldots \quad \ldots\ldots\ldots\ldots\ldots\ldots \\ x_n &= a_n + b_{n1}t_1 + \ldots + b_{nk}t_k \end{cases}$$

Proposition.

Soient $\mathcal{F}$ un sous-espace affine de dimension k de l'espace affine $\mathcal{E}$ ($\dim(\mathcal{E}) = n$) et $A \in \mathcal{F}$. Il existe des formes linéaires indépendantes $f_1, \dots, f_{n-k}$ telles que $\mathcal{F} = \{M \in \mathcal{E} \mid f_1(\overrightarrow{AM}) = 0, \dots, f_{n-k}(\overrightarrow{AM}) = 0\}$. Réciproquement, soient $A \in \mathcal{E}$ et $f_1, \dots, f_{n-k}$ une famille libre de formes linéaires. Alors les $n-k$ équations $f_1(\overrightarrow{AM}) = 0, \dots, f_{n-k}(\overrightarrow{AM}) = 0$ définissent un sous-espace affine $\mathcal{F}$ de dimension k de $\mathcal{E}$.

Démonstration. Dans la dualité entre E et son dual E^*, la direction F de $\mathcal{F}$, de dimension k, a un orthogonal $F^\perp$ de dimension $n-k$. Il suffit de considérer une base $(f_1, \dots, f_{n-k})$ de $F^\perp$. Alors l'orthogonal $\{f_1, \dots, f_{n-k}\}^\perp$ dans E de cette famille libre de E^* est $(F^\perp)^\perp = F$ d'où la première assertion. Réciproquement, si $(f_1, \dots, f_{n-k})$ est libre dans E^*, alors $F = \{f_1, \dots, f_{n-k}\}^\perp = [\text{Vect}\,((f_i)_{1 \leqslant i \leqslant n-k})]^\perp$ est un sous-espace vectoriel de dimension k de E et on a $\mathcal{F} = A + F$, d'où la proposition. ∎

Définition 2.

Soit $\mathcal{E}$ un espace affine de dimension finie n. On appelle hyperplan de $\mathcal{E}$ un sous-espace affine de $\mathcal{E}$ de dimension $n-1$.

Corollaire.

Soient $\mathcal{E}$ un espace affine de dimension finie n, muni d'une origine O et $\mathcal{H}$ un hyperplan de $\mathcal{E}$, ne passant pas par O. Il existe $f \in E^*$, unique, telle que

$$\mathcal{H} = \{M \in \mathcal{E} \mid f(\overrightarrow{OM}) = 1\}.$$

Démonstration. Soit H la direction $\mathcal{H}$. On a $\dim(H) = n-1$ donc $H^\perp$ est une droite de E^*. Les éléments non nuls de $H^\perp$ sont proportionnels. Si on fixe $A \in \mathcal{H}$, alors il existe $f \in H^\perp$ unique telle que $f(\overrightarrow{OA}) = 1$. ∎

Remarque. Revenons à l'expression paramétrique (1) des points du sous-espace affine $\mathcal{F}$. Rappelons deux méthodes classiques pour éliminer les paramètres $t_1, \dots, t_k$ et obtenir $n-k$ formes linéaires indépendantes donnant, comme dans la proposition, des équations de $\mathcal{F}$. Ces équations sont celles d'hyperplans dont l'intersection est $\mathcal{F}$.

Dans la méthode de Gauss, on choisit des pivots successifs, k pivots ici car $\overrightarrow{v_1}, \dots, \overrightarrow{v_k}$ étant libres, le système est de rang k. Cela détermine k équations principales. L'élimination de $t_1, \dots, t_k$ des $n-k$ équations non principales (ce qui revient à remplacer $t_1, \dots, t_k$ par leurs valeurs tirées des k premières équations), donne $n-k$ conditions pour que le système aux inconnues $t_1, \dots, t_k$ ait des solutions. Ce sont des formes linéaires indépendantes. Elles donnent des équations de $\mathcal{F}$, de la forme :

$$(2) \qquad 0 = a_1(x_1 - a_1) + \cdots + a_n(x_n - a_n).$$

L'autre méthode est celle des déterminants bordants. Puisque $\overrightarrow{v_1}, \dots, \overrightarrow{v_k}$ sont libres, la matrice $(b_{ij}) \in \mathcal{M}_{n,k}(K)$ de leurs coordonnées dans la base $(\overrightarrow{e_1}, \dots, \overrightarrow{e_n})$ est de rang k. Il existe donc un déterminant, de format k, extrait de cette matrice qui est non nul. Le choix d'un tel déterminant détermine k équations principales qui constituent un système de Cramer par rapport aux inconnues $t_1, \dots, t_k$. Quitte à changer la numérotation des vecteurs de base, supposons que les k premières équations soient principales. L'unique solution de ce système de Cramer doit vérifier chacune des équation non principale. Cela se traduit par la nullité de $n-k$ déterminants "bordants". Par exemple, pour que $t_1, \dots, t_k$ vérifient la $(k+1)^{\text{ièmes}}$ équation, on doit avoir :

$$(2) \qquad 0 = \begin{vmatrix} x_1 - a_1 & b_{11} & \cdots & b_{1k} \\ \cdots & \cdots & \cdots & \cdots \\ x_k - a_k & b_{k1} & \cdots & b_{kk} \\ x_{k+1} - a_{k+1} & b_{k+1,1} & \cdots & b_{k+1,k} \end{vmatrix} .$$

On obtient ainsi $n-k$ équations caractérisant les points de $\mathcal{F}$. Les formes linéaires obtenues sont indépendantes car échelonnées dans la base de E^* duale de $\mathcal{B}$ ((2) contient la variable x_{k+1} et pas les suivantes, l'équation qui suit contient x_{k+2} mais pas les suivantes, etc...). Si par exemple $\mathcal{F}$ est un hyperplan, alors $k = n-1$ et on obtient une seule condition, équation de cet hyperplan.

Exercice. Dans l'espace $\mathcal{E} = \mathcal{E}_3(\mathbb{R})$ muni d'un repère cartésien $(O, \overrightarrow{\imath}, \overrightarrow{\jmath}, \overrightarrow{k})$, étudier la courbe (C) définie paramétriquement par :

$$x = 2\cos s + \sin s + 1 \quad , \quad y = \cos s - \sin s + 1 \quad , \quad z = \cos s + 2\sin s + 2 .$$

Solution. Introduisons $\overrightarrow{v_1} = 2\overrightarrow{\imath} + \overrightarrow{\jmath} + \overrightarrow{k}$, $\overrightarrow{v_2} = \overrightarrow{\imath} - \overrightarrow{\jmath} + 2\overrightarrow{k}$ et le point $A(1,1,2)$. Puisque $\begin{vmatrix} 2 & 1 \\ 1 & -1 \end{vmatrix} \neq 0$, la famille $(\overrightarrow{v_1}, \overrightarrow{v_2})$ est libre. C'est une base de $P = \mathrm{Vect}(\overrightarrow{v_1}, \overrightarrow{v_2}) \subset E$. Considérons le plan affine $\mathcal{P}$ de $\mathcal{E}$, de direction P issu de A. Ce plan $\mathcal{P}$ admet pour repère cartésien $R = (A, \overrightarrow{v_1}, \overrightarrow{v_2})$; c'est l'ensemble des points $M = O + \overrightarrow{OA} + t_1\overrightarrow{v_1} + t_2\overrightarrow{v_2}$. Le paramétrage de (C) s'écrit vectoriellement :

$$M = O + \overrightarrow{OA} + \cos(s)\,\overrightarrow{v_1} + \sin(s)\,\overrightarrow{v_2} .$$

On voit que (C) est contenue dans $\mathcal{P}$ et définie paramétriquement dans le repère R de $\mathcal{P}$ par $t_1 = \cos(s)$, $t_2 = \sin(s)$. Elle a pour équation dans ce repère $t_1^2 + t_2^2 = 1$. Elle est donc du genre ellipse. Son centre de symétrie est A et $\overrightarrow{v_1}, \overrightarrow{v_2}$ sont deux diamètres conjugués, axes de symétrie "obliques" (nous sommes en géométrie affine, nous n'avons pas de produit scalaire, ni d'orthogonalité). Le plan $\mathcal{P}$ a pour équation :

$$0 = \det(\overrightarrow{AM}, \overrightarrow{v_1}, \overrightarrow{v_2}) = x - y - z + 2 .$$

6.8 Sous-espaces affines et applications affines

Proposition.

On considère deux espaces vectoriels E, E' sur le corps K, des espaces affines $\mathcal{E}, \mathcal{E}'$ sur E et E' respectivement et $f \in \mathcal{A}(\mathcal{E}, \mathcal{E}')$.

(i) *Soit $\mathcal{F}$ un sous-espace affine de $\mathcal{E}$ de direction F. Alors $f(\mathcal{F})$ est un sous-espace affine de $\mathcal{E}'$ de direction $v_f(F)$.*

(ii) *Soit $\mathcal{F}'$ un sous-espace affine de $\mathcal{E}'$ de direction F'. Si $f^{-1}(\mathcal{F}')$ est non vide, c'est un sous-espace affine de $\mathcal{E}$ de direction $(v_f)^{-1}(F')$.*

(iii) *Soit $g \in \mathcal{A}(\mathcal{E}, \mathcal{E}')$. Si $\{M \in \mathcal{E} \mid f(M) = g(M)\}$ est non vide, c'est un sous-espace affine de $\mathcal{E}$ de direction $\mathrm{Ker}\,(v_f - v_g)$.*

Démonstration. Nous laissons les démonstrations comme exercice au lecteur. ∎

Corollaire 1.

Si f est une application affine, elle conserve le parallélisme.

Démonstration. Cela résulte de l'assertion (i) de la proposition. ∎

Corollaire 2.

Soient $\mathcal{E}$ un espace affine et $f \in \mathcal{A}(\mathcal{E})$. Si l'ensemble des points de $\mathcal{E}$ fixes par f est non vide, c'est un sous-espace affine de $\mathcal{E}$ de direction $Ker(f - Id_E)$.

Corollaire 3.

Soient $\mathcal{E}$ un espace affine et $f \in \mathcal{A}(\mathcal{E})$. Pour tout $M \in \mathcal{E}$, posons $M' = f(M)$.

(i) *Supposons qu'il existe $A \in \mathcal{E}$ tel que $\overrightarrow{AA'} \in Im(v_f - Id_E)$. Alors f admet des points fixes et on a $\overrightarrow{MM'} \in Im(v_f - Id_E)$ pour tout $M \in \mathcal{E}$.*

(ii) *Si f a un point fixe, celui-ci est unique si et seulement si $Ker(v_f - Id_E) = \{0\}$.*

(iii) *Supposons $\mathcal{E}$ de dimension finie. Pour que f admette un point fixe unique, il faut et il suffit que 1 ne soit pas valeur propre de v_f.*

Démonstration. (i) Considérons $A \in \mathcal{E}$. Pour tout $\overrightarrow{x} \in E$ on a :

$$f(A + \overrightarrow{x}) = f(A) + v_f(\overrightarrow{x}) = A' + v_f(\overrightarrow{x}) = A + \overrightarrow{AA'} + v_f(\overrightarrow{x}).$$

Donc f admet un point fixe si et seulement s'il existe $\overrightarrow{x} \in E$ tel que $A + \overrightarrow{x} = f(A + \overrightarrow{x})$, soit si $\overrightarrow{AA'} = (v_f - \mathrm{Id}_E)(-\overrightarrow{x})$. On a alors $\overrightarrow{AA'} \in \mathrm{Im}(v_f - \mathrm{Id}_E)$. Réciproquement, s'il existe $\overrightarrow{y} \in E$ tel que $\overrightarrow{AA'} = (v_f - \mathrm{Id}_E)(\overrightarrow{y})$, alors $I = A + (-\overrightarrow{y})$ est fixe par f.

(ii) Résulte du corollaire 2.

(iii) D'après (ii), la condition est nécessaire. Réciproquement, si $\mathrm{Ker}(v_f - \mathrm{Id}_E) = \{0\}$, d'après le th. du rang : $\mathrm{Im}(v_f - \mathrm{Id}_E) = E$ et f a des points fixes d'après (i). ∎

Exercice. Considérons un espace affine $\mathcal{E}$ de dimension finie, un scalaire λ différent de 0 et de 1. Soit $f \in \mathcal{A}(\mathcal{E})$ telle que $v_f = \lambda\ \mathrm{Id}_E$. Montrer que f est une homothétie et déterminer son centre.

Solution. Puisque 1 n'est pas valeur propre de v_f, f a un point fixe unique I (cor.3, (iii)). On a $I = A + \overrightarrow{x}$ où $\overrightarrow{x}$ est caractérisé par $\overrightarrow{AA'} = -v_f(\overrightarrow{x}) + \overrightarrow{x} = (1 - \lambda)\overrightarrow{x}$, soit $\overrightarrow{x} = \frac{1}{1-\lambda}\overrightarrow{AA'}$. Ainsi $f : M \mapsto f(I + \overrightarrow{IM}) = f(I) + v_f(\overrightarrow{IM}) = I + \lambda\overrightarrow{IM}$ est l'homothétie de centre I de rapport λ.

6.9 Groupe affine

Définition.

Un isomorphisme de l'espace affine $\mathcal{E}$ sur $\mathcal{E}$ est appelé un automorphisme de $\mathcal{E}$. L'ensemble des automorphismes de $\mathcal{E}$, que nous noterons $Aut(\mathcal{E})$, sera appelé le groupe des automorphismes affines de $\mathcal{E}$ ou plus brièvement le groupe affine de $\mathcal{E}$.

Lemme.

Considérons un espace affine $\mathcal{E}$ sur l'espace vectoriel E et une application $f : \mathcal{E} \to \mathcal{E}$. Les conditions suivantes sont équivalentes.

(i) *f est une translation.*

(ii) *f est affine et $v_f = Id_E$.*

(iii) *f commute avec toute translation.*

Démonstration. (i) $\Rightarrow$ (iii) car le groupe T des translations est commutatif.

(iii) $\Rightarrow$ (ii) D'après (iii), la condition (2) de la définition 6-3 est vérifiée :

$$\forall\ \overrightarrow{x} \in E \qquad f \circ t_{\vec{x}} = t_{\vec{x}} \circ f = t_{\mathrm{Id}_E(\vec{x})} \circ f\,.$$

(ii) $\Rightarrow$ (i) Soient $A \in \mathcal{E}$, $A' = f(A)$ et $\overrightarrow{a} = \overrightarrow{AA'}$. Pour tout $M \in \mathcal{E}$, en posant $\overrightarrow{y} = \overrightarrow{AM}$, on obtient en utilisant (ii) :

$$\begin{aligned} f(M) &= f(A + \overrightarrow{y}) = f(A) + v_f(\overrightarrow{y}) = A' + \overrightarrow{y} \\ &= (A + \overrightarrow{AA'}) + \overrightarrow{AM} = (A + \overrightarrow{AM}) + \overrightarrow{AA'} = M + \overrightarrow{AA'} = t_{\vec{a}}(M)\,. \end{aligned}$$

■

Proposition.

Soit $\mathcal{E}$ un espace affine.

(i) *Muni de l'opération de composition $\mathrm{Aut}(\mathcal{E})$ est un groupe.*

(ii) *$\nu : f \mapsto v_f$ est un homomorphisme de groupes, surjectif, de $\mathrm{Aut}(\mathcal{E})$ sur $\mathrm{GL}(E)$.*

(iii) *Le noyau de ν est l'ensemble T des translations de $\mathcal{E}$. C'est un sous-groupe commutatif maximal et distingué de $\mathrm{Aut}(\mathcal{E})$.*

(iv) *Le groupe $\mathrm{Aut}(\mathcal{E})$ est isomorphe au produit semi-direct $E_\alpha \mathrm{GL}(E)$ où α désigne l'action naturelle de $\mathrm{GL}(E)$ sur E définie par $(u, \overrightarrow{x}) \mapsto u(\overrightarrow{x})$.*

Démonstration. (i) D'après 6-5, prop. et cor. 1, $\mathrm{Aut}(\mathcal{E})$ est un groupe.

(ii) D'après 6-3, prop. 2 et prop. 1, ν est un homomorphisme de groupes. D'après 6-4, prop. il est surjectif.

(iii) D'après le lemme, $\mathrm{Ker}(\nu) = \{f \in \mathrm{Aut}(\mathcal{E}) \mid v_f = \mathrm{Id}_E\}$ est l'ensemble T des translations. Donc T est un sous-groupe distingué de $\mathrm{Aut}(\mathcal{E})$. Comme T est l'image du groupe abélien $(E, +)$ par l'homomorphisme $t : \overrightarrow{x} \mapsto t_{\vec{x}}$, c'est un groupe commutatif. Il est commutatif maximal, d'après l'assertion (iii) du lemme.

(iv) Fixons une origine A de $\mathcal{E}$. Le stabilisateur G_A de A dans l'action de $\mathrm{Aut}(\mathcal{E})$ sur $\mathcal{E}$, est un sous-groupe de $\mathrm{Aut}(\mathcal{E})$. D'après 6-4, prop., l'homomorphisme de groupes $f \mapsto v_f$ est une bijection de G_A sur $\mathrm{GL}(E)$. C'est donc un isomorphisme de groupes. Le groupe T des translations est un sous-groupe distingué de $\mathrm{Aut}(\mathcal{E})$, isomorphe au groupe additif E par l'application $\overrightarrow{x} \mapsto t_{\vec{x}}$. On a $G_A \cap T = \{\mathrm{Id}_{\mathcal{E}}\}$ car la seule translation qui fixe A est la translation de vecteur nul. Considérons $f \in \mathrm{Aut}(\mathcal{E})$ et posons $A' = f(A)$. Soit t la translation de vecteur $\overrightarrow{AA'}$. Puisque A est fixe pour $g = t^{-1} \circ f$, on a $g \in G_A$ et $f = t \circ g$. Cela prouve que $\mathrm{Aut}(\mathcal{E}) = TG_A$. Ainsi $\mathrm{Aut}(\mathcal{E})$ est isomorphe au produit semi-direct $T \times_\alpha G_A$ où α est l'homomorphisme de G_A dans $\mathrm{Aut}(T)$ défini par $\alpha(g)(t_{\vec{x}}) = g \circ t_{\vec{x}} \circ g^{-1} = t_{v_g(\vec{x})}$ (d'après 6-3, $g \circ t_{\vec{x}} = t_{v_g(\vec{x})} \circ g$). Identifions E avec T par l'isomorphisme $\vec{x} \mapsto t_{\vec{x}}$. Identifions G_A avec $\mathrm{GL}(E)$ par l'isomorphisme $f \mapsto v_f$. L'action $\alpha : (g, t_{\vec{x}}) \mapsto t_{v_g(\vec{x})}$ apparaît alors comme étant $(v, \vec{x}) \mapsto v(\vec{x})$. ■

Exercice. Déterminer le centre Z de $\mathrm{Aut}(\mathcal{E})$.

Solution. Il suffit de déterminer le centre Z' de $G = E \times_\alpha \mathrm{GL}(E)$, où $\alpha : (\overrightarrow{x}, u) \mapsto u(\overrightarrow{x})$. Soit $(\overrightarrow{x}, u) \in G$. C'est un élément de Z' si pour tout $(\overrightarrow{y}, v) \in G$ les termes

$$(\overrightarrow{x},u)(\overrightarrow{y},v) = (\overrightarrow{x}+u(\overrightarrow{y}),uv) \quad \text{et} \quad (\overrightarrow{y},v)(\overrightarrow{x},u) = (\overrightarrow{y}+v(\overrightarrow{x}),vu).$$

soient égaux. On doit avoir $uv = vu$ pour tout v donc u appartient au centre de $\mathrm{GL}(E)$. Il existe donc $\lambda \in K_*$ tel que $u = \lambda\,\mathrm{Id}_E$ (voir Ex. 1-5). En outre, on doit avoir :

$$\forall\ \overrightarrow{y} \in E \quad \forall\ v \in \mathrm{GL}(E) \qquad \overrightarrow{x} + \lambda\overrightarrow{y} = \overrightarrow{y} + v(\overrightarrow{x}).$$

Avec $\overrightarrow{y} = \overrightarrow{0}$, on obtient $\overrightarrow{x} = v(\overrightarrow{x})$ pour tout $v \in \mathrm{GL}(E)$, d'où $\overrightarrow{x} = \overrightarrow{0}$ et ensuite $\lambda\overrightarrow{y} = \overrightarrow{y}$ pour tout $y \in E$, d'où $\lambda = 1$. Ainsi, $(\overrightarrow{x},u) \in Z'$ si $\overrightarrow{x} = \overrightarrow{0}$ et $u = \mathrm{Id}_E$. Donc $Z' = \{e\}$ et $Z = \{\mathrm{Id}_{\mathcal{E}}\}$.

6.10 Groupe des homothéties et translations

Lemme.

Soient H, K deux groupes et $\varphi \in Hom(K, Aut(H))$ une action de K sur H par automorphismes. On considère le produit semi-direct $G = H \times_\varphi K$. On identifie H et K à des sous-groupes de G par les homomorphismes injectifs $h \mapsto (h,e)$ et $k \mapsto (e,k)$. Soit G_0 un sous-groupe de G, contenant le sous-groupe distingué H de G. Posons $K_0 = G_0 \cap K$. Notons φ_0 la restriction de φ à K_0. Alors $G_0 = H \times_{\varphi_0} K_0$. De plus G_0 est distingué dans G si et seulement si K_0 est distingué dans K.

Démonstration. On a $H \cap K_0 = \{e\}$ car $H \cap K = \{e\}$ et $K_0 \subset K$. Soit $g_0 \in G_0$. Comme $HK = G$, il existe $h \in H$, $k \in K$ tels que $g_0 = hk$. On a $H \subset G_0$ donc $k = h^{-1}g_0 \in G_0 \cap K = K_0$. Cela montre que $G_0 = HK_0$. On a $H \lhd G$ et donc $H \lhd G_0$. Tout cela prouve que G_0 est un produit semi-direct $H \times_{\varphi_0} K_0$, où $\varphi_0 = \varphi|_{K_0}$ est la restriction à K_0 de l'homomorphisme $\varphi : k \mapsto \mathrm{Ad}_k|_H = \varphi(k)$.

Nous laissons la vérification de la dernière assertion comme exercice au lecteur. ∎

Proposition.

Considérons un espace vectoriel E sur le corps K, un espace affine $\mathcal{E}$ sur E et $H = \{ f \in Aut(\mathcal{E}) \mid \exists\,\lambda \in K_* \quad v_f = \lambda\, Id_E \}$.

(i) *H est un sous-groupe distingué de $Aut(\mathcal{E})$.*

(ii) *Le groupe T des translations est un sous-groupe distingué de H.*

(iii) *Pour tout $A \in \mathcal{E}$, le groupe H_A des homothéties de centre A est un sous-groupe de H et les sous-groupes $(H_B)_{B\in\mathcal{E}}$ sont les conjugués de H_A.*

(iv) *H est réunion de T et des sous-groupes $(H_A)_{A\in\mathcal{E}}$.*

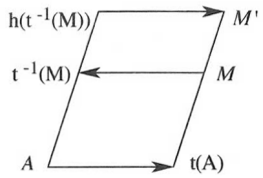
(v) *H est isomorphe au produit semi-direct $E \times_\alpha K_*$ où α désigne l'action naturelle $(\lambda, \overrightarrow{x}) \mapsto \lambda\overrightarrow{x}$ de K_* sur E.*

Démonstration. (i) Le centre du groupe $\mathrm{GL}(E)$ est $Z = \{\lambda\ \mathrm{Id}_E ;\ \lambda \in K_*\}$ (résultat classique ; voir Ex. 1-5). Il est distingué. Donc $H = \nu^{-1}(Z)$, où $\nu : f \mapsto v_f$, est un sous-groupe distingué de $\mathrm{Aut}(\mathcal{E})$.

(ii) D'après le 6-9, lemme, on a $T = \nu^{-1}(\mathrm{Id}_E) = \mathrm{Ker}(\nu) \subset H$ et $T \lhd \mathrm{Aut}(\mathcal{E})$.

(iii) Soit $A \in \mathcal{E}$. L'ensemble des homothéties $h_{A,\lambda} : M \mapsto A + \lambda\overrightarrow{AM}$ de centre A est le stabilisateur $H_A = \{f \in \mathrm{Aut}(\mathcal{E}) \mid f(A) = A \text{ et } \exists\,\lambda \in K_* \quad v_f = \lambda\ \mathrm{Id}_E\}$ de A dans le groupe H.

L'action de H est transitive sur $\mathcal{E}$ puisque $T \subset H$ agit transitivement sur $\mathcal{E}$. Les stabilisateurs H_A et H_B de deux points A et B de $\mathcal{E}$ sont donc conjugués (2-2, prop.). Par exemple, si $t = t_{\vec{a}}$ et $h = h_{A,\lambda}$, la figure montre que :



$$t \circ h_{A,\lambda} \circ t^{-1} = h_{t(A),\lambda}$$

(iv) Soit $f \in H$ avec $f \notin T$. On a $v_f = \lambda \operatorname{Id}_E$, avec $\lambda \neq 1$.
Nous avons vu en 6-8, ex., que f a un point fixe unique A et que $f \in H_A$.

(v) résulte du lemme et de la prop. 6-9, (iv). ∎

Exercice. Montrer que le sous-groupe G de $\operatorname{Aut}(\mathcal{E})$ engendré par l'ensemble S des symétries points s_A, où $A \in \mathcal{E}$, est distingué et décrire G.

Solution. Soient $A \in \mathcal{E}$ et $s = s_A$. Pour tout $M \in \mathcal{E}$, on a $s(M) = A + (-\overrightarrow{AM})$. Ainsi s est une homothétie de rapport -1. On a $s \in \operatorname{Aut}(\mathcal{E})$ et $v_s = -\operatorname{Id}_E$.

Considérons $\overrightarrow{x} \in E$, puis $B = A + \frac{1}{2}\overrightarrow{x}$. Alors $f = s_B \circ s_A = t_{\vec{x}}$.
En effet, $v_f = (-\operatorname{Id}_E) \circ (-\operatorname{Id}_E) = \operatorname{Id}_E$ donc f est une translation et
$f(A) = s_B(A) = B + (-\overrightarrow{BA}) = A + 2\overrightarrow{AB} = A + \overrightarrow{x}$.
Ainsi G contient le sous-groupe T des translations.

Puisque $Z_0 = \{\operatorname{Id}_E, -\operatorname{Id}_E\}$ est un sous-groupe du centre de $\mathrm{GL}(E)$, il est distingué dans $\mathrm{GL}(E)$ donc $\nu^{-1}(Z_0) = \{f \in \operatorname{Aut}(\mathcal{E}) \mid v_f \in Z_0\}$ est un sous-groupe distingué de $\operatorname{Aut}(\mathcal{E})$. D'après la proposition, si $v_f = \operatorname{Id}_E$ alors f est une translation et si $v_f = -\operatorname{Id}_E$ alors f est une homothétie de rapport -1, c'est-à-dire un élément de l'ensemble S. On a donc $\nu^{-1}(Z_0) = T \cup S$. C'est un sous-groupe distingué de $\operatorname{Aut}(\mathcal{E})$. Il est égal à G.

Si le corps est $\mathbb{R}$ et si $\dim(\mathcal{E}) = n$ est finie, alors $\det(v_{s_A}) = (-1)^n$. Tous les éléments de S et donc tous ceux de G, sont directs au sens du paragraphe suivant si et seulement si n est pair.

6.11 Orientation d'un espace affine réel

Définition 1.

Soient E un espace vectoriel de dimension n sur le corps $\mathbb{R}$ et $\mathcal{E}$ un espace affine sur E. Nous dirons qu'un repère cartésien $R = (O, \overrightarrow{e_1}, \ldots, \overrightarrow{e_n})$ de $\mathcal{E}$ est de même orientation qu'un autre repère cartésien $R' = (O', \overrightarrow{e'_1}, \ldots, \overrightarrow{e'_n})$ de $\mathcal{E}$, si l'unique isomorphisme affine f de $\mathcal{E}$ qui applique R sur R' est tel que $\det(v_f)$ soit positif.

Rappelons que deux bases B et B' de l'espace vectoriel réel de dimension finie E sont dites de même orientation, si l'unique isomorphisme v de E qui applique B sur B' est de déterminant positif. Donc deux repères R et R' sont de même orientation si les bases $(\overrightarrow{e_1}, \ldots, \overrightarrow{e_n})$ et $(\overrightarrow{e'_1}, \ldots, \overrightarrow{e'_n})$ de E sont de même orientation.

Proposition 1.

La relation binaire "avoir la même orientation" est une relation d'équivalence sur l'ensemble des repères cartésiens de $\mathcal{E}$. Pour cette relation d'équivalence, il existe deux classes d'équivalence.

Démonstration. Cette relation binaire est réflexive car $\mathrm{Id}_{\mathcal{E}}$ a pour application linéaire associée Id_E. Si $f \in \mathcal{A}(\mathcal{E})$ applique R sur R', alors f^{-1} applique R' sur R et $\det(v_{f^{-1}}) = \det(v_f)^{-1}$ est de même signe que $\det(v_f)$. La relation est donc symétrique. Si $f \in \mathcal{A}(\mathcal{E})$ applique R sur R' et si $g \in \mathcal{A}(\mathcal{E})$ applique R' sur un autre repère R'', d'après 6-3, prop. 2, on a $\det(v_{g\circ f}) = \det(v_g \circ v_f) = \det(v_g)\det(v_f)$. La relation est donc transitive.

Soit $R = (A, \overrightarrow{e_1}, \ldots, \overrightarrow{e_n})$ un repère de $\mathcal{E}$. Le repère $R' = (A, -\overrightarrow{e_1}, \overrightarrow{e_2}, \ldots, \overrightarrow{e_n})$, n'est pas de même orientation que R. Il existe donc au moins deux classes d'équivalence de repères. Pour tout automorphisme affine f de $\mathcal{E}$, le réel $\det(v_f)$ est soit dans $]0, +\infty[$, soit dans $]-\infty, 0[$. Tout repère de $\mathcal{E}$ est donc dans la classe de R ou dans celle de R'. Il existe donc exactement deux classes d'équivalence de repères. ∎

Définition 2.

On dit que l'on oriente $\mathcal{E}$ en choisissant l'une des deux classes d'équivalences précédentes. Il suffit pour cela de donner un repère $R = (O, \overrightarrow{e_1}, \ldots, \overrightarrow{e_n})$ de cette classe. Les repères de la classe choisie sont dits directs, les autres sont dits indirects.

Soit $f \in Aut(\mathcal{E})$ et soit R un repère de $\mathcal{E}$. Si R et $f(R)$ sont de même orientation, on dit que f est direct, sinon on dit que f est indirect.

Remarques. La dernière définition ne dépend pas du repère R choisi. En effet, pour comparer les orientations de R et de $f(R)$, on doit examiner le déterminant des vecteurs de $f(R)$ dans la base $\mathcal{B}$ des vecteurs de R, c'est-à-dire le déterminant de la matrice A de v_f dans la base $\mathcal{B}$. Or si on considère un autre repère $R' = (O', \mathcal{B}')$, la matrice de v_f dans la base $\mathcal{B}'$ est équivalente à A et a le même déterminant (qui est $\det(v_f)$, notion indépendante de la base de E considérée). Ainsi, f est direct si et seulement si $\det(v_f) > 0$.

Soit $R = (O, \mathcal{B})$ un repère. Si on remplace l'origine O, par une autre origine O', le repère $R' = (O', \mathcal{B})$ a la même orientation que R. En fait, c'est le choix de la base $\mathcal{B}$ de E qui donne l'orientation de $\mathcal{E}$.

Proposition 2.

L'ensemble $Aut(\mathcal{E})^+$ des automorphismes affines directs de $\mathcal{E}$ est un sous-groupe distingué d'indice 2 du groupe $Aut(\mathcal{E})$.

Démonstration. D'après 6-9, $\nu : f \mapsto v_f$ est un homomorphisme de $\mathrm{Aut}(\mathcal{E})$ sur $\mathrm{GL}(E)$. Comme $\det : v \mapsto \det(v)$ est un homomorphime de $\mathrm{GL}(E)$ sur $\mathbb{R}^*$, on voit que $\varphi : f \mapsto \det(v_f)$ est un homomorphisme de groupes de $\mathrm{Aut}(\mathcal{E})$ sur $\mathbb{R}^*$. Le sous-groupe $\mathbb{R}_+^* =]0, +\infty[$ de $\mathbb{R}^*$, est distingué puisque $\mathbb{R}^*$ est abélien. Donc $\varphi^{-1}(\mathbb{R}^*) = \mathrm{Aut}(\mathcal{E})^+$ est un sous-groupe distingué de $\mathrm{Aut}(\mathcal{E})$. Dans $\mathrm{Aut}(\mathcal{E})$, les deux classes d'équivalence que donne l'orientation sont également les classes modulo le sous-groupe distingué $\mathrm{Aut}(\mathcal{E})^+$. On a donc $[\mathrm{Aut}(\mathcal{E}) : \mathrm{Aut}(\mathcal{E})^+] = 2$. ∎

Exercice. Soit G un sous-groupe fini, d'ordre impair, de $\mathrm{Aut}(\mathcal{E}_n(\mathbb{R}))$. Montrer que tous les éléments de G sont directs.

Solution. Posons $[G : 1] = 2k+1$. D'après le th. de Lagrange, l'ordre de tout $g \in G$ divise $2k+1$, donc $g^{2k+1} = \mathrm{Id}_{\mathcal{E}}$. On en déduit $1 = \det(\mathrm{Id}_E) = (\det(v_g))^{2k+1}$. On ne peut avoir $\det(v_g) < 0$ donc g est direct. Autrement dit, un automorphisme indirect de $\mathcal{E}_n(\mathbb{R})$ ne peut avoir qu'un ordre pair.

Exercices du chapitre 6

Ex 6 - 1

Soient E, E' des espaces vectoriels sur le même corps, $\mathcal{E}, \mathcal{E}'$ des espaces affines sur E et E'. Pour $(M,N) \in \mathcal{E} \times \mathcal{E}'$ et $(\vec{x},\vec{y}) \in E \times E'$ on pose

(1) $\quad (M,N) + (\vec{x},\vec{y}) = (M+\vec{x}, N+\vec{y})$.

a) Montrer que (1) munit $\mathcal{E} \times \mathcal{E}'$ d'une structure d'espace affine sur $E \times E'$.

b) Montrer que les projections canoniques de $\mathcal{E} \times \mathcal{E}'$ sur $\mathcal{E}$ et $\mathcal{E}'$ sont des applications affines.

c) Soient $A \in \mathcal{E}$ et $B \in \mathcal{E}'$. Montrer que $\mathcal{E} \times \{B\}$ et $\{A\} \times \mathcal{E}'$ sont des sous-espaces affines de $\mathcal{E} \times \mathcal{E}'$ isomorphes à $\mathcal{E}$ et $\mathcal{E}'$ respectivement.

Ex 6 - 2

Dans le plan affine réel $\mathcal{E}$, muni d'un repère cartésien $(O, \overrightarrow{\imath}, \overrightarrow{\jmath})$, on considère la famille $\mathcal{F}$ des coniques $C_{\alpha,\beta}$, où α, β sont deux paramètres réels, d'équations :

$$(1-\alpha)x^2 - 2\beta xy + (1+\alpha)y^2 \\ -2\alpha x - 2\beta y + (\alpha - 1) = 0\,.$$

a) Etudier le genre de $C_{\alpha,\beta}$. Si $\mathcal{E}$ est le plan euclidien et si $(O, \overrightarrow{\imath}, \overrightarrow{\jmath})$ est orthonormé, pour quelles valeurs de (α,β) la conique est elle un cercle ? une hyperbole équilatère ?

b) Si (α,β) décrit la droite D d'équation $ux + vy + w = 0$ de $\mathbb{R}^2$, montrer que le centre de $C_{\alpha,\beta}$ varie sur une conique Σ_D. En examinant ses points à l'infini, deviner le genre de Σ_D en fonction de la position de D dans $\mathbb{R}^2$ et confirmer ces résultats par le calcul.

c) Supposons $\mathcal{E}$ euclidien et $(O, \overrightarrow{\imath}, \overrightarrow{\jmath})$ orthonormé. Quelle est l'enveloppe des axes des paraboles de la famille $\mathcal{F}$?

Ex 6 - 3

Soit $\mathcal{E}$ un espace affine.

a) Dans $G = \mathrm{Aut}(\mathcal{E})$ quels sont les conjugués d'une translation $t_{\vec{a}}$?
Quel est le stabilisateur de $t_{\vec{a}}$?

b) Soit K un sous-groupe de G contenant le sous-groupe T des translations.
Déterminer le centre Z de K.

Ex 6 - 4

Soit $\mathcal{E}$ un espace affine de dimension finie n. Notons $\mathcal{P}$ l'ensemble des applications affines f de $\mathcal{E}$ dans $\mathcal{E}$, telles que $f^2 = f$ et posons $G = \mathrm{Aut}(\mathcal{E})$.

a) Quelle est la nature géométrique des éléments de $\mathcal{P}$.

b) Pour tout $g \in G$, tout $f \in \mathcal{P}$, on pose $g \cdot f = g \circ f \circ g^{-1}$. Vérifier que l'on définit ainsi une action de G sur $\mathcal{P}$.
Quel est le nombre d'orbites ?

Ex 6 - 5

Soient E un espace vectoriel de dimension finie $n \geqslant 1$, $\mathcal{E}$ un espace affine sur E et $A \in \mathcal{E}$. On considère des formes linéaires $f_1, ..., f_k$ sur E et $\alpha_1, ..., \alpha_k \in \mathbb{R}$.

a) $\{M \in \mathcal{E} \mid f_i(\overrightarrow{AM}) = \alpha_i \ \ \forall i = 1, ..., k\}$ est-il un sous-espace affine de $\mathcal{E}$?
Si oui, préciser sa dimension.

b) Dans $\mathcal{E}_4(\mathbb{R})$ muni d'un repère cartésien, étudier l'ensemble $\mathcal{F}$ défini par :

$$\begin{cases} x + y + z + t = 1 \\ 2x - y + 2z - t = -1 \\ -x + 5y - z + 5t = 5 \end{cases}.$$

Exprimer la projection sur $\mathcal{F}$ parallèlement au plan des axes $(z'z)$, $(t't)$.

Ex 6 - 6

a) Etudier la composée $h \circ h'$ de deux homothéties $h = h(A,k)$ et $h' = h(A',k')$ d'un espace affine $\mathcal{E}$.

b) On suppose $kk' \neq 1$. A tout point $M \in \mathcal{E}$ on associe l'unique point fixe $g(M)$ de $h(A,k) \circ h(M,k')$. Montrer que l'application g ainsi définie est affine et caractériser g.

c) Déterminer $\{f \circ h \circ f^{-1}\,;\, f \in \mathrm{Aut}(\mathcal{E})\}$. Quel est le sous-groupe dérivé H' du groupe H des homothéties et translations ?

Ex 6 - 7

Dans le plan affine euclidien, soient $C_1, \ldots, C_n$, des cercles avec C_1 tangent à C_2 en un point I_1, ..., C_{n-1} tangent à C_n en un point I_{n-1} et C_n tangent à C_1 en un point I_n. Pour tout point $M \in C_1$ on considère le point M_2 où la droite (MI_1) recoupe le cercle C_2 ($M_2 = I_1$ si $M_1 = I_1$). De manière analogue, on associe à $M_2 \in C_2$ un point de C_3, etc. Pour finir, on associe à $M_n \in C_n$ le point $M' \in C_1$, où la droite $(M_n I_n)$ recoupe C_1. Préciser la position du point M' par rapport à M sur le cercle C_1.

Ex 6 - 8

Soient E un espace vectoriel réel, $\mathcal{E}$ un espace affine sur E, $\overrightarrow{a} \in E$ non nul, $A \in \mathcal{E}$ et $\lambda \in \mathbb{Q}$, avec $\lambda \notin \{0,1,-1\}$. On veut étudier le sous-groupe G de $\mathrm{Aut}(\mathcal{E})$ engendré par l'homothétie $h(A,\lambda)$ et la translation $t_{\vec{a}}$. On note A_λ l'ensemble des $x \in \mathbb{Q}$ tels qu'il existe $p \in \mathbb{N}$ et $P \in \mathbb{Z}[X]$ tels que $x = \frac{P(\lambda)}{\lambda^p}$.

a) Montrer que A_λ est un sous-anneau du corps $\mathbb{Q}$. Pour $\lambda = \frac{1}{10}$, quel est ce sous-anneau ?

b) Pour tout $k \in \mathbb{Z}$, montrer que $\varphi_k : x \mapsto \lambda^k x$ est un automorphisme du groupe additif A_λ et que $\varphi : k \mapsto \varphi_k$ est une action du groupe additif $\mathbb{Z}$ sur A_λ. Expliciter la loi de composition interne du groupe $\Gamma = A_\lambda \times_\varphi \mathbb{Z}$.

c) Montrer que $\{h_{A,\lambda^k}\,;\, k \in \mathbb{Z}\}$ est un sous-groupe de G isomorphe à $(\mathbb{Z},+)$.

d) Pour tout $\overrightarrow{u} \in E$ et tout $k \in \mathbb{Z}$, montrer que $h_{A,\lambda^k} \circ t_{\vec{u}} \circ h_{A,\lambda^{-k}}$ est une translation dont on précisera le vecteur. En déduire que pour tout $x = \frac{P(\lambda)}{\lambda^p} \in A_\lambda$, on a $t_{x\vec{a}} \in G$.

e) Pour tout $k \in \mathbb{Z}$ et tout $x \in A_\lambda$ on pose $f_{x,k} = t_{x\vec{a}} \circ h_{A,\lambda^k}$. Montrer que $\{f_{x,k}\,;\, x \in A_\lambda, k \in \mathbb{Z}\}$ est égal à G et que G est isomorphe à Γ.

Ex 6 - 9

Notons G le groupe des homéomorphismes de $\mathcal{E} = \mathcal{E}_n(\mathbb{R})$. Montrer que le normalisateur N dans G du groupe T des translations de $\mathcal{E}$ est le groupe $\mathrm{Aut}(\mathcal{E})$.

Ex 6 - 10

On considère des points $I_1, \ldots, I_n$ d'un espace affine $\mathcal{E}$. Déterminer les lignes polygonales $A_1A_2 \ldots A_nA_1$ telles que $I_1, \ldots, I_n$ soient les milieux des côtés A_1A_2, A_2A_3, ..., A_nA_1.

Ex 6 - 11

Soient E un espace vectoriel, $\mathcal{E}$ un espace affine sur E et G le groupe des symétries-point et translations. Déterminer le centre Z et le groupe dérivé G' de G. Montrer que G est isomorphe à un produit semi-direct $E \times_\varphi \mathbb{Z}/2\mathbb{Z}$.

Indications

Ex 6 - 1

Appliquer les définitions.

Ex 6 - 2

a) La conique est de genre ellipse si (α, β) est à l'intérieur du disque unité, de genre hyperbole s'il est à l'extérieur, de genre parabole s'il est sur le cercle unité.

b) L'équation de Σ_D s'obtient en éliminant α et β entre $u\alpha + v\beta + w = 0$ et les relations donnant les coordonnées du centre.

c) Ces axes enveloppent une parabole.

Ex 6 - 3

Pour b), utiliser le fait qu'une application affine qui commute avec toute translation est une translation.

Ex 6 - 4

a) Montrer que $f \in \mathcal{P}$ a des points fixes et que $v_f \in \mathcal{L}(E)$ est un projecteur. Les éléments de $\mathcal{P}$ sont les projections sur les sous-espaces affines de $\mathcal{E}$.

b) Il existe $n+1$ orbites, caractérisées par la dimension de l'image de $f \in \mathcal{P}$.

Ex 6 - 5

a) Si $\mathcal{F} \neq \emptyset$, c'est un sous-espace affine de dimension $n - r$, où r est le rang du système d'équations.

b) Ici, $\mathcal{F} \neq \emptyset$, $r = 2$ et $\dim(\mathcal{F}) = 2$.

Ex 6 - 6

a) Caractériser l'application linéaire associée à $h(A,k) \circ h(A',k')$.

b) g est une homothétie ou constante.

c) $\{ f \circ h \circ f^{-1} ;\ f \in \mathrm{Aut}(\mathcal{E}) \}$ est l'ensemble des homothéties de rapport k et H' est le groupe T des translations.

Ex 6 - 7

On passe de M à M' par une composée de n homothéties. Cette composée laisse globalement invariant le cercle C_1.

Ex 6 - 8

a) Pour $\lambda = \frac{1}{10}$, on obtient l'anneau des nombres décimaux.

b) Vérifier que $\varphi : x \mapsto \lambda x$ est un automorphisme de A_λ et que $\varphi_k = \varphi^k$.

c) Sans difficulté.

d) $f \circ t_{\vec{u}} \circ f^{-1} = t_{v_f(\vec{u})}$ pour $f \in \mathcal{A}(\mathcal{E})$.

e) Utiliser d).

Ex 6 - 9

Pour tout $f \in N$, $f \circ t_{\vec{x}} \circ f^{-1}$ est une autre translation $t_{\vec{y}}$. On peut donc définir une application $u : \overrightarrow{x} \mapsto \overrightarrow{y}$. On vérifiera qu'elle est linéaire. Alors f est affine.

Ex 6 - 10

Si une telle ligne polygonale existe, la composée des symétries par rapport aux points $I_1, \ldots, I_n$ applique A_1 sur A_1.

Ex 6 - 11

$Z = \{ \mathrm{Id}_{\mathcal{E}} \}$ d'après Ex. 6-3, b) et $G' = T$ groupe des translations. Enfin la structure de produit semi-direct découle de 6-10, lemme.

Solutions des exercices du chapitre 6

Ex 6 - 1

a) Plus généralement, si des groupes G, H agissent à droite sur des ensembles X, Y, en posant $(x,y)\cdot(g,h) = (x\cdot g\,,\, y\cdot h)$, on définit une action à droite de $G\times H$ sur $X\times Y$. Si les actions de G sur X et de H sur Y sont transitives (resp. libres), pour tous $x, x'\in X$ et tous $y, y'\in Y$, il existe un (resp. au plus un) $g\in G$ tel que $x' = x\cdot g$ et un (resp. au plus un) $h\in H$ tel que $y' = y\cdot h$. On en déduit qu'il existe un (resp. au plus un) $(g,h)\in G\times H$ tel que $(x',y') = (x,y)\cdot(g,h)$. L'action de $G\times H$ sur $X\times Y$ est transitive (resp. libre), d'où le résultat.

b) La projection $f : (M,N)\mapsto M$ est affine et l'application linéaire associée est la projection $p : (\overrightarrow{x}\,,\overrightarrow{y}\,)\mapsto \overrightarrow{x}$ car pour tous $(M,N)\in\mathcal{E}\times\mathcal{E}'$, $(\overrightarrow{x}\,,\overrightarrow{y}\,)\in E\times E'$,

$$f((M,N)+(\overrightarrow{x}\,,\overrightarrow{y}\,)) = f(M+\overrightarrow{x}\,, N+\overrightarrow{y}\,) = M+\overrightarrow{x} = f(M,N)+p(\overrightarrow{x}\,,\overrightarrow{y}\,).$$

On a un résultat analogue pour la projection sur $\mathcal{E}'$.

c) On peut vérifier de même que $g : M\mapsto (M,B)$ est une application affine de $\mathcal{E}$ dans $\mathcal{E}\times\mathcal{E}'$, d'application linéaire associée $\overrightarrow{x}\mapsto(\overrightarrow{x}\,,\overrightarrow{0}\,)$. Son image $\mathcal{E}\times\{B\}$ est donc un sous-espace affine de $\mathcal{E}\times\mathcal{E}'$. Par ailleurs, directement :

$$\mathcal{E}\times\{B\} = \{(A+\overrightarrow{x}\,,B)\,;\ \overrightarrow{x}\in E\} = \{(A,B)+(\overrightarrow{x}\,,\overrightarrow{0}\,)\,;\ \overrightarrow{x}\in E\}.$$

On reconnaît le sous-espace affine de $\mathcal{E}\times\mathcal{E}'$, issu de (A,B), dont la direction est le sous-espace vectoriel $E\times\{0\}$ de $E\times E'$. De même, $\{A\}\times\mathcal{E}'$ est un sous-espace affine. L'intersection de ces sous-espaces est $\{(A,B)\}$.

Ex 6 - 2

a) Munissons $\mathbb{R}^2$ du produit scalaire canonique. La matrice $A = \begin{pmatrix}1-\alpha & -\beta\\ -\beta & 1+\alpha\end{pmatrix}$ de la forme quadratique $q(x,y) = (1-\alpha)x^2 - 2\beta xy + (1+\alpha)y^2$ est symétrique. Il existe une base orthonormée $\mathcal{B}' = (\overrightarrow{\imath'}\,,\overrightarrow{\jmath'}\,)$ de $\mathbb{R}^2$ qui la diagonalise. Si P est la matrice de passage de $\mathcal{B} = (\overrightarrow{\imath}\,,\overrightarrow{\jmath}\,)$ à $\mathcal{B}'$, on a $A = P\begin{pmatrix}\lambda & 0\\ 0 & \mu\end{pmatrix}P^{-1}$. Dans le repère $(O,\overrightarrow{\imath'}\,,\overrightarrow{\jmath'}\,)$, l'équation de $C_{\alpha,\beta}$ sera de la forme $\lambda x^2+\mu y^2+ax+by+c$. Donc,

$C_{\alpha,\beta}$ est de genre ellipse si et seulement si λ et μ sont non nuls et de même signe, c'est-à-dire si $\det(A)>0$, soit si $\alpha^2+\beta^2<1$,

$C_{\alpha,\beta}$ est de genre hyperbole si λ et μ sont non nuls et de signes opposés, soit si $\det(A)<0$, soit si $\alpha^2+\beta^2>1$,

$C_{\alpha,\beta}$ est de genre parabole si $\det(A)=0$, soit si $\alpha^2+\beta^2=1$.

La conique est un cercle (de rayon réel ou imaginaire) si et seulement si $\lambda=\mu$, c'est-à-dire si le polynôme caractéristique $X^2-\mathrm{tr}(A)X+\det(A) = X^2-2X+1-\alpha^2-\beta^2$ a une racine double, soit si $\alpha^2+\beta^2=0$. Donc $C_{0,0}$ est le seul cercle de cette famille.

La conique est une hyperbole équilatère si et seulement si $\lambda = -\mu$ soit si $\mathrm{tr}(A) = 0$. Ici, $\mathrm{tr}(A) = 2 \neq 0$. Il n'y a pas d'hyperbole équilatère dans la famille.

b) Si la conique $C_{\alpha,\beta}$ a un centre, ses coordonnées sont solution du système :

$$0 = \tfrac{1}{2} f'_x = (1-\alpha)x - \beta y - \alpha \qquad , \qquad 0 = \tfrac{1}{2} f'_y = -\beta x + (1+\alpha)y - \beta$$

Ainsi, α et β sont liés par ces deux relations linéaires et par $u\alpha + v\beta + w = 0$ (avec $u \neq 0$ ou $v \neq 0$). Ces trois équations en α et β sont compatibles si et seulement si

$$\begin{aligned} 0 &= \begin{vmatrix} -(x+1) & -y & x \\ y & -(x+1) & y \\ u & v & w \end{vmatrix} \\ &= (u+w)x^2 + 2vxy + (w-u)y^2 + (u+2w)x + vy + w. \end{aligned}$$

On ne peut avoir $u + w = 0$, $v = 0$, $u - w = 0$ sinon on aurait $u = 0$ et $v = 0$. C'est donc l'équation d'une courbe de degré 2, c'est-à-dire d'une conique Σ_D. Si D coupe le cercle trigonométrique C d'équation $\alpha^2 + \beta^2 = 1$ en deux points (α_1, β_1) et (α_2, β_2), alors C_{α_1,β_1} et C_{α_2,β_2} sont des paraboles, de centres "rejetés à l'infini". On doit s'attendre à trouver deux directions à l'infini pour Σ_D qui devrait donc être du genre hyperbole. Si $D \cap C = \emptyset$, alors Σ_D devrait être du genre ellipse. Si D est tangente à C, alors Σ_D devrait être du genre parabole.

Cela est confirmé par l'étude de la matrice $\begin{pmatrix} w+u & v \\ v & w-u \end{pmatrix}$ dont le déterminant $w^2 - u^2 - v^2$ est négatif si la distance $\frac{|w|}{\sqrt{u^2+v^2}}$ de O à D est inférieure à 1.

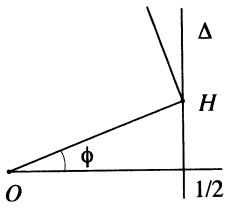
c) D'après a), $C_{\alpha,\beta}$ est une parabole si et seulement si $(\alpha, \beta) \in C$. Il existe alors $\theta \in [0, 2\pi[$ tel que $\alpha = \cos\theta$, $\beta = \sin\theta$. Cherchons l'axe de cette parabole d'équation :

$$\begin{aligned} 0 &= (1-\cos\theta)x^2 - 2\sin\theta\, xy + (1+\cos\theta)y^2 - 2\cos\theta\, x - 2\sin\theta\, y + (\cos\theta - 1) \\ &= 2\sin^2\tfrac{\theta}{2}\, x^2 - 4\sin\tfrac{\theta}{2}\cos\tfrac{\theta}{2}\, xy + 2\cos^2\tfrac{\theta}{2}\, y^2 - 2\cos\theta\, x - 2\sin\theta\, y + (\cos\theta - 1) \end{aligned}$$

La direction asymptotique double est $\sin\frac{\theta}{2}\, x - \cos\frac{\theta}{2}\, y = 0$ de pente $\tan\frac{\theta}{2}$. En coupant la parabole perpendiculairement à cette direction, le milieu du segment obtenu est sur l'axe. En posant $\varphi = \frac{\theta}{2} - \frac{\pi}{2}$, le calcul donne pour équation de l'axe :

$$\cos\varphi\, x + \sin\varphi\, y - \tfrac{1}{2\cos\varphi} = 0.$$

C'est la droite ayant $(\cos\varphi, \sin\varphi)$ pour vecteur normal, telle que la projection H de O sur cette droite vérifie $\overline{OH} = \frac{1}{2\cos\varphi}$. Ainsi H varie sur la droite verticale Δ d'abscisse $1/2$. Les axes des paraboles enveloppent donc la parabole de foyer O de tangente au sommet Δ.



Ex 6 - 3

a) Soient $f \in G = \mathrm{Aut}(\mathcal{E})$ et $\overrightarrow{a} \in E$. L'application $f \circ t_{\vec{a}} \circ f^{-1}$ est une translation $t_{\vec{b}}$ car le sous-groupe T des translations est distingué. Soit $A \in \mathcal{E}$, on a

$$(f \circ t_{\vec{a}} \circ f^{-1})(f(A)) = f \circ t_{\vec{a}}(A) = f(A + \overrightarrow{a}) = f(A) + v_f(\overrightarrow{a}).$$

On a donc $\overrightarrow{b} = v_f(\overrightarrow{a})$. On sait que $v : f \mapsto v_f$ est surjective, de G sur $\mathrm{GL}(E)$. Si $\overrightarrow{a} \neq \overrightarrow{0}$ alors $\{v_f(\overrightarrow{a})\,;\ f \in \mathrm{Aut}(\mathcal{E})\} = E \setminus \{0_E\}$. L'orbite de $t_{\vec{a}}$ est donc

$T \setminus \{\mathrm{Id}_{\mathcal{E}}\}$. Le stabilisateur de $t_{\vec{a}}$ est l'ensemble des $f \in G$ tels que $v_f(\overrightarrow{a}) = \overrightarrow{a}$. Si $\overrightarrow{a} = \overrightarrow{0}$, alors $t_{\vec{a}} = \mathrm{Id}_{\mathcal{E}}$. L'ensemble des conjugués de $t_{\vec{a}}$ est $\{\mathrm{Id}_{\mathcal{E}}\}$. Le stabilisateur de $t_{\vec{a}}$ est G.

b) Soit $g \in Z$. On a $T \subset K$ donc g commute avec toute translation. D'après 6-9, lemme, g est une translation $t_{\vec{a}}$. Pour tout $f \in K$ on doit avoir $f \circ t_{\vec{a}} \circ f^{-1} = t_{\vec{a}}$ et donc $v_f(\overrightarrow{a}) = \overrightarrow{a}$. Soit $E_0 = \{\overrightarrow{a} \in E \mid \forall f \in K \ \ v_f(\overrightarrow{a}) = \overrightarrow{a}\}$. Le centre Z de K est l'ensemble des translations $t_{\vec{a}}$, où $\overrightarrow{a} \in E_0$. Par exemple, si $K = \mathrm{Aut}(\mathcal{E})$, alors $E_0 = \{\overrightarrow{0}\}$. On retrouve que le centre de $\mathrm{Aut}(\mathcal{E})$ est $\{\mathrm{Id}_{\mathcal{E}}\}$ (voir 6-9, ex.).

Ex 6 - 4

a) Soit $f \in \mathcal{P}$. Pour tout $M \in \mathcal{E}$, on a $f(f(M)) = f(M)$. Tout point de $\mathcal{F} = \mathrm{Im}(f)$ est donc fixe par f. Réciproquement, tout point fixe appartient à l'image de f. Notons E l'espace vectoriel direction de $\mathcal{E}$. On a $v_f = v_{f^2} = v_f^2$ donc v_f est un projecteur de $\mathcal{L}(E)$. Il est alors classique que E est la somme directe $E_1 \oplus E_0$ des sous-espaces propres du projecteur v_f relatifs aux valeurs propres 1 et 0. Soit $A \in \mathcal{F}$. D'après 6-8, cor. 2, on a $\mathcal{F} = A + E_1$. Pour tout $M \in \mathcal{E}$, posons $\overrightarrow{AM} = \overrightarrow{x} = \overrightarrow{x_1} + \overrightarrow{x_0}$, où $\overrightarrow{x_1} \in E_1$ et $\overrightarrow{x_0} \in E_0$. On a

$$f(M) = f(A + \overrightarrow{AM}) = f(A) + v_f(\overrightarrow{AM}) = f(A) + \overrightarrow{x_1} = A + \overrightarrow{x_1}.$$

Ainsi, f est la projection de $\mathcal{E}$ sur $\mathcal{F}$ parallèlement à la direction E_0.

b) D'abord, $(g, f) \mapsto g \cdot f = g \circ f \circ g^{-1}$ est une action à gauche de G sur l'ensemble $\mathcal{A}(\mathcal{E})$ des applications affines de $\mathcal{E}$ dans $\mathcal{E}$. En effet, $g \circ f \circ g^{-1} \in \mathcal{A}(\mathcal{E})$ et on a :

$$\forall f \in \mathcal{A}(\mathcal{E}) \quad \mathrm{Id}_{\mathcal{E}} \cdot f = f,$$

$$\forall g \in G \ \forall g' \in G \ \forall f \in \mathcal{A}(\mathcal{E}) \ \ g \cdot (g' \cdot f) = g(g' f g'^{-1}) g^{-1} = (gg') f (gg')^{-1} = gg' \cdot f.$$

Pour cette action, la partie $\mathcal{P}$ de $\mathcal{A}(\mathcal{E})$ est stable : si $f^2 = f$, alors $(g \circ f \circ g^{-1})^2 = g \circ f \circ g^{-1}$. On a donc une action de G sur $\mathcal{P}$. Soient $f \in \mathcal{P}, g \in G$. L'image de $g \circ f \circ g^{-1}$ est $g(f(\mathcal{E}))$ de même dimension que $f(\mathcal{E})$ car g est un isomorphisme. Réciproquement, considérons $f' \in \mathcal{P}$ tel que $f'(\mathcal{E})$ et $f(\mathcal{E})$ aient la même dimension k. Les projecteurs $v_{f'}$ et v_f sont associés à des décompositions en somme directe $E = E_1' \oplus E_0'$ et $E = E_1 \oplus E_0$ avec $\dim(E_1') = \dim(E_1) = k$ et $\dim(E_0') = \dim(E_0) = n - k$. Si on choisit des bases $(\overrightarrow{e_1}, \ldots, \overrightarrow{e_k})$ et $(\overrightarrow{f_1}, \ldots, \overrightarrow{f_k})$ de E_1 et E_1' et des bases $(\overrightarrow{e_{k+1}}, \ldots, \overrightarrow{e_n})$ et $(\overrightarrow{f_{k+1}}, \ldots, \overrightarrow{f_n})$ de E_0 et E_0' il existe un automorphisme v de l'espace vectoriel E tel que $v(\overrightarrow{e_i}) = \overrightarrow{f_i}$ pour tout $i = 1, \ldots, n$. Choisissons $A \in \mathcal{F}$ et $A' \in \mathcal{F}'$. D'après 6-4, prop., il existe $g \in G$ unique tel que $g(A) = A'$ et $v_g = v$ (6-4, prop.). On a alors $g \circ f \circ g^{-1}(A') = A'$ et $v_{g \circ f \circ g^{-1}} = v_{f'}$ et donc $g \circ f \circ g^{-1} = f'$. Ainsi, les éléments de l'orbite de $f \in \mathcal{P}$ sont caractérisés par la dimension de l'image de f. On a donc $n + 1$ orbites.

Ex 6 - 5

a) $F = \cap \mathrm{Ker}\,(f_i)$ est le sous-espace vectoriel $\{f_1, \ldots, f_k\}^\perp$ de E, orthogonal de la partie $\{f_1, \ldots, f_k\}$ de E^*. L'orthogonal $F^\perp = \{f_1, \ldots, f_k\}^{\perp\perp}$ de F dans le dual E^* de E est le sous-espace vectoriel engendré par $f_1, \ldots f_k$. Sa dimension est le rang r de $\{f_1, \ldots, f_k\}$. La dimension de son orthogonal F dans E est $n - r$.

Dans l'espace affine $\mathcal{E}$, les hyperplans d'équations $f_i(\overrightarrow{AM}) = \alpha_i$ peuvent avoir une intersection vide (par exemple dans $\mathcal{E}_3(\mathbb{R})$ si trois plans sont parallèles ou si leurs directions contiennent une même droite). Si leur intersection est non vide, c'est un sous-espace affine de direction F, de dimension r.

b) Par exemple, la méthode du pivot de Gauss montre que le système des trois équations est compatible, de rang 2 et que les deux premières formes linéaires sont indépendantes (d'ailleurs, on a $\begin{vmatrix} 1 & 1 \\ 2 & -1 \end{vmatrix} = -3 \neq 0$). Les trois hyperplans ont donc une intersection $\mathcal{F}$ non vide, égale à l'intersection des deux premiers hyperplans. C'est un sous-espace affine de $\mathcal{E}$ de dimension $4 - 2 = 2$. Sa direction admet pour équations $x + z = 0$, $y + t = 0$ et pour base $(\overrightarrow{u} = (1, 0, -1, 0), \overrightarrow{v} = (0, 1, 0, -1))$. Notons (e_i) la base canonique de $\mathbb{R}^4$. Comme $\overrightarrow{u}$, $\overrightarrow{v}$, $\overrightarrow{e}_3$, $\overrightarrow{e}_4$ sont libres (leur déterminant vaut $1 \neq 0$), on a $\mathbb{R}^4 = F \oplus F'$, où F' est engendré par $\overrightarrow{e}_3$, $\overrightarrow{e}_4$. La projection p sur $\mathcal{F}$ parallèlement à F' existe donc. Pour tout $M(x, y, z, t)$, un point $P(x, y, z + \lambda, t + \mu)$ du plan parallèle à F' issu de M appartient à $\mathcal{F}$ si $\lambda = -x - z$, $\mu = 1 - y - t$, d'où les coordonnées de P, c'est-à-dire l'expression analytique de p :

$$X = x \quad , \quad Y = y \quad , \quad Z = -x \quad , \quad T = -y + 1.$$

Ex 6 - 6

a) $v_{h \circ h'} = v_h \circ v_{h'} = (k\ \mathrm{Id}_E) \circ (k'\ \mathrm{Id}_E) = kk'\ \mathrm{Id}_E$.

- Si $kk' = 1$, alors $h \circ h'$ est une translation (6-9, lemme). On a :

$$(h \circ h')(A') = h(A') = A + k\overrightarrow{AA'} = A' + \overrightarrow{A'A} + k\overrightarrow{AA'}.$$

Le vecteur de la translation est donc $\overrightarrow{a} = (k - 1)\overrightarrow{AA'}$.

- Si $kk' \neq 1$, alors $h \circ h'$ admet un unique point fixe I (6-8, cor. 3) et $h \circ h'$ est une homothétie (6-10, prop. (iv)). Donc $h \circ h' = h(I, kk')$. On doit avoir :

$$\begin{aligned} I &= (h \circ h')(I) = h[h'(A' + \overrightarrow{A'I})] = h(A' + k'\overrightarrow{A'I}) = h(A + \overrightarrow{AA'} + k'\overrightarrow{A'I}) \\ &= A + k(\overrightarrow{AA'} + k'\overrightarrow{A'I}) = I + \overrightarrow{IA} + k(\overrightarrow{AA'} + k'\overrightarrow{A'A} + k'\overrightarrow{AI}). \end{aligned}$$

Ainsi $\overrightarrow{AI} = \frac{k(1-k')}{1-kk'}\overrightarrow{AA'}$. Notons que si $k' = 1$, on a évidemment $I = A$.

b) L'application g associe à $M = A'$ le point I. Si $k' \neq 1$, c'est donc l'homothétie de centre A, de rapport $\frac{k(1-k')}{1-kk'}$. Si $k' = 1$, c'est l'application constante de valeur A.

c) $g = f \circ h \circ f^{-1}$ est affine et bijective car f et g le sont. Elle laisse fixe le point $B = f(A)$ et on a $v_g = v_f \circ k\,\mathrm{Id}_E \circ v_f^{-1} = k\,\mathrm{Id}_E$. Donc $g = h(B,k)$. Si f décrit $\mathrm{Aut}(\mathcal{E})$, l'ensemble des conjugués $f \circ h \circ f^{-1} = h(f(A),k)$ décrit l'ensemble de toutes les homothéties de rapport k. En effet, pour tout $B \in \mathcal{E}$, il existe $f \in \mathrm{Aut}(\mathcal{E})$ telle que $f(A) = B$ (par exemple la translation de vecteur $\overrightarrow{AB}$).

Soient $f \in \mathrm{Aut}(\mathcal{E})$ et $h \in H$ de rapport k. Alors $f' = f \circ h \circ f^{-1} \circ h^{-1}$ a pour application linéaire associée $v_f \circ k\,\mathrm{Id}_E \circ v_f^{-1} \circ k^{-1}\,\mathrm{Id}_E = \mathrm{Id}_E$. C'est donc une translation $t_{\vec{a}}$. On a donc $H' \subset T$.

Si $h = t_{\vec{x}}$ est une translation, on a $f' = v_f \circ t_{\vec{x}} \circ v_f^{-1} \circ t_{-\vec{x}} = t_{v_f(\vec{x})-\vec{x}}$. Pour tout $a \in E$ en prenant pour f une homothétie de rapport $\lambda \neq 1$ et $\overrightarrow{x} = \frac{1}{\lambda-1}\overrightarrow{a}$, on aura $f' = t_{\vec{a}}$. Donc $H' = T$.

Si $h = h(A,k)$ est une homothétie, avec $k \neq 1$, en posant $B = f(A)$,

$$f'(A) = h(f(A),k) \circ h(A,k^{-1})(A) = f(A) + k\overrightarrow{BA} = A + \overrightarrow{AB} - k\overrightarrow{AB}.$$

Donc $\overrightarrow{a} = (1-k)\overrightarrow{AB}$. Pour tout $\overrightarrow{a} \in E$, on peut choisir $f \in H$ tel que $B = f(A)$ vérifie $(1-k)\overrightarrow{AB} = \overrightarrow{a}$, par exemple f peut être une homothétie. Ainsi, toute translation est également le commutateur de deux homothéties.

Ex 6 - 7

Notons r_i le rayon du cercle C_i. L'image de M par l'homothétie $h_1 = h(I_1, -\frac{r_2}{r_1})$ est M_2. On a une situation analogue pour les applications suivantes. La dernière, qui applique M_n sur M' est l'homothétie $h_n = h(I_n, -\frac{r_1}{r_n})$. On passe de M à M' par la composée $h = h_n \circ \cdots \circ h_1$ qui est un élément du groupe H des homothéties et translations. Comme h applique C_1 sur C_1, elle laisse fixe le centre de C_1 et son rapport k est en valeur absolue égal à 1 (rapport du rayon de C_1 à lui-même). Ce rapport est aussi le produit $(-\frac{r_1}{r_n}) \cdots (-\frac{r_2}{r_1})$ des rapports. Si n est pair, k est positif et vaut 1. Alors h est une translation qui laisse fixe le centre de C_1, c'est-à-dire l'identité. Si n est impair, alors k est négatif et vaut -1. Dans ce cas, h est la symétrie par rapport au centre de C_1 et M' est diamétralement l'opposé de M.

Notons que dans l'espace, en remplaçant les cercles par des sphères successivement tangentes entre elles, on aurait une réponse analogue au problème analogue.

Ex 6 - 8

a) On a $A_\lambda \neq \emptyset$ car $\mathbb{Z} \subset A_\lambda$. Soient $x = \frac{P(\lambda)}{\lambda^p} \in A_\lambda, y = \frac{Q(\lambda)}{\lambda^q} \in A_\lambda$, avec $P, Q \in \mathbb{Z}[X]$ et $p, q \in \mathbb{N}$. Posons $r = p + q \in \mathbb{N}$ et $R(X) = X^q P(X) - X^p Q(X) \in \mathbb{Z}[X]$.

$$x - y = \frac{P(\lambda)}{\lambda^p} - \frac{Q(\lambda)}{\lambda^q} = \frac{\lambda^q P(\lambda) - \lambda^p Q(\lambda)}{\lambda^{p+q}} = \frac{R(\lambda)}{\lambda^r} \in A_\lambda \qquad , \qquad xy = \frac{P(\lambda)Q(\lambda)}{\lambda^r} \in A_\lambda .$$

Donc A_λ est un sous-anneau de $\mathbb{Q}$ et $1 = \frac{1}{\lambda^0} \in A_\lambda$. Pour $\lambda = \frac{1}{10}$, ce sous-anneau de $\mathbb{Q}$ est l'ensemble des nombres décimaux. (Un nombre rationnel est dit décimal s'il est la classe d'une fraction $\frac{m}{10^k}$, où $m \in \mathbb{Z}$, $k \in \mathbb{N}$.)

b) $\varphi_1 : x \mapsto \lambda x$ est un endomorphisme du groupe additif A_λ car le produit de l'anneau A_λ distribue l'addition. Il est bijectif, d'application réciproque $x \mapsto \frac{1}{\lambda}x$. C'est un automorphisme du groupe A_λ.

D'après la propriété universelle du groupe symétrisé $\mathbb{Z}$ de $\mathbb{N}$, il existe un homomorphisme $\varphi : k \mapsto \varphi_1^k$ de $\mathbb{Z}$ sur le sous-groupe $\langle\varphi_1\rangle$ de $\mathrm{Aut}(A_\lambda)$.

Soit $x \in A_\lambda$. On voit par récurrence, que $\varphi_1^k(x) = \lambda^k x = \varphi_k(x)$ pour tout $k \in \mathbb{N}$. Pour $k < 0$ dans $\mathbb{Z}$. On a $\varphi_1^k(x) = (\varphi_1^{-1})^{|k|}(x) = \frac{1}{\lambda}^{|k|} x = \lambda^k x = \varphi_k(x)$.

Donc $\varphi_1^k = \varphi_k$ pour tout $k \in \mathbb{Z}$ et $\varphi : k \mapsto \varphi_k$ est un homomorphisme de $\mathbb{Z}$ sur $\langle\varphi_1\rangle \in \mathrm{Aut}(A_\lambda)$, c'est-à-dire une action par automorphismes de $\mathbb{Z}$ sur le groupe A_λ. On peut donc considérer $\Gamma = A_\lambda \times_\varphi \mathbb{Z}$. Sa loi de composition est définie par

$$(x,k) * (y,m) = (x + \varphi^k(y), k+m) = (x + \lambda^k y, k+m).$$

c) On a $h_{A,\lambda} \in G \subset \mathrm{Aut}(\mathcal{E})$. L'application $\psi : k \mapsto (h_{A,\lambda})^k = h_{A,\lambda^k}$, est un homomorphisme de $\mathbb{Z}$ sur le sous-groupe $\langle h_{A,\lambda}\rangle$ de G engendré par $h_{A,\lambda}$. Le noyau de ψ est l'ensemble des $k \in \mathbb{Z}$ tels que $h_{A,\lambda^k} = \mathrm{Id}_\mathcal{E}$, c'est-à-dire tels que $\lambda^k = 1$. Comme $|\lambda| \neq 1$, la condition $|\lambda|^k = 1$ implique $k = 0$. Donc ψ est injectif. C'est un isomorphisme de $\mathbb{Z}$ sur $\psi(\mathbb{Z}) = \langle h_{A,\lambda}\rangle$.

d) Si f est affine, il existe $v = v_f \in \mathcal{L}(E)$ telle que $f \circ t_{\vec{u}} = t_{v(\vec{u})} \circ f$ pour tout $\overrightarrow{u} \in E$. Avec $f = h_{A,\lambda^k}$ et $\overrightarrow{u} = \overrightarrow{a}$, on a $v_f = \lambda^k \mathrm{Id}_E$ et donc $h_{A,\lambda^k} \circ t_{\vec{a}} \circ h_{A,\lambda^{-k}} = t_{\lambda^k \vec{a}}$. D'après c), $t_{\lambda^k\vec{a}} \in G$. On en déduit que pour $b \in \mathbb{Z}$, on a $t_{b\lambda^k\vec{a}} = (t_{\lambda^k\vec{a}})^b \in G$.

Si $P(X) = b_0 + b_1 X + \cdots + b_n X^n$, alors $x = \frac{P(\lambda)}{\lambda^k} = b_0\lambda^{-k} + \cdots + b_n\lambda^{n-k}$ et donc $t_{x\vec{a}} = t_0 \circ \cdots \circ t_n$, où pour $j = 0, \ldots, n$ on pose $t_j = [t_{\lambda^{j-k}\vec{a}}]^{b_j}$. On a $t_{\lambda^{j-k}\vec{a}} \in G$ et donc $t_{x\vec{a}} \in G$.

e) Pour $k, m \in \mathbb{Z}$, $x, y \in A_\lambda$, on obtient en utilisant d) :

$$\begin{aligned} f_{x,k} \circ f_{y,m} &= [t_{x\vec{a}} \circ h_{A,\lambda^k}] \circ [t_{y\vec{a}} \circ h_{A,\lambda^m}] \\ &= t_{x\vec{a}} \circ [h_{A,\lambda^k} \circ t_{y\vec{a}} \circ h_{A,\lambda^{-k}}] \circ h_{A,\lambda^k} \circ h_{A,\lambda^m} \\ &= t_{x\vec{a}} \circ t_{\lambda^k y\vec{a}} \circ h_{A,\lambda^{k+m}} = f_{x+\lambda^k y, k+m}. \end{aligned}$$

Cela prouve que $f_{x,k} \circ f_{y,m} = f_{z,l}$ où $(z,l) = (x + \lambda^k y, k+m) = (x,k) * (y,m)$. Donc $\theta : (x,k) \mapsto f_{x,k}$ est un homomorphisme de groupes, à valeurs dans G d'après d). Son image est un sous-groupe de G contenant $t_{\vec{a}}$ et $h_{A,\lambda}$. C'est donc tout G. Vérifions que θ est injectif. Ce sera un isomorphisme. On a :

$$f_{x,k} \in \mathrm{Ker}(\theta) \quad \Leftrightarrow \quad t_{x\vec{a}} \circ h_{A,\lambda^k} = \mathrm{Id}_\mathcal{E}.$$

L'application linéaire associée $\lambda^k \mathrm{Id}_E$ doit être égale à Id_E. Cela necessite $\lambda^k = 1$ et donc $k = 0$ (voir c)). Ensuite $t_{x\vec{a}} = \mathrm{Id}_\mathcal{E}$ nécessite $x\vec{a} = \vec{0}$ et donc $x = 0$.

Ex 6 - 9

Soit $f \in N$. On a $f \circ t_{\vec{x}} \circ f^{-1} \in T$ pour tout $\overrightarrow{x} \in E$. Il existe donc $\overrightarrow{y} \in E$ unique tel que $f \circ t_{\vec{x}} \circ f^{-1} = t_{\vec{y}}$. Posons $\overrightarrow{y} = u(\overrightarrow{x})$. Cela définit une application u de E dans E, caractérisée par le fait que $f \circ t_{\vec{x}} \circ f^{-1} = t_{u(\vec{x})}$ pour tout $\overrightarrow{x} \in E$ ou encore par la condition $f \circ t_{\vec{x}} = t_{u(\vec{x})} \circ f$ pour tout $\overrightarrow{x} \in E$.

Vérifions que u est linéaire. Alors f sera affine, d'application linéaire associée u. De plus, l'homéomorphisme f étant bijectif, f sera élément de $\mathrm{Aut}(\mathcal{E})$.

Soient $\overrightarrow{a} \in E$, $\overrightarrow{b} \in E$. On a :

$$f \circ t_{\vec{a}+\vec{b}} \circ f^{-1} = f \circ t_{\vec{a}} \circ t_{\vec{b}} \circ f^{-1} = (f \circ t_{\vec{a}} \circ f^{-1}) \circ (f \circ t_{\vec{b}} \circ f^{-1}) = t_{u(\vec{a})} \circ t_{u(\vec{b})} = t_{u(\vec{a})+u(\vec{b})}.$$

Cela prouve que $u(\overrightarrow{a} + \overrightarrow{b}) = u(\overrightarrow{a}) + u(\overrightarrow{b})$ pour tout $\overrightarrow{a} \in E$ et pour tout $\overrightarrow{b} \in E$. Il en résulte que $u(k\overrightarrow{a}) = ku(\overrightarrow{a})$ pour tout $k \in \mathbb{N}$, puis pour tout $k \in \mathbb{Q}$. Si nous montrons que u est continue, par passage à la limite la relation sera valable pour $k \in \mathbb{R}$ et u sera linéaire. Soit $B \in \mathcal{E}$ et posons $A = f^{-1}(B)$. D'après la définition de u,

$$B + u(\overrightarrow{a}) = t_{u(\vec{a})}(B) = f \circ t_{\vec{a}} \circ f^{-1}(B) = f(A + \overrightarrow{a}).$$

Cela prouve que $u = \varphi_B^{-1} \circ f \circ \varphi_A$, où $\varphi_A = \overrightarrow{x} \mapsto A + \overrightarrow{x}$ désigne la bijection de $\mathbb{R}^n$ sur $\mathcal{E}$ associée au choix de l'origine A. Comme φ_A est un homéomorphisme de $\mathbb{R}^n$ sur $\mathcal{E}$ (voir 8-1), u est un homéomorphisme. En conclusion, on a $N \subset \mathrm{Aut}(\mathcal{E})$.

Inversement, on a $\mathrm{Aut}(\mathcal{E}) \subset N$ car $T \lhd \mathrm{Aut}(\mathcal{E})$. Ainsi $N = \mathrm{Aut}(\mathcal{E})$.

Ex 6 - 10

La composée f des symétries par rapport aux points $I_1, \ldots, I_n$ a pour application linéaire associée $v_f = (-\mathrm{Id}_E)^n$. Si n est pair f est une translation, si n est impair, on a $v_f = -\mathrm{Id}_E$ et alors f est une symétrie par rapport à un point K.

Si $n = 2k$ est pair, on a $s_{I_2} \circ s_{I_1} = t_{\vec{a_1}}, \ldots, s_{I_{2k}} \circ s_{I_{2k-1}} = t_{\vec{a_k}}$, avec $\overrightarrow{a_1} = 2\overrightarrow{I_1I_2}, \ldots, \overrightarrow{a_k} = 2\overrightarrow{I_{2k-1}I_{2k}}$. Ainsi, $f = t_{\vec{a}}$, avec $\overrightarrow{a} = 2(\overrightarrow{I_1I_2} + \cdots + \overrightarrow{I_{2k-1}I_{2k}})$. S'il existe une ligne polygonale $A_1 \ldots A_n A_1$ dont $I_1, \ldots, I_n$ soient les milieux des côtés, alors on a $f(A_1) = A_1$ et donc $\overrightarrow{a} = \overrightarrow{0}$. Réciproquement, si $\overrightarrow{a} = \overrightarrow{0}$, alors $f = \mathrm{Id}_{\mathcal{E}}$. Pour tout choix de $A_1 \in \mathcal{E}$, il existe une unique ligne polygonale $A_1 \ldots A_n A_1$ solution. Les points A_i s'obtiennent à partir de A_1, en prenant les images successives par $s_{I_1}, \ldots, s_{I_{n-1}}$.

Si n est impair, $f = s_K$. Si une ligne polygonale existe, on aura $f(A_1) = A_1$. Or, f a pour seul point fixe K. Donc nécessairement $A_1 = K$. Réciproquement, le choix de $A_1 = K$ fournit effectivement une solution, qui est unique.

Ex 6 - 11

D'après Ex. 6-3, b), le centre de G est $\{ t_{\vec{a}} \mid \forall f \in G \quad v_f(\overrightarrow{a}) = \overrightarrow{a} \}$. Si $f = s_A$, on a $v_f = -\mathrm{Id}_E$, sans autre vecteur fixe que $\overrightarrow{0}$. Donc $Z = \{ \mathrm{Id}_{\mathcal{E}} \}$.

Soit $f \in \mathrm{Aut}(\mathcal{E})$. Le commutateur $[f, t_{\vec{a}}]$ (resp. $[f, s_A]$) a pour application linéaire associée $v_f \circ \mathrm{Id}_E \circ (v_f)^{-1} \circ \mathrm{Id}_E = \mathrm{Id}_E$ (resp. $v_f \circ (-\mathrm{Id}_E) \circ (v_f)^{-1} \circ (-\mathrm{Id}_E) = \mathrm{Id}_E$). On en déduit que $G' \subset T$. Par ailleurs, pour tout $\overrightarrow{a} \in E$ posons $\overrightarrow{b} = \frac{1}{2}\overrightarrow{a}$ et soit $A \in \mathcal{E}$. On a

$$t_{\vec{b}} \circ s_A \circ (t_{\vec{b}})^{-1} \circ (s_A)^{-1} = t_{\vec{b}} \circ (s_A \circ t_{-\vec{b}} \circ (s_A)^{-1}) = t_{\vec{b}} \circ t_{\vec{b}} = t_{2\vec{b}} = t_{\vec{a}}.$$

Cela prouve que $T \subset G'$ et donc que $G' = T$.

Soit $A \in \mathcal{E}$. D'après 6-10, prop. et lemme, le sous-groupe G du groupe des symétries-point et translations est isomorphe à un produit semi-direct $T \times_\varphi \{ \mathrm{Id}_{\mathcal{E}}, s_A \}$ et donc à $E \times_\alpha \mathbb{Z}/2\mathbb{Z}$, où l'action α de $\mathbb{Z}/2\mathbb{Z}$ sur E est définie par $\alpha(\bar{0}) = \mathrm{Id}_E$ et $\alpha(\bar{1}) = -\mathrm{Id}_E$.

Chapitre 7

Barycentres en géométrie affine

7.1 Barycentres

Soient E un espace vectoriel sur le corps K et $\mathcal{E}$ un espace affine sur E. Soient $A_1, \ldots, A_k \in \mathcal{E}$ et $\lambda_1, \ldots, \lambda_k \in K$. Choisissons une origine O de $\mathcal{E}$. Etudions l'application $\varphi : M \mapsto \sum_{i=1}^{k} \lambda_i \overrightarrow{A_iM}$ de $\mathcal{E}$ dans E. Posons $\overrightarrow{a} = \sum_{i=1}^{k} \lambda_i \overrightarrow{A_iO}$ et $\lambda = \sum_{i=1}^{k} \lambda_i$. D'après la relation de Chasles, on a :

$$\varphi(M) = \sum_{i=1}^{k} \lambda_i \overrightarrow{A_iO} + (\sum_{i=1}^{k} \lambda_i)\overrightarrow{OM} = \lambda \overrightarrow{OM} + \overrightarrow{a}.$$

Si $\lambda = 0$, alors φ est l'application constante $M \mapsto \overrightarrow{a}$.
Si $\lambda \neq 0$, il existe $G \in \mathcal{E}$ unique tel que $\varphi(G) = \overrightarrow{0}$, caractérisé par chacune des relations suivantes, qui sont équivalentes :

$$(1) \qquad \sum_{i=1}^{k} \lambda_i \overrightarrow{GA_i} = \overrightarrow{0}.$$

$$(2) \qquad (\sum_{i=1}^{k} \lambda_i)\overrightarrow{OG} = \sum_{i=1}^{k} \lambda_i \overrightarrow{OA_i}.$$

Ce point G ne dépend pas de l'origine O choisie car O n'intervient pas dans (1).

Définition.

Nous appellerons point pondéré, un couple (A, λ) de $\mathcal{E} \times K$.

Soient $(A_1, \lambda_1), \ldots, (A_k, \lambda_k)$ des points pondérés tels que $\sum_{i=1}^{k} \lambda_i \neq 0$. Le point G de $\mathcal{E}$ caractérisé par (1) ou (2), est appelé le barycentre de cette famille de points pondérés. Nous le noterons $\text{bar}\,((A_i, \lambda_i)_{1 \leqslant i \leqslant k})$.

Si $\lambda_1 = \lambda_2 = \cdots = \lambda_k \neq 0$ on dit que G est l'isobarycentre des points $A_1, \ldots, A_k$.

L'application φ de $\mathcal{E}$ dans E est appelée la fonction vectorielle de Leibniz. Elle est constante si $\sum_{i=1}^{k} \lambda_i = 0$. Sinon, c'est un isomorphisme d'espaces affines de $\mathcal{E}$ sur $\mathcal{E}_E$.

Si on remplace $\lambda_1, \ldots, \lambda_k$ par des "masses" proportionnelles $\lambda\lambda_1, \ldots, \lambda\lambda_k$, où $\lambda \neq 0$, (1) ou (2), montre que le barycentre reste le même. Pour définir le barycentre de la famille $((A_1, \lambda_1), \ldots, (A_k, \lambda_k))$, on peut donc supposer que $\lambda_1 + \cdots + \lambda_k = 1$.

Supposons $\mathcal{E}$ de dimension finie, muni d'un repère cartésien $(A, \overrightarrow{e_1}, \ldots, \overrightarrow{e_n})$. Les coordonnées $y_1, \ldots, y_n$ de G s'expriment à partir des coordonnées $x_{1i}, \ldots, x_{ni}$ des points A_i. Par exemple, si $\lambda_1 + \cdots + \lambda_k = 1$, d'après (2) on a :

$$\left\{\begin{array}{lcl} y_1 &=& \lambda_1\, x_{11} + \cdots + \lambda_k\, x_{1k} \\ \cdots & \cdots & \cdots\cdots\cdots\cdots\cdots \\ y_n &=& \lambda_1\, x_{n1} + \cdots + \lambda_k\, x_{nk} \end{array}\right. .$$

Proposition.

Soit $(A_i, \lambda_i)_{i\in I}$ une famille finie de points pondérés de l'espace affine $\mathcal{E}$, telle que $\sum_{i\in I} \lambda_i \neq 0$. Soit $I = \bigcup_{p=1}^{s} I_p$ une partition de I. Supposons que $\mu_p = \sum_{i\in I_p} \lambda_i \neq 0$ pour $p = 1, \ldots, s$ et introduisons $G_p = \mathrm{bar}\,((A_i, \lambda_i)\,;\ i \in I_p)$. Alors le barycentre G de la famille $(A_i, \lambda_i)_{i\in I}$ est aussi le barycentre de la famille $(G_p, \mu_p)_{1\leqslant p\leqslant s}$.

Démonstration. Cette propriété d'associativité du barycentre résulte de

$$\overrightarrow{0} = \sum_{i\in I} \lambda_i \overrightarrow{GA_i} = \sum_{p=1}^{s} \Big(\sum_{i\in I_p} \lambda_i \overrightarrow{GA_i}\Big) = \sum_{p=1}^{s} \Big(\sum_{i\in I_p} \lambda_i\Big) \overrightarrow{GG_p} = \sum_{p=1}^{s} \mu_p \overrightarrow{GG_p}\,. \qquad \blacksquare$$

Exemple. Soient $A \in \mathcal{E}$, $B \in \mathcal{E}$ distincts. Fixons une origine O dans $\mathcal{E}$. Les barycentres $G = \mathrm{bar}\,((A, 1-\lambda), (B, \lambda))$, où $\lambda \in K$, sont caractérisés par :

$$\overrightarrow{OG} = (1-\lambda)\overrightarrow{OA} + \lambda \overrightarrow{OB} = \overrightarrow{OA} + \lambda \overrightarrow{AB}\,.$$

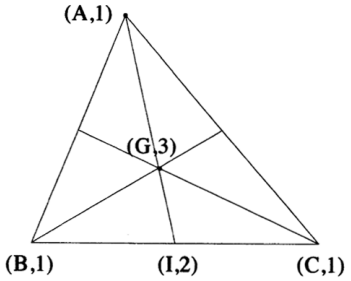
Leur ensemble est la droite affine (AB) issue de A dirigée par le vecteur $\overrightarrow{AB}$.

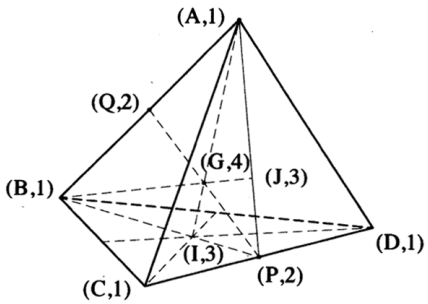
Si le corps K est $\mathbb{R}$, pour $0 \leqslant \lambda \leqslant 1$ l'ensemble de ces barycentres est appelé le *segment* $[AB]$. L'isobarycentre, obtenu pour $\lambda = \frac{1}{2}$, est le *milieu* I du segment $[AB]$. Il est caractérisé par la propriété $\overrightarrow{OI} = \overrightarrow{OA} + \frac{1}{2}\overrightarrow{AB}$ ou par $\overrightarrow{IA} + \overrightarrow{IB} = \overrightarrow{0}$.

L'isobarycentre G de trois points A, B, C de l'espace affine $\mathcal{E}_n(\mathbb{R})$ est appelé le *centre de gravité* du triangle ABC. Considérons le barycentre I de $((B,1),(C,1))$, qui est le milieu du segment $[BC]$. Par associativité, $G = \mathrm{bar}((I,2),(A,1))$ et on a :

$$3\overrightarrow{AG} = 1\overrightarrow{AA} + 2\overrightarrow{AI} = 2\,\overrightarrow{AI}\,.$$

Ainsi, G est situé sur la médiane $[AI]$ du triangle ABC, aux deux tiers à partir de A. De même, il est situé sur les médianes $[BJ]$ et $[BK]$. C'est une démonstration classique du fait que les médianes d'un triangle sont concourantes au point G et que G est situé aux deux tiers de chacune d'elles en partant du sommet.





Exercice 1. a) Pour un tétraèdre non aplati $ABCD$, de l'espace affine $\mathcal{E}_4(\mathbb{R})$ faire une étude analogue. Plus généralement, pour un simplexe $S = A_0A_1\cdots A_n$ de $\mathcal{E}_n(\mathbb{R})$, combien de droites concourantes obtient-on par ce procédé ?

b) Quelles masses placer en A, B, C, D pour obtenir comme barycentre le milieu U d'une "médiane" $[AI]$ du tétraèdre ?

Solution. a) Soit I l'isobarycentre de B, C, D, centre de gravité du triangle BCD. Alors $G = \text{bar}((A,1),(I,3))$ est situé sur AI, aux trois quarts de ce segment à partir de A. De même, il est situé aux trois quarts des segments $[BJ]$, $[CK]$, $[DL]$ définis de manière analogue. Ces quatre droites concourent donc en G.

On peut aussi considérer les isobarycentres Q de (A,B) et P de (C,D), milieux des arêtes $[AB]$ et $[CD]$. Alors $G = \text{bar}((P,2),(Q,2))$, est milieu du segment $[PQ]$. Les trois segments reliant les milieux de deux arêtes opposées du tétraèdre $ABCD$, concourent eux aussi au point G qui est milieu de chacun d'eux.

Soit X une partie de l'ensemble des sommets du simplexe S, ayant k éléments, avec $1 \leqslant k \leqslant n$. Soient I et J les isobarycentres des points de X et de son complémentaire X^c. L'isobarycentre G des $n+1$ sommets, est barycentre de $((I,k),(J,n+1-k))$. Quand X varie, on obtient des droites (IJ) concourantes en G. Comme X et X^c donnent la même droite, le nombre M_n de droites obtenues est

$$\tfrac{1}{2}\sum_{k=1}^{n} C_{n+1}^k = \tfrac{1}{2}\left[\sum_{k=0}^{n+1} C_{n+1}^k - 2\right] = 2^n - 1 \text{ (nombres de Mersenne).}$$

b) Si U est le milieu de $[AI]$, en utilisant l'associativité du barycentre,

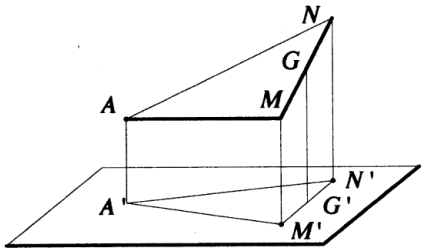
$$U = \text{bar}[(A,\tfrac{1}{2}),(I,\tfrac{1}{2})] = \text{bar}[(A,\tfrac{1}{2}),(\text{bar}((B,\tfrac{1}{3}),(C,\tfrac{1}{3}),(D,\tfrac{1}{3})),\tfrac{1}{2})]$$
$$= \text{bar}[(A,\tfrac{1}{2}),(B,\tfrac{1}{6}),(C,\tfrac{1}{6}),(D,\tfrac{1}{6})].$$

7.2 Applications affines et barycentres

Proposition.

Soient $\mathcal{E}$ et $\mathcal{E}'$ des espaces affines sur le corps K. Pour que $f : \mathcal{E} \to \mathcal{E}'$ soit affine, il faut et il suffit que pour toute famille finie $(A_i,\lambda_i)_{i\in I}$ de points pondérés de $\mathcal{E}$, telle que $\sum_{i\in I}\lambda_i = 1$, on ait $f[\text{bar}((A_i,\lambda_i)_{i\in I})] = \text{bar}((f(A_i),\lambda_i)_{i\in I})$.

Démonstration. *Supposons f affine.* Pour tout point $M \in \mathcal{E}$, notons M' (même lettre avec prime) son image $f(M) \in \mathcal{E}'$. Le barycentre d'une famille de points pondérés $(A_i,\lambda_i)_{i\in I}$, où $\sum_{i\in I}\lambda_i \neq 0$, est caractérisée par la condition $\overrightarrow{0} = \sum_{i\in I}\lambda_i \overrightarrow{GA_i}$. On en déduit $\overrightarrow{0} = \sum_{i\in I}\lambda_i\, v_f(\overrightarrow{GA_i}) = \sum_{i\in I}\lambda_i \overrightarrow{G'A_i'}$ donc G' est le barycentre de $(A_i',\lambda_i)_{i\in I}$.



Supposons que f conserve le barycentre. Soient $A \in \mathcal{E}$ et $A' = f(A)$. Pour tout $\overrightarrow{x} \in E$, notons $v(\overrightarrow{x})$ le vecteur de E' tel que $f(A+\overrightarrow{x}) = A' + v(\overrightarrow{x})$. Montrons que l'application v de E dans E' ainsi définie est linéaire. Alors f sera affine (6-4, rem.).

Soient $\overrightarrow{x}, \overrightarrow{y} \in E$ et $\lambda, \mu \in K$. Considérons $M = A + \overrightarrow{x}$, $N = A + \overrightarrow{y}$. Posons $M' = f(M)$, $N' = f(N)$. Le barycentre G de $((A,1-\lambda-\mu),(M,\lambda),(N,\mu))$ vérifie

$$\overrightarrow{AG} = \lambda\overrightarrow{AM} + \mu\overrightarrow{AN} = \lambda\overrightarrow{x} + \mu\overrightarrow{y}.$$

Par hypothèse, son image G' est barycentre de $((A',1-\lambda-\mu),(M',\lambda),(N',\mu))$ donc

$$\overrightarrow{A'G'} = \lambda\overrightarrow{A'M'} + \mu\overrightarrow{A'N'} = \lambda\, v(\overrightarrow{x}) + \mu\, v(\overrightarrow{y}).$$

Puisque $\overrightarrow{A'G'} = v(\overrightarrow{AG})$, on a $v(\lambda\overrightarrow{x} + \mu\overrightarrow{y}) = \lambda v(\overrightarrow{x}) + \mu v(\overrightarrow{y})$. (La figure est faite pour f projection de $\mathcal{E}_3$ sur un plan de $\mathcal{E}_3$, parallèlement à une direction donnée.) ∎

Remarques.

a) Dans la démonstration précédente, pour que f soit affine, il a suffit que f conserve le barycentre de trois points. Si le corps K n'est pas de caractéristique 2, il suffit pour cela que f conserve le barycentre de tout couple de points pondérés.

En effet, soit $G = \text{bar}((A_1,\lambda_1),(A_2,\lambda_2),(A_3\lambda_3))$, avec $\lambda_1+\lambda_2+\lambda_3 = 1$. On peut supposer $\lambda_1,\lambda_2,\lambda_3$ non nuls. On ne peut avoir simultanément $\lambda_2+\lambda_3 = 0$, $\lambda_3+\lambda_1 = 0$, $\lambda_1+\lambda_2 = 0$, sinon en ajoutant on obtient $2(\lambda_1+\lambda_2+\lambda_3) = 0$ et donc $\lambda_1+\lambda_2+\lambda_3 = 0$ puisque $2 = 1+1 \neq 0$ dans K. Si par exemple $\lambda_2+\lambda_3 \neq 0$, soit $I = \text{bar}((A_2,\lambda_2),(A_3,\lambda_3))$. On a $G = \text{bar}((A_1,\lambda_1),(I,\lambda_2+\lambda_3))$. Si f conserve le barycentre pour les couples de points, on a $f(G) = \text{bar}((f(A_1),\lambda_1),(f(I),\lambda_2+\lambda_3)) = \text{bar}((f(A_1),\lambda_1),(\text{bar}((f(A_2),\lambda_2),(f(A_3),\lambda_3)),\lambda_2+\lambda_3) = \text{bar}((f(A_i),\lambda_i)_{1\leqslant i\leqslant 3})$.

b) Supposons que $f \in \text{Aut}(\mathcal{E})$ permute les points $A_1,\dots,A_k$ de $\mathcal{E}$. D'après la proposition, f laisse fixe l'isobarycentre G de ces points.

7.3 Sous-espaces affines et barycentres

Proposition.

Soit $\mathcal{E}$ un espace affine sur l'espace vectoriel E et soit $\mathcal{F}$ une partie non vide de $\mathcal{E}$. Pour que $\mathcal{F}$ soit un sous-espace affine de $\mathcal{E}$, il faut et il suffit que tout barycentre de points pondérés de $\mathcal{F}$ soit un élément de $\mathcal{F}$.

Démonstration. Soit $\mathcal{F}$ un sous-espace affine de $\mathcal{E}$ de direction F. Considérons des points pondérés $(A_0,\lambda_0),\dots,(A_k,\lambda_k)$ de $\mathcal{F}$ avec $\sum_{i=0}^{k}\lambda_i = 1$. Montrons que leur barycentre G appartient à $\mathcal{F}$. Pour $i = 1,\dots,k$, on a $\overrightarrow{A_0A_i} \in F$. On en déduit que $\overrightarrow{A_0G} = \lambda_1\overrightarrow{A_0A_1}+\cdots+\lambda_k\overrightarrow{A_0A_k} \in F$. Donc G est élément de $\mathcal{F}$.

Réciproquement, supposons que $\mathcal{F}$ soit stable par barycentres. Fixons une origine A_0 dans $\mathcal{F}$. Vérifions que l'ensemble F des vecteurs $\overrightarrow{A_0M}$, où M décrit $\mathcal{F}$, est un sous-espace vectoriel de E. Alors $\mathcal{F}$ sera le sous-espace affine de $\mathcal{E}$ de direction F. Soient $\overrightarrow{A_0A_1}$ et $\overrightarrow{A_0A_2}$ deux tels vecteurs et λ_1, λ_2 des scalaires. Posons $\lambda_0 = 1-\lambda_1-\lambda_2$. Le barycentre G de $((A_0,\lambda_0),(A_1,\lambda_1),(A_2,\lambda_2))$ est élément de $\mathcal{F}$. Le vecteur $\overrightarrow{A_0G} = \lambda_1\overrightarrow{A_0A_1}+\lambda_2\overrightarrow{A_0A_2}$ est donc élément de F et F est un sous-espace vectoriel de E. ∎

Corollaire.

Soit $X \neq \emptyset$ une partie de l'espace affine $\mathcal{E}$. Le sous-espace affine $\mathcal{F}$ de $\mathcal{E}$ engendré par X est l'ensemble des barycentres des familles finies de points pondérés de X.

Démonstration. Tous ces barycentres sont éléments de $\mathcal{F}$ d'après la proposition. Réciproquement, montrons que tout $M \in \mathcal{F}$ est barycentre d'éléments de X. Notons F la direction de $\mathcal{F}$. Soit $A_0 \in X$. D'après 6-6, cor., $\overrightarrow{A_0M} \in F$ admet une expression de la forme $\overrightarrow{A_0M} = \lambda_1\overrightarrow{A_0A_1}+\cdots+\lambda_k\overrightarrow{A_0A_k}$, où $k \in \mathbb{N}^*$, $A_1,\dots,A_k \in X$ et $\lambda_1,\dots,\lambda_k \in K$. Posons $\lambda_0 = 1-(\lambda_1+\cdots+\lambda_k)$. La relation précédente montre que M est le barycentre de $((A_0,\lambda_0),(A_1,\lambda_1),\dots,(A_k,\lambda_k))$. ∎

7.4 Repères affines

Définitions.

On considère un espace affine $\mathcal{E}$ sur le corps K. On dit qu'une partie finie $X = \{A_1, \ldots, A_k\}$ de $\mathcal{E}$ est affinement libre si pour tout point M du sous-espace affine engendré par X, il existe un seul système $\{\lambda_1, \ldots, \lambda_k\}$ de scalaires tel que

$$\sum_{i=1}^{k} \lambda_i = 1 \qquad \text{et} \qquad M = \text{bar}((A_1, \lambda_1), \ldots, (A_k, \lambda_k)) .$$

Si X n'est pas affinement libre, on dit qu'elle est affinement liée.

On dit que X est affinement génératrice si le sous-espace affine de $\mathcal{E}$ engendré par X est égal à $\mathcal{E}$.

On dit que X est un repère affine de $\mathcal{E}$, si X est affinement libre et génératrice.
Dans ce cas, pour tout point M de $\mathcal{E}$ il existe des scalaires $\lambda_1, \ldots, \lambda_k$ uniques tels que $\sum_{i=1}^{k} \lambda_i = 1$ et $M = \text{bar}((A_1, \lambda_1), \ldots, (A_k, \lambda_k))$. On appelle ces scalaires les coordonnées barycentriques du point M dans le repère affine X.

Proposition.

Pour qu'une partie $X = \{A_0, \ldots, A_k\}$ de $\mathcal{E}$ soit une partie affinement libre (resp. une partie affinement génératrice, un repère affine) de $\mathcal{E}$, il faut et il suffit que $\mathcal{B} = \{\overrightarrow{A_0A_1}, \ldots, \overrightarrow{A_0A_k}\}$ soit une famille libre (resp. une famille génératrice, une base) de l'espace vectoriel E.

Démonstration. 1°/ *Supposons X affinement libre.* Soient $\lambda_1, \ldots, \lambda_k$ des scalaires tels que $\lambda_1 \overrightarrow{A_0A_1} + \cdots + \lambda_k \overrightarrow{A_0A_k} = \overrightarrow{0}$. Posons $\lambda_0 = 1 - (\lambda_1 + \cdots + \lambda_k)$. On a $\sum_{i=0}^{k} \lambda_i = 1$ et $\sum_{i=0}^{k} \lambda_i \overrightarrow{A_0A_i} = \overrightarrow{0}$. Donc $A_0 = \text{bar}((A_0, \lambda_0), \ldots, (A_k, \lambda_k))$. Par ailleurs, $A_0 = \text{bar}((A_0, 1), (A_1, 0), \ldots, (A_k, 0))$. Comme X est affinement libre, $\lambda_0 = 1$, $\lambda_1 = 0$, $\ldots$, $\lambda_k = 0$, ce qui prouve que $\mathcal{B}$ est libre dans l'espace vectoriel E.

2°/ *Supposons $\mathcal{B}$ libre dans E.* Soient $\lambda_0, \ldots, \lambda_k$ des scalaires tels que $\sum_{i=0}^{k} \lambda_i = 1$ et considérons $M = \text{bar}((A_i, \lambda_i)\,;\ i = 0, \ldots, k)$. En plaçant l'origine au point A_0, on obtient $\overrightarrow{A_0M} = \lambda_1 \overrightarrow{A_0A_1} + \cdots + \lambda_k \overrightarrow{A_0A_k}$. Comme $\mathcal{B}$ est libre, cette relation détermine de manière unique $\lambda_1, \ldots, \lambda_k$. Alors $\lambda_0 = 1 - (\lambda_1 + \cdots + \lambda_k)$ est déterminé. Cela prouve que X est affinement libre.

3°/ *Supposons $\mathcal{B}$ génératrice pour E.* Pour tout $M \in \mathcal{E}$, il existe des scalaires $\lambda_1, \ldots, \lambda_k$ tels que $\overrightarrow{A_0M} = \lambda_1 \overrightarrow{A_0A_1} + \cdots + \lambda_k \overrightarrow{A_0A_k}$. En posant $\lambda_0 = 1 - (\lambda_1 + \cdots + \lambda_k)$ on a $\overrightarrow{A_0M} = \lambda_0 \overrightarrow{A_0A_0} + \lambda_1 \overrightarrow{A_0A_1} + \cdots + \lambda_k \overrightarrow{A_0A_k}$ donc $M = \text{bar}((A_i, \lambda_i)\,;\ i = 0, \ldots, k)$. Ainsi le sous-espace affine engendré par X est $\mathcal{E}$.

4°/ *Supposons que X engendre $\mathcal{E}$.* Pour tout $\overrightarrow{x} \in E$, le point $M = A_0 + \overrightarrow{x}$ est barycentre de $((A_i, \lambda_i)\,;\ i = 0, \ldots, k)$ pour un choix convenable de scalaires λ_i tels que $\sum_{i=0}^{k} \lambda_i = 1$. En plaçant l'origine en A_0, on obtient :

$$\overrightarrow{x} = \overrightarrow{A_0M} = \lambda_1 \overrightarrow{A_0A_1} + \cdots + \lambda_k \overrightarrow{A_0A_k} ,$$

ce qui prouve que $\overrightarrow{A_0A_1}, \ldots, \overrightarrow{A_0A_k}$ engendrent E. ∎

Remarques.

a) Cet énoncé relie repères affines et repères cartésiens de $\mathcal{E}$. En effet, $(A, \overrightarrow{e_1}, \ldots, \overrightarrow{e_n})$ est un repère cartésien si et seulement si $\{A_0\ ,\ A_1 = A_0 + \overrightarrow{e_1}\ , \ldots,\ A_n = A_0 + \overrightarrow{e_n}\}$ est un repère affine de $\mathcal{E}$. En permutant les points $A_0, \ldots, A_n$ on a encore un repère affine de $\mathcal{E}$ donc $(A_i\ ,\ (\overrightarrow{A_iA_j})_{0\leqslant j\leqslant n\ ,\ j\neq i})$ est un repère cartésien de $\mathcal{E}$ pour tout $i = 0, \ldots, n$.

Si $\mathcal{E}$ est de dimension finie n, tout repère affine de $\mathcal{E}$ a pour cardinal $n+1$. Dans le plan $\mathcal{E}_2(\mathbb{R})$ (resp. l'espace $\mathcal{E}_3(\mathbb{R})$) un repère affine est formé des sommets d'un triangle (resp. d'un tétraèdre) non aplati.

b) En utilisant la proposition, les propriétés classiques des espaces vectoriels, notamment le th. de la base incomplète, donnent des propriétés de l'espace affine. Sans vouloir les énoncer toutes, en voici quelques unes.

Une sous-famille d'une famille de points affinement libre est affinement libre.

On peut compléter une famille affinement libre, à l'aide de points d'une famille finie affinement génératrice donnée, pour constituer un repère affine de $\mathcal{E}$. En particulier, on peut extraire d'une famille finie génératrice, un repère affine.

Une famille $(A_0, \ldots, A_k)$ affinement libre engendre un sous-espace affine $\mathcal{F}$, pour lequel elle est un repère affine. Donc $\dim(\mathcal{F}) = k$. Soit $B \in \mathcal{E}$ avec $B \notin \mathcal{F}$. Alors, $(A_0, \ldots, A_k, B)$ est affinement libre et engendre un sous-espace affine de dimension $k+1$. En effet, $(\overrightarrow{A_0A_1}, \ldots, \overrightarrow{A_0A_k}, \overrightarrow{A_0B})$ est libre car $(\overrightarrow{A_0A_1}, \ldots, \overrightarrow{A_0A_k})$ est libre et $\overrightarrow{A_0B} \notin \text{Vect}\,(\overrightarrow{A_0A_1}, \ldots, \overrightarrow{A_0A_k})$.

Corollaire.

Considérons deux espaces vectoriels E et E' sur un même corps et des espaces affines $\mathcal{E}$ et $\mathcal{E}'$ sur E et E'. Supposons $\mathcal{E}$ muni d'un repère affine $(A_0, \ldots, A_n)$ et soient $B_0, \ldots, B_n$ des points de $\mathcal{E}'$. Il existe une application affine f unique de $\mathcal{E}$ dans $\mathcal{E}'$ telle que $f(A_i) = B_i$ pour $i = 0, \ldots, n$. De plus f est un isomorphisme si et seulement si $(B_0, \ldots, B_n)$ est un repère affine de $\mathcal{E}'$.

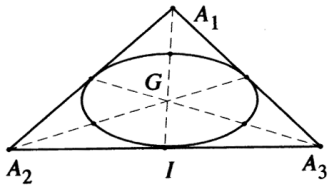
Démonstration. Comme $\overrightarrow{A_0A_1}, \ldots, \overrightarrow{A_0A_n}$ constituent une base de E, il existe une application linéaire unique v de E dans E' telle que $v\,(\overrightarrow{A_0A_i}) = \overrightarrow{B_0B_i}$ pour $i = 1, \ldots, n$. D'après 6-4, il existe une application affine unique de $\mathcal{E}$ dans $\mathcal{E}'$ telle que $f(A_0) = B_0$ et telle que l'application linéaire associée soit v. Cette application f a les propriétés voulues. Par ailleurs, c'est la seule, car la condition $f(A_i) = B_i$ pour $i = 0, \ldots, n$ impose $f(A_0) = B_0$ et $v\,(\overrightarrow{A_0A_i}) = \overrightarrow{B_0B_i}$ pour $i = 1, \ldots, n$, ce qui détermine v.

Pour que f soit un isomorphisme, il faut et il suffit que v soit un isomorphisme d'espaces vectoriels, c'est-à-dire que les vecteurs $v\,(\overrightarrow{A_0A_i}) = \overrightarrow{B_0B_i}$ constituent une base de E', ou encore que $(B_0, \ldots, B_n)$ soit un repère affine de $\mathcal{E}'$. ∎

Exercice. Dans le plan affine réel $\mathcal{E}_2$, on considère un triangle non aplati $A_1A_2A_2$. Soit $\Lambda = (\lambda_1, \lambda_2, \lambda_3) \in \mathbb{R}^3$, tel que $\sum_{i=1}^{3} \lambda_i \neq 0$. Pour toute permutation $s \in \mathcal{S}_3$ on considère $G_s = \text{bar}((A_1, \lambda_{s(1)}), (A_2, \lambda_{s(2)}), (A_3, \lambda_{s(3)}))$. Montrer que les six points G_s obtenus quand s décrit $\mathcal{S}_3$, appartiennent à une même ellipse E_Λ. Montrer que toutes les ellipses E_Λ ont le même centre. Préciser la position de ce centre. Etudier les cas particuliers où $\lambda_1 = 0$, puis où $\lambda_1 = 0$, $\lambda_2 = \lambda_3$.
Dans l'espace affine réel $\mathcal{E}_3$, donner une propriété analogue pour un tétraèdre.

Solution. Introduisons un produit scalaire sur $\mathbb{R}^2$, d'où une structure d'espace affine euclidien sur $\mathcal{E}_2$ (plan euclidien usuel). Soit $B_1B_2B_3$ un triangle équilatéral de ce plan. D'après le corollaire, il existe un automorphisme affine φ unique de $\mathcal{E}_2$ tel que $\varphi(A_i) = B_i$ pour $i = 1,2,3$. Comme φ conserve le barycentre, il suffit d'étudier le problème dans le triangle équilatéral $B_1B_2B_3$. Pour lui c'est facile. En effet, toute permutation $s \in \mathcal{S}_3$ des sommets est réalisée par une isométrie. La transposition $t_i = [j,k]$ l'est par la symétrie orthogonale par rapport à la médiatrice de $[A_jA_k]$. Le cycle $c = (1,2,3)$ par une rotation de centre le centre de gravité G_0 du triangle $B_1B_2B_3$, d'angle $\pm\frac{2\pi}{3}$, de même pour c^2. Ainsi, les six points G_s appartiennent au cercle C_Λ de centre G_0, passant par l'un d'eux. En revenant dans $A_1A_2A_2$ par φ^{-1}, on voit que les six points appartiennent à une l'ellipse E_Λ de centre G, centre de gravité du triangle $A_1A_2A_3$. Ces ellipses sont homothétiques. Si $\lambda_1 = 1$, $\lambda_2 = \lambda_3 = 0$, on trouve dans la famille des cercles C_Λ, le cercle C circonscrit au triangle dans $B_1B_2B_3$. L'ellipse E_1 image par φ^{-1} de C appartient à la famille E_Λ. Elle passe par les sommets et par les symétriques de G par rapport aux milieux des côtés du triangle.

Si $\lambda_1 = 0$, le barycentre de $((A_1,0),(A_2,\lambda_2),(A_3,\lambda_3))$ est le point I qui divise $[A_2A_3]$ dans le rapport $\frac{\overline{IA_2}}{\overline{IA_3}} = -\frac{\lambda_3}{\lambda_2} = k$. Par permutation des masses, on obtient les six points qui sont sur les côtés $[A_iA_j]$ du triangle (deux par côté), tels que $\frac{\overline{IA_i}}{\overline{IA_j}} = k$. Si de plus $\lambda_2 = \lambda_3$, les deux points situés sur un même côté viennent se confondre au milieu du côté. Il existe donc une ellipse qui est tangente aux trois côtés du triangle en leurs milieux. Son centre est le centre de gravité G du triangle. Comme G est aux deux tiers de chaque médiane cette conique passe en plus par les milieux des segments $[A_iG]$ pour $i = 1,2,3$. Cette ellipse est appelée l'ellipse de Steiner. Elle est homothétique de E_1, donc la tangente en A_1 à E_1 est parallèle à A_2A_3.



Pour un tétraèdre T de $\mathcal{E}_3$, l'étude se répète. Supposons $\mathcal{E}_3$ euclidien et T régulier. Le groupe des isométries de T est d'ordre $4! = 24$. En donnant $\Lambda = (\lambda_1,\lambda_2,\lambda_3,\lambda_4) \in \mathbb{R}^4$, tel que $\sum_{i=1}^{4} \lambda_i \neq 0$, on obtiendra, en permutant les constantes, 24 points appartenant à une même sphère de centre l'isobarycentre G des sommets. Pour un tétraèdre quelconque, ces sphères deviennent des ellipsoïdes concentriques, homothétiques.

7.5 Espace affine hyperplan d'un espace vectoriel

Dans l'espace affine $\mathcal{E}_{n+1}(K)$, où K est un corps commutatif, considérons un repère cartésien $R_0 = (O, \overrightarrow{e_0}, \ldots, \overrightarrow{e_n})$. D'après 7-4, O, $A_0 = O + \overrightarrow{e_0}$, $\ldots$, $A_n = O + \overrightarrow{e_n}$ constituent un repère affine de $\mathcal{E}_{n+1}(K)$.

Les $n+1$ points $A_0, \ldots, A_n$, sont affinement libres. Ils engendrent un hyperplan $\mathcal{H}$ de $\mathcal{E}_{n+1}(K)$. Dans le repère R_0, l'hyperplan d'équation $f(\overrightarrow{OM}) = x_0 + \cdots + x_n = 1$ contient $A_0, \ldots, A_n$. Il est donc égal à $\mathcal{H}$.

Considérons maintenant un espace affine $\mathcal{E}$ de dimension n sur K muni d'un repère affine R. Il existe un isomorphisme unique de $\mathcal{E}$ sur $\mathcal{H}$ appliquant R sur $(A_0, \ldots, A_n)$. On peut identifier $\mathcal{E}$ muni du repère R avec $\mathcal{H}$ muni du repère $(A_0, \ldots, A_n)$. L'espace vectoriel E associé à $\mathcal{E}$ apparaît alors comme la direction de $\mathcal{H}$, c'est-à-dire comme un sous-espace vectoriel de K^{n+1}, de dimension n. Ce procédé est fructueux car on dispose dans K^{n+1} de toutes les ressources de l'algèbre linéaire.

Proposition.

Effectuons l'identification que nous venons de décrire.

(i) *Pour tout $M \in \mathcal{H}$, les coordonnées barycentriques de M dans le repère affine $(A_0, \dots, A_n)$ de $\mathcal{H}$, sont aussi les coordonnées de M dans le repère cartésien $(O, \overrightarrow{e_0}, \dots, \overrightarrow{e_n})$ de l'espace affine $\mathcal{E}_{n+1}$.*

(ii) *Des points $M_1, \dots, M_k$ de $\mathcal{H}$ sont affinement libres (resp. affinement générateurs) dans $\mathcal{H}$, si et seulement si les vecteurs $\overrightarrow{OM_1}, \dots, \overrightarrow{OM_k}$ sont libres (resp. générateurs) dans K^{n+1}.*

(iii) *Une application f de $\mathcal{H}$ dans $\mathcal{H}$ est affine si et seulement s'il existe une application linéaire T de K^{n+1} dans lui-même, laissant $\mathcal{H}$ stable, dont f soit la restriction à $\mathcal{H}$. Cette application linéaire est unique. Elle est bijective si et seulement si f est bijective.*

Démonstration. (i) Les coordonnées barycentriques $\lambda_0, \dots, \lambda_n$ de M dans le repère affine $R = (A_0, \dots, A_n)$ de $\mathcal{H}$ sont telles que $\lambda_0 \overrightarrow{MA_0} + \cdots + \lambda_n \overrightarrow{MA_n} = \overrightarrow{O}$. Cette relation étant toujours vraie dans K^{n+1}, elle montre que M est également barycentre de $((A_i, \lambda_i)_{0 \leqslant i \leqslant n})$ dans $\mathcal{E}_{n+1}(K)$. On a donc bien :

$$\overrightarrow{OM} = \lambda_0 \overrightarrow{OA_0} + \cdots + \lambda_n \overrightarrow{OA_n} = \lambda_0 \overrightarrow{e_0} + \cdots + \lambda_n \overrightarrow{e_n} \quad \text{avec} \sum_{i=0}^{n} \lambda_i = 1 .$$

(ii) Supposons $M_1, \dots, M_k$ affinement libres dans $\mathcal{H}$. Puisque $O \notin \mathcal{H}$, les points $O, M_1, \dots, M_k$ sont affinement libres dans $\mathcal{E}_{n+1}(K)$ (7-4, rem. b). D'après 7-4, prop., $(\overrightarrow{OM_1}, \dots, \overrightarrow{OM_k})$ est libre dans K^{n+1}.

Réciproquement, si $(\overrightarrow{OM_1}, \dots, \overrightarrow{OM_k})$ est libre, alors $(O, M_1, \dots, M_k)$ est affinement libre dans $\mathcal{E}_{n+1}(K)$ et $(M_1, \dots, M_k)$ est affinement libre dans $\mathcal{H}$.

Si $M_1, \dots, M_k$ sont affinement générateurs dans $\mathcal{H}$, alors $(O, M_1, \dots, M_k)$ engendre un sous-espace affine de $\mathcal{E}_{n+1}(K)$ de dimension strictement supérieure à $n = \dim(\mathcal{H})$ car $O \notin \mathcal{H}$ et donc de dimension $n+1$. Ils engendrent donc $\mathcal{E}_{n+1}(K)$. D'après 7-4, prop., $\overrightarrow{OM_1}, \dots, \overrightarrow{OM_k}$ engendrent K^{n+1}.

Si $\overrightarrow{OM_1}, \dots, \overrightarrow{OM_k}$ engendrent K^{n+1}, alors pour tout $M \in \mathcal{H}$, il existe des scalaires $\lambda_1, \dots, \lambda_k$ tels que $\overrightarrow{OM} = \lambda_1 \overrightarrow{OM_1} + \cdots + \lambda_k \overrightarrow{OM_k}$. On a :

$$1 = f(\overrightarrow{OM}) = \lambda_1 f(\overrightarrow{OM_1}) + \cdots + \lambda_k f(\overrightarrow{OM_k}) = \lambda_1 + \cdots + \lambda_k .$$

Donc $M = \mathrm{bar}((M_1, \lambda_1), \dots, (M_k, \lambda_k))$ ce qui montre que $M_1, \dots, M_k$ engendrent $\mathcal{H}$.

(iii) Un endomorphisme linéaire T de K^{n+1} est affine pour la structure d'espace affine canonique. S'il laisse stable $\mathcal{H}$, sa restriction f à $\mathcal{H}$ est affine (par exemple, d'après 7-2).

Réciproquement, soit f une application affine de $\mathcal{H}$ dans $\mathcal{H}$. Pour $i = 0, \dots, n$, posons $A'_i = f(A_i)$ où $(A_0, \dots, A_n)$ est le repère affine de $\mathcal{H}$ déja considéré. Soit $T \in \mathcal{L}(K^n)$ appliquant les vecteurs $\overrightarrow{e_0} = \overrightarrow{OA_0}, \dots, \overrightarrow{e_n} = \overrightarrow{OA_n}$ de la base canonique sur $\overrightarrow{OA'_0}, \dots, \overrightarrow{OA'_n}$. Alors T est affine, elle laisse stable $\mathcal{H}$ car $R = (A_0, \dots, A_n)$ est un repère affine de $\mathcal{H}$ et $T(A_0) \in \mathcal{H}, \dots, T(A_n) \in \mathcal{H}$. La restriction de T à $\mathcal{H}$ et f sont égales car elles coïncident sur le repère affine R.

Enfin, f est un isomorphisme affine si et seulement si $(A'_0, \dots, A'_n)$ est un repère affine de $\mathcal{H}$, c'est-à-dire d'après (iii), si $(\overrightarrow{OA'_0}, \dots, \overrightarrow{OA'_n})$ est une base de K^{n+1}. Ainsi f est bijective si et seulement si T applique la base canonique de K^{n+1} sur une base de K^{n+1}, c'est-à-dire si T est bijective. ∎

Exercice. Soient $\mathcal{E}$ un espace affine de dimension n et $(A_0, \dots, A_n)$ un repère affine. Montrer que $n+1$ points $P_0, \dots, P_n$ de $\mathcal{E}$ sont affinement liés, si et seulement si le déterminant des coordonnées barycentriques de $P_0, \dots, P_n$ est nul.

Dans le plan $\mathcal{E}_2(\mathbb{R})$ muni d'un repère affine (A_0, A_1, A_2), soient $A \neq B$, de coordonnées barycentriques $(\alpha_0, \alpha_1, \alpha_2)$ et $(\beta_0, \beta_1, \beta_2)$. Quelle relation doivent lier les coordonnées barycentriques (x_0, x_1, x_2) d'un point M pour que M appartienne à la droite (AB) (équation barycentrique de la droite (AB)) ?

Démontrer le th. de Ménélaüs.

Solution. Identifions $\mathcal{E}$ avec un hyperplan de $\mathcal{E}_{n+1}(K)$ ne passant pas par l'origine O. La proposition montre qu'il suffit d'écrire que $\overrightarrow{OP_0}, \dots, \overrightarrow{OP_n}$ sont liés. Pour cela il faut et il suffit que $\det(\overrightarrow{OP_0}, \dots, \overrightarrow{OP_n}) = 0$, c'est-à-dire que que le déterminant des coordonnées barycentriques des points soit nul.

Si $\mathcal{E}$ est le plan $\mathcal{E}_2(\mathbb{R})$, on a $M \in (AB)$ si et seulement si $\overrightarrow{OM}$ appartient au plan OAB de $\mathcal{E}_3(\mathbb{R})$, c'est-à-dire si $\overrightarrow{OM}$ est lié avec $\overrightarrow{OA}$ et $\overrightarrow{OB}$, d'où la condition :

$$\begin{vmatrix} x_0 & \alpha_0 & \beta_0 \\ x_1 & \alpha_1 & \beta_1 \\ x_2 & \alpha_2 & \beta_2 \end{vmatrix} = 0.$$

Considérons des points $M_0 \in [A_1A_2]$, $M_1 \in [A_2A_0]$, $M_2 \in [A_0A_1]$, qui ne soient pas des sommets du triangle $A_0A_1A_2$. On a $M_0 = \text{bar}[(A_1, \lambda_1), (A_2, 1), (A_0, 0)]$ où $\lambda_1 = -\frac{\overline{M_0A_2}}{\overline{M_0A_1}}$ car $\lambda_1\overrightarrow{M_0A_1} + \overrightarrow{M_0A_2} = \overrightarrow{0}$. On obtient les coordonnées barycentriques (à une constante multiplicative près) des deux autres points, par permutation circulaire. Les points M_0, M_1, M_2 sont alignés si et seulement si

$$0 = \begin{vmatrix} 0 & 1 & \lambda_0 \\ \lambda_1 & 0 & 1 \\ 1 & \lambda_2 & 0 \end{vmatrix} = 1 + \lambda_1\lambda_2\lambda_0 = 1 - \frac{\overline{M_0A_2}}{\overline{M_0A_1}} \times \frac{\overline{M_1A_0}}{\overline{M_1A_2}} \times \frac{\overline{M_2A_1}}{\overline{M_2A_0}}.$$

7.6 Parties convexes d'un espace affine réel

Lemme.

Soit C une partie d'un espace affine réel $\mathcal{E}$. Les conditions suivantes sont équivalentes.

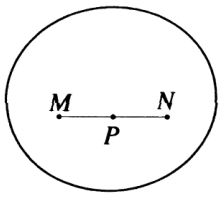
(i) *Le barycentre G de toute famille finie $\{(A_1, \lambda_1), \dots, (A_k, \lambda_k)\}$ de points pondérés de C, telle que $\lambda_1 \geqslant 0, \dots, \lambda_k \geqslant 0$ et $\sum_{i=1}^{k} \lambda_i = 1$, appartient à C.*

(ii) $\forall\, M \in C \quad \forall\, N \in C \quad [MN] = \{M + \lambda\overrightarrow{MN}\,;\ 0 \leqslant \lambda \leqslant 1\} \subset C.$

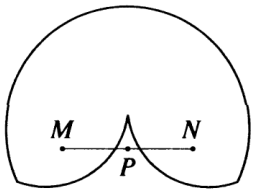
Démonstration. (i) $\Rightarrow$ (ii) en appliquant (i) aux points pondérés $(M, 1-\lambda), (N, \lambda)$.
(ii) $\Rightarrow$ (i) Quitte à supprimer les termes où $\lambda_i = 0$, considérons $\{(A_1, \lambda_1), \dots, (A_k, \lambda_k)\}$ où $\lambda_i > 0$ pour tout i. Si (ii) est vérifiée, en utilisant l'associativité des barycentres, on voit que $G_2 = \text{bar}\,((A_1, \lambda_1), (A_2, \lambda_2))$ est élément de $[A_1A_2] \subset C$. Ensuite, on voit de même que $G_3 = \text{bar}\,((G_2, \lambda_1 + \lambda_2), (A_3, \lambda_3))$ est un élément de $[G_2A_3] \subset C, \dots$ Par une récurrence finie on montre que $G = \text{bar}\,((A_i, \lambda_i))$ appartient à C. ∎

Définition.

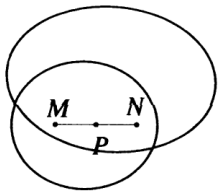
Une partie C de $\mathcal{E}$ vérifiant les conditions équivalentes précédentes est dite convexe. Nous appellerons dimension de C la dimension du sous-espace affine engendré par C. Nous considèrerons la partie $\emptyset$ comme étant convexe.



Convexe



Non convexe



Intersection de convexes

Proposition.

Soit $\mathcal{E}$ un espace affine réel. Pour toute famille $(C_i)_{i\in I}$ de parties convexes de $\mathcal{E}$, l'intersection $\bigcap_{i\in I} C_i$ est convexe.

Si f est une application affine de $\mathcal{E}$ dans un autre espace affine $\mathcal{E}'$, l'image $f(C)$ de toute partie convexe C de $\mathcal{E}$ est convexe et l'image réciproque $f^{-1}(C')$ de toute partie convexe C' de $\mathcal{E}'$ est convexe.

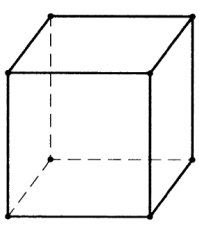
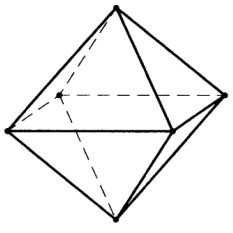
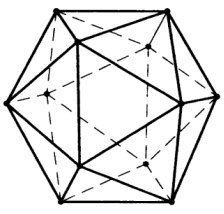
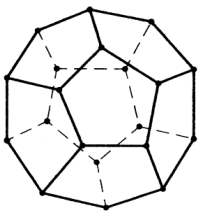
Démonstration. Le lecteur vérifiera l'une des conditions du lemme. ∎

Exercice. Soit E un espace vectoriel normé réel. Montrer que sa boule unité fermée E_1 est convexe. Si $E = \mathbb{R}^3$ muni de la norme $||\overrightarrow{x}|| = \max(|x_1|, |x_2|, |x_3|)$, quelle est la forme géométrique de E_1 et celle de la boule E_1' de son dual E' ?

Solution. Soient $\overrightarrow{x} \in E_1$, $\overrightarrow{y} \in E_1$, $\lambda \in [0,1]$. Dans $\mathcal{E}_E$ muni de l'origine $\overrightarrow{0}$, on a $\text{bar}[(\overrightarrow{x}, 1-\lambda), (\overrightarrow{y}, \lambda)] = (1-\lambda)\overrightarrow{x} + \lambda\overrightarrow{y}$. Ce barycentre est un élément de E_1 car $||(1-\lambda)\overrightarrow{x} + \lambda\overrightarrow{y}|| \leqslant (1-\lambda)\,||\overrightarrow{x}|| + \lambda\,||\overrightarrow{y}|| \leqslant (1-\lambda) + \lambda = 1$. Donc E_1 est convexe.

La boule unité $\{\overrightarrow{x} \mid |x_i| \leqslant 1, 1 \leqslant i \leqslant 3\} = [-1,1]^3$ de $E = \mathbb{R}^3$ muni de la norme considérée, est un cube C dont les 6 faces sont des carrés dans les plans affines d'équations $x_i = \pm 1$. Munissons le dual E' de la base $\mathcal{B}' = (\varphi_1, \varphi_2, \varphi_3)$ duale de la base canonique de $\mathbb{R}^3$. Les formes linéaires φ_i sont les fonctions coordonnées $\varphi_i : (x_1, x_2, x_3) \mapsto x_i$. Sur E', la norme duale est définie par $||\overrightarrow{\varphi}||' = \sup\{|\varphi(\overrightarrow{x})| ; \ \overrightarrow{x} \in E_1\}$. Sa boule unité est l'octaèdre Σ dont les 8 faces sont des triangles équilatéraux situés dans les plans d'équations $\pm y_1 \pm y_2 \pm y_3 = 1$. Les 6 sommets de Σ sont les formes linéaires $\pm\varphi_i$ intervenant dans les équations des faces du cube C. De même, les 8 sommets du cube C sont les formes linéaires sur E' intervenant dans les équations des faces de Σ. On dit que C et Σ sont des polyèdres réguliers duaux. Une façon géométrique de définir le polyèdre Σ dual d'un polyèdre convexe C, sans passer au dual de $\mathbb{R}^3$, est de construire Σ dont les sommets sont les centres des faces de C.

Un autre exemple de polyèdres réguliers duaux est donné par l'icosaèdre et le dodécaèdre. Le tétraèdre régulier est lui son propre dual. Ces cinq polyèdres réguliers, dits platoniciens, étaient connus au siècle de Périclès et fascinaient par leur régularité, leur perfection. Ce sont les seuls polyèdres réguliers dans l'espace euclidien (th. de Cauchy) comme nous allons le voir en 7-10.

7.7 Enveloppe convexe d'une partie

Proposition.

Soit $X \neq \emptyset$, une partie d'un espace affine réel $\mathcal{E}$. L'intersection $\mathrm{co}(X)$ de toutes les parties convexes de $\mathcal{E}$ qui contiennent X est la plus petite partie convexe de $\mathcal{E}$ qui contient X. C'est l'ensemble des barycentres $G = \mathrm{bar}\,[(A_1,\lambda_1),\dots,(A_k,\lambda_k)]$ où $k \in \mathbb{N}^*$, $A_1,\dots,A_k \in X$, $\lambda_1,\dots,\lambda_k \in \mathbb{R}^+$ avec $\sum_{i=1}^{k} \lambda_i = 1$.

Démonstration. D'après 7-6, prop., $\mathrm{co}(X)$ est convexe. Evidemment, $\mathrm{co}(X)$ contient X et $\mathrm{co}(X)$ est contenue dans toute partie convexe de $\mathcal{E}$ qui contient X. Notons C l'ensemble de tous les barycentres G de points de X pondérés avec des masses positives. Comme $\mathrm{co}(X)$ est convexe, elle contient tout élément de C. Vérifions que C est convexe. Comme C contient X, il en résultera que C contient la plus petite partie convexe $\mathrm{co}(X)$ contenant X. On aura $C = \mathrm{co}(X)$.

Soient $M = \mathrm{bar}\,((A_1,\lambda_1),\dots,(A_p,\lambda_p))$, $N = \mathrm{bar}\,((B_1,\mu_1),\dots,(B_q,\mu_q))$ des points de C, où $A_1,\dots,A_p,B_1,\dots,B_q$ appartiennent à X et $\lambda_1,\dots,\lambda_p,\mu_1,\dots,\mu_q$ à $\mathbb{R}^+$, avec $\sum_{i=1}^{p} \lambda_i = 1$, $\sum_{j=1}^{q} \mu_j = 1$. Soit $\lambda \in [0,1]$. On a $\mathrm{bar}((M,1-\lambda),(N,\lambda)) =$ $\mathrm{bar}[A_1,(1-\lambda)\lambda_1),\dots,(A_p,(1-\lambda)\lambda_p),(B_1,\lambda\mu_1),\dots,(B_q,\lambda\mu_q)] \in C$ car les masses figurant au second membre sont positives, de somme 1, d'où la conclusion. ∎

Définition.

On appelle $\mathrm{co}(X)$ l'enveloppe convexe de X.

Corollaire.

Soient $\mathcal{E}$ et $\mathcal{E}'$ des espaces affines et $f \in \mathcal{A}(\mathcal{E},\mathcal{E}')$. Alors $f(\mathrm{co}(X)) = \mathrm{co}(f(X))$.

Démonstration. Comme f conserve le barycentre (voir 7-2), c'est évident. ∎

Exemples. Si $X = \{A,B\}$, où $A \neq B$, $\mathrm{co}(X)$ est le segment $[AB]$.
Si $X = \{A,B,C\}$, où $A \neq B$ et $C \notin AB$, alors $\mathrm{co}(X)$ est le triangle ABC (bord compris) dans le plan affine engendré par A,B,C.

7.8 Points extrémaux d'une partie convexe

Lemme.

Soit C une partie convexe d'un espace affine réel $\mathcal{E}$ et soit $P \in C$. Les conditions suivantes sont équivalentes.

(i) $\forall M \in C \quad \forall N \in C \quad P = \mathrm{bar}\left((M,\frac{1}{2}),(N,\frac{1}{2})\right) \quad \Rightarrow \quad M = P = N$.

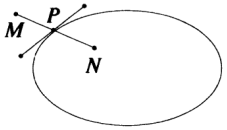
(ii) $\forall M \in C \ \forall N \in C \ \forall \lambda \in]0,1[\quad P = \mathrm{bar}\,((M,1-\lambda),(N,\lambda)) \ \Rightarrow \ M = P = N$.

(iii) *Le complémentaire C_0 de $\{P\}$ dans C est convexe.*

Démonstration. (i) ⇒ (ii) Soient $M,N \in C$, $\lambda \in]0,1[$, $P = \mathrm{bar}\,((M,1-\lambda),(N,\lambda))$. Si $\lambda = \frac{1}{2}$, d'après (i) on a $M = P = N$. Supposons $\lambda \neq \frac{1}{2}$, par exemple $\lambda < \frac{1}{2}$. On a $\overrightarrow{MP} = (1-\lambda)\overrightarrow{MM} + \lambda\overrightarrow{MN} = \lambda\overrightarrow{MN}$ donc P est entre M et le milieu du segment $[MN]$.

Soit $Q = \text{bar}((M, 1-\lambda'), (M, \lambda'))$ où $\lambda' = 2\lambda$. On a $\overrightarrow{MQ} = 2\lambda\overrightarrow{MN} = 2\overrightarrow{MP}$ donc Q est symétrique de M par rapport à P et $Q \in [MN] \subset C$ car $0 < 2\lambda < 1$. On a donc $P = \text{bar}\left((M, \frac{1}{2}), (Q, \frac{1}{2})\right)$. D'après (i), $M = P = Q$. Comme $2\lambda\overrightarrow{MN} = \overrightarrow{MQ} = \overrightarrow{0}$, on obtient $N = M = P$.

(ii) $\Rightarrow$ (iii) Soient $M \in C_0$, $N \in C_0$, $\lambda \in [0,1]$ et $G = \text{bar}\left((M, 1-\lambda), (N, \lambda)\right)$. Vérifions que $G \in C_0$. Pour $\lambda = 0$ ou 1 on a $G \in C_0$ car $G = M$ ou N. Pour $\lambda \in]0,1[$, on a $G \in C$ car C est convexe. Si on avait $G = P$, on aurait $M = P = N$ d'après (ii). C'est exclu car $M, N \in C_0$. Donc $G \in C_0$ et C_0 est convexe.



(iii) $\Rightarrow$ (i) Soient $M, N \in C$ d'isobarycentre P. Si on avait $M, N \in C_0$, (iii) donnerait $P \in C_0$. C'est absurde. On a donc $M = P$ ou $N = P$. Alors $M = P = N$ car $\overrightarrow{MP} = \overrightarrow{PN}$. ∎

Définition.

Un tel point P de la partie convexe C, qui ne peut être isobarycentre de deux points distincts de C, est appelé un point extrémal de C.

Proposition.

Soit C une partie convexe de $\mathcal{E}_n$. Toute application affine f de $\mathcal{E}_n$ dans lui-même telle que $f(C) = C$ permute les points extrémaux de C.

Démonstration. Soit $\mathcal{F}$ le sous-espace affine de $\mathcal{E}_n$ engendré par C. Alors $f(\mathcal{F})$ est engendré par $f(C) = C$ donc $f(\mathcal{F}) = \mathcal{F}$. Ainsi $\mathcal{F}$ est invariant par f qui induit une application affine de $\mathcal{F}$ dans lui-même, que nous appelons encore f, quitte à remplacer $\mathcal{E}_n$ par $\mathcal{F}$. Comme $\mathcal{F}$ est de dimension finie, l'application affine surjective f est un automorphisme affine de $\mathcal{F}$ (6-3, prop. 1). C'est une bijection de C sur C.

Soit P un point extrémal de C. Vérifions que $P' = f(P)$ est un point extrémal de C. Supposons que $P' = \text{bar}((M', \frac{1}{2}), (N', \frac{1}{2}))$, où $M' \in C$, $N' \in C$. Les points $M = f^{-1}(M')$ et $N = f^{-1}(N')$ appartiennent à $C = f^{-1}(C)$ et $P = \text{bar}((M, \frac{1}{2}), (N, \frac{1}{2}))$ car l'application affine f^{-1} conserve le barycentre. Puisque P est extrémal, on en déduit que $P = M = N$ et donc que $P' = M' = N'$. Ainsi P' est extrémal pour C.

Appliquons à f^{-1} ce résultat. Pour tout point extrémal P de C on a $P_0 = f^{-1}(P)$ extrémal et $P = f(P_0)$. La restriction s_f de f à l'ensemble X des points extrémaux de C est donc surjective de X sur X. Comme f est injective on a $s_f \in \mathcal{S}_X$. ∎

Exercice 1. Dans un espace vectoriel euclidien E, déterminer l'ensemble X des points extrémaux de la boule unité E_1. Montrer que $\text{co}(X) = E_1$.

Solution. Notons O le centre de E_1. Si P est à l'intérieur de E_1, il existe une boule fermée de centre P de rayon $r > 0$ contenue dans E_1. Si $[AB]$ est un diamètre de cette boule, on a $P = \text{bar}[(A, \frac{1}{2}), (B, \frac{1}{2})]$ et P n'est pas extrémal.

Soit P un point frontière de E_1. On a $OP = 1$. Soient $A \in E_1, B \in E_1$, tels que $P = \text{bar}[(A, \frac{1}{2}), (B, \frac{1}{2})]$. Si on suppose $A \neq B$, la formule de la médiane donne

$$2OP^2 < 2OP^2 + \tfrac{1}{2}AB^2 = OA^2 + OB^2 \leqslant 2 \quad \text{d'où} \quad OP < 1.$$

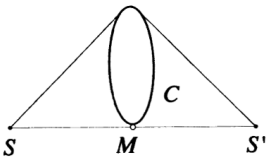
C'est absurde donc $A = B$ et P est extrémal. Ainsi X est la sphère unité.

Comme O est milieu de tout diamètre $[AB]$, c'est un point de $\text{co}(X)$. Soit $M \in E_1 \setminus \{O\}$. Posons $r = OM$. Soit A le point de X tel que $\overrightarrow{OA} = \frac{1}{r}\overrightarrow{OM}$. Alors $M = \text{bar}[(O, r), (A, 1-r)] \in \text{co}(X)$. Donc $\text{co}(X)$ contient E_1. Comme $\text{co}(X)$ est la plus petite partie convexe qui contient X, on a $\text{co}(X) \subset E_1$ et donc $\text{co}(X) = E_1$.

Exercice 2. Soit C une partie convexe du plan affine réel $\mathcal{E}_2$. Montrer que l'ensemble X des points extrémaux de C est fermé dans C. Montrer que cette propriété n'est plus vraie dans l'espace affine euclidien $\mathcal{E}_3$.

Solution. Soit $P \in C$ qui est limite d'une suite (P_n) de X. Montrons par l'absurde que P est extrémal. Supposons que P ne soit pas extrémal. Il existe alors $A \in C, B \in C$, distincts, tels que P soit le milieu de $[AB]$. Quitte à supprimer de (P_n) les premiers termes, on peut supposer $PP_n < PA$ pour tout n. Les points P_n ne peuvent alors appartenir à $]AB[\subset C$ sinon ils ne seraient pas extrémaux. Il existe donc une infinité de points P_n dans l'un des demi-plans ouverts délimités par la droite (AB). Quitte à remplacer la suite (P_n) par une sous-suite, on peut supposer qu'ils appartiennent tous au même demi-plan ouvert. Soit P_{n_0} un de ces points. Puisque la suite (P_n) tend vers P sans appartenir à la droite (AB), pour n assez grand, le point P_n est à l'intérieur du triangle $P_{n_0}AB \subset C$. Il existe deux points distincts de ce triangle dont P_n est le milieu. Cela contredit le fait que P_n soit un point extrémal de C.

Pour avoir un contre-exemple dans $\mathcal{E}_3$, considérons par exemple un cône convexe fermé de sommet S dont la base est un disque fermé limité par un cercle Γ et dont une génératrice (SM) est perpendiculaire à la base. Considérons la réunion C de ce cône avec le cône symétrique par rapport à la base et dont S' est le sommet. Les points extrémaux du convexe C obtenu sont S, S' et les points de $\Gamma \setminus \{M\}$, qui n'est pas fermé.



7.9 Sommets des polygones et polyèdres convexes

Proposition.

Dans le plan affine réel $\mathcal{E}_2$, si l'intersection C d'un nombre fini de demi-plans fermés est non vide, c'est une partie convexe. Ses points extrémaux sont les sommets de C. De même dans l'espace affine réel $\mathcal{E}_3$, les points extrémaux d'un polyèdre convexe fermé sont les sommets du polyèdre.

Démonstration. Munissons $\mathcal{E}_2$, d'un repère cartésien $(O, \overrightarrow{i}, \overrightarrow{j})$. Considérons deux droites concourantes D et D', d'équations

$$ax + by - c = 0 \qquad , \qquad a'x + b'y - c' = 0\,.$$

Les demi-plans $\Gamma = \{M(x,y) \mid ax + by - c \geqslant 0\}$ et $\Gamma' = \{M(x,y) \mid a'x + b'y - c' \geqslant 0\}$, sont convexes car images réciproques de $[0, +\infty[$, qui est convexe, par des applications affines. L'angle $C = \Gamma \cap \Gamma'$ est donc une partie convexe de $\mathcal{E}_2$. Vérifions que $P = D \cap D'$ est un point extrémal de C. Soient $M, N \in C$ et $\lambda \in]0,1[$, tels que $P = \text{bar}\,((M, 1-\lambda), (N, \lambda))$. On a $\overrightarrow{OP} = (1-\lambda)\,\overrightarrow{OM} + \lambda\,\overrightarrow{ON}$ donc :

$$x_P = (1-\lambda)\,x_M + \lambda\,x_N \qquad , \qquad y_P = (1-\lambda)\,y_M + \lambda\,y_N\,.$$

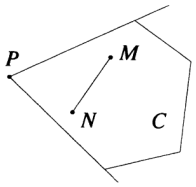
Exprimons que $P \in D$:

$$0 = ax_P + by_P - c = (1-\lambda)(ax_M + by_M - c) + \lambda(ax_N + by_N - c)\,.$$

On a $\lambda > 0$, $1 - \lambda > 0$. Les parenthèses ci-dessus sont positives. Donc nécessairement $ax_M + by_M - c = 0$ et $ax_N + by_N - c = 0$. De même, le fait que $0 = a'x_P + b'y_P - c'$, nécessite que $a'x_M + b'y_M - c' = 0$ et $a'x_N + b'y_N - c' = 0$. On a donc $M \in D \cap D'$ et $N \in D \cap D'$, d'où $M = P = N$. Ainsi P est point extrémal de C.

Si C est un polygone convexe, intersection d'un nombre fini de demi-plans fermés, d'après ce qui précède, chaque sommet P est point extrémal de l'angle formé par les deux côtés de C aboutissant au point P. Il est donc *a fortiori* extrémal pour C.

Par ailleurs, tout point de C intérieur à C ou situé sur un côté de C sans être un sommet, est isobarycentre de deux points distincts de C. Il n'est pas extrémal.



De même, dans $\mathcal{E}_3$ les points extrémaux d'un polyèdre convexe sont les sommets du polyèdre. (Tout cela se généralise à $\mathcal{E}_n$.) ■

Corollaire.

Soit C un polygone (resp. un polyèdre) convexe de $\mathcal{E}_2$ (resp. $\mathcal{E}_3$), non aplati. L'ensemble G des applications affines f de $\mathcal{E}_2$ (resp. $\mathcal{E}_3$) dans lui-même telles que $f(C) = C$ est un sous-groupe de $Aut(\mathcal{E}_2)$ (resp. $Aut(\mathcal{E}_3)$). Tout $f \in G$ induit une permutation s_f de l'ensemble X des sommets de C et $\varphi : f \mapsto s_f$ est un homomorphisme injectif de G dans $\mathcal{S}_X$.

Démonstration. Tout $f \in G$ est surjective car le sous-espace affine $f(\mathcal{E}_2)$ contient $f(C) = C$ qui engendre $\mathcal{E}_2$. Donc f est bijective (voir 6-3). Pour tous f et g dans G, on a $g^{-1} \circ f(C) = C$ donc G est un sous-groupe de $\mathrm{Aut}(\mathcal{E}_2)$. D'après les propositions 7-8 et 7-9, tout $f \in G$ définit une permutation s_f des sommets. On a évidemment $s_{f\circ g} = s_f \circ s_g$ donc $\varphi : f \mapsto s_f$ est un homomorphisme de groupes de G dans $\mathcal{S}_X$. Si $s_f = \mathrm{Id}$, on a $f = \mathrm{Id}_{\mathcal{E}_2}$ car l'ensemble des sommets de C contient un triangle non aplati, c'est-à-dire un repère affine de $\mathcal{E}_2$. Donc $\mathrm{Ker}(\varphi) = \{\mathrm{Id}_{\mathcal{E}_2}\}$ et φ est injectif. ■

Exercice. Dans le plan affine réel $\mathcal{E}_2$ considérons un vrai triangle $C = A_1A_2A_3$. Etudier le sous-groupe G de $\mathrm{Aut}(\mathcal{E}_2)$ qui laisse C invariant.

Solution. Ici, $\{A_1, A_2, A_3\}$ est un repère affine de $\mathcal{E}_2$. Pour tout $s \in \mathcal{S}_3$, il existe (d'après 7-4, cor.) $f \in \mathcal{A}(\mathcal{E}_3)$ telle que $f(A_i) = s(A_i)$ pour $i = 1,2,3$ et f est alors telle que $f(C) = C$ d'après 7-7, cor. Donc G est un sous-groupe de $\mathrm{Aut}(\mathcal{E}_2)$ isomorphe à $\mathcal{S}_3$. On peut voir de même que dans $\mathcal{E}_3$ les applications affines qui conservent un tétraèdre non aplati C, constituent un groupe isomorphe à $\mathcal{S}_4$.

7.10 Les polyèdres convexes réguliers

Appelons graphe dans $\mathcal{E}_n(\mathbb{R})$ un système $G = (G_0, G_1)$, où G_0 est une famille finie non vide de points appelés sommets et où G_1 est une famille finie d'arcs de courbe continus, sans points doubles (arcs simples de Jordan), appelés arêtes. Chaque arête a pour extrémités deux sommets distincts, seuls éléments de G_0 sur cette arête. Deux arêtes distinctes ne peuvent se couper qu'en leurs extrémités. Posons $s = \mathrm{card}(G_0)$ et $a = \mathrm{card}(G_1)$.

Proposition.

Soit G un graphe connexe tracé sur une sphère S de $\mathcal{E}_3(\mathbb{R})$. Le nombre f de composantes connexes de $S \setminus G$ vérifie la relation d'Euler $s - a + f = 2$.

Démonstration. Montrons la formule par récurrence sur le nombre a d'arêtes.
Si $a = 0$ alors $s = 1$ car $G_0 \neq \emptyset$ et G est connexe et $f = 1$. La formule est vraie.
Supposons vraie la relation pour les graphes connexes tracés sur S comportant $a - 1$ arêtes. Considérons G ayant a arêtes, avec $a \geqslant 1$.

Si G comporte un cycle (succession d'arêtes distinctes $\gamma_1, \ldots, \gamma_k$ constituant un chemin fermé), supprimons γ_1, mais pas les sommets qui sont ses extrémités. On

obtient un graphe connexe G' ayant $a' = a - 1$ arêtes, $s' = s$ sommets et délimitant $f' = f - 1$ composantes connexes de $S \setminus G'$ car γ_1 borde deux composantes connexes de $S \setminus G$ qui vont être réunies en retirant γ_1 (cette propriété topologique de la sphère ne serait pas vraie pour d'autres surfaces comme par exemple un tore). D'après l'hypothèse de récurrence $s - a + f = s' - a' + f' = 2$.

Si G ne comporte aucun cycle, étant connexe, c'est un arbre fini. Soit γ une arête aboutissant à un point terminal B. En supprimant γ et B, mais pas l'autre sommet extrémité de γ, on obtient un graphe connexe G' ayant $a' = a - 1$ arêtes, $s' = s - 1$ sommets et délimitant $f' = f$ composantes connexes. On a $s - a + f = s' - a' + f' = 2$ d'après l'hypothèse de récurrence. ∎

Corollaire 1. (Euler)

Soit P un polyèdre convexe compact (non aplati) de $\mathcal{E}_3(\mathbb{R})$. Les nombres s, a, f de sommets, d'arêtes, de faces de P sont tels que $s - a + f = 2$.

Démonstration. Choisissons un produit scalaire sur $\mathbb{R}^3$. Choisissons $A \in P$. Puisque P n'est pas aplati, on peut choisir dans P des points $B \neq A$, $C \notin (AB)$ et D n'appartenant pas au plan du triangle ABC. Comme P est convexe, le tétraèdre $T = ABCD$ est inclus dans P. L'isobarycentre O de A, B, C, D est un point intérieur pour T et donc pour P. Soit $r > 0$ tel que la boule B de centre O de rayon r soit à l'intérieur de P. Pour tout point M de la frontière δP de P, on a $[OM] \cap \delta P = \{M\}$ (car $[OM[$ est à l'intérieur de P). Le segment $[MO]$ rencontre la sphère $S = \delta B$ en un point M' et l'application $\varphi : M \mapsto M'$ est bijective. Elle est continue car $\overrightarrow{OM'} = r(||\overrightarrow{OM}||)^{-1}\overrightarrow{OM}$. C'est donc un homéomorphisme car δP et S sont compacts. L'image par φ des sommets et des arêtes du polyèdre P est un graphe connexe sur S, d'où la relation d'Euler. ∎

Corollaire 2. (Cauchy)

Dans $\mathcal{E}_3(\mathbb{R})$, les cinq solides platoniciens sont les seuls polyèdres convexes réguliers.

Démonstration. Plus généralement, considérons un polyèdre convexe non aplati P tel que le nombre d'arêtes aboutissant à un sommet soit le même pour tous les sommets, égal à $p \geqslant 3$ et tel que toutes les faces possèdent le même nombre, soit $q \geqslant 3$, de côtés. Nous allons montrer que (p, q) a au plus 5 valeurs.

Toute arête sépare deux faces donc $fq = 2a$. Toute arête relie deux sommets donc $sp = 2a$. On a aussi la relation d'Euler, $s - a + f = 2$. Résolvons en s, a, f ce système :

$$s = \frac{4q}{2p + 2q - pq} \quad , \quad a = \frac{2pq}{2p + 2q - pq} \quad , \quad s = \frac{4p}{2p + 2q - pq}.$$

On a nécessairement $2p + 2q - pq > 0$ avec $p \geqslant 3$ et $q \geqslant 3$. Traçons l'hyperbole d'équation $2p + 2q - pq = 0$. Le domaine défini par les trois inégalités précédentes, ne contient que les couples d'entiers $(3,3)$, $(3,4)$, $(4,3)$, $(3,5)$, $(5,3)$.

On retrouve les nombres du tétraèdre régulier (qui est son propre dual), du cube et de l'octaèdre qui sont duaux (7-6, ex.), du dodécaèdre et de l'icosaèdre qui sont duaux. On peut se demander si pour (p, q) donné il n'y aurait pas plusieurs polyèdres réguliers. Mais les propriétés métriques d'un tel polyèdre montrent qu'il est unique (à déplacement près) si ses arêtes sont de longueur un (voir 8-12, figures). ∎

Exercices du chapitre 7

Ex 7 - 1

Soit $\mathcal{E}$ un espace affine sur un corps K de caractéristique $p \neq 3$. Montrer que deux triangles ABC et $A'B'C'$ ont le même isobarycentre si et seulement si $\overrightarrow{AA'} + \overrightarrow{BB'} + \overrightarrow{CC'} = \overrightarrow{0}$. Généraliser.

Ex 7 - 2

Dans $\mathbb{C}$, quel est l'isobarycentre des racines primitives 15^{e} de l'unité ?

Ex 7 - 3

Soient E un espace vectoriel sur le corps K et $\mathcal{E}$ un espace affine sur E. On considère trois points distincts A, B, C de $\mathcal{E}$ et $\sigma = (\alpha, \beta, \gamma) \in K^3$ tel que $\alpha + \beta + \gamma \neq -1$. On note f_σ l'application qui associe à $M \in \mathcal{E}$, le barycentre M' de $\big((A,\alpha),(B,\beta),(C,\gamma),(M,1)\big)$.

Montrer que f_σ est affine. Selon les valeurs de σ, préciser sa nature.

Soit $\overrightarrow{a} \in E$. Existe-t-il σ tel que f_σ soit la translation $t_{\vec{a}}$?

Soient $I \in \mathcal{E}$ et $\lambda \in K\backslash\{0\}$. Existe-t-il σ tel que f_σ soit l'homothétie $h_{I,\lambda}$?

Ex 7 - 4

Soit $R = (A, B, C)$ un repère affine du plan euclidien $\mathcal{E}_2(\mathbb{R})$. Montrer que les coordonnées barycentriques α, β, γ, relatives à R, d'un point $M \in \mathcal{E}_2$ vérifient :

$$\begin{array}{rcrcl} \beta\overrightarrow{MB} \wedge \overrightarrow{MA} & + & \gamma\overrightarrow{MC} \wedge \overrightarrow{MA} & = & \overrightarrow{0} \\ \gamma\overrightarrow{MC} \wedge \overrightarrow{MB} & + & \alpha\overrightarrow{MA} \wedge \overrightarrow{MB} & = & \overrightarrow{0} \\ \alpha\overrightarrow{MA} \wedge \overrightarrow{MC} & + & \beta\overrightarrow{MB} \wedge \overrightarrow{MC} & = & \overrightarrow{0}. \end{array}$$

En déduire que α, β, γ sont proportionnels aux aires algébriques des triangles construits sur $(\overrightarrow{MB}, \overrightarrow{MC})$, $(\overrightarrow{MC}, \overrightarrow{MA})$, $(\overrightarrow{MA}, \overrightarrow{MB})$. Montrer que le centre du cercle inscrit au triangle ABC est le barycentre de $(A,a),(B,b),(C,c)$, où $a = BC$, $b = CA$, $c = AB$. Quelles sont les coordonnées barycentriques des centres des cercles exinscrits ?

Ex 7 - 5

Soit $P \in \mathbb{C}[X]$, avec $\mathrm{d}^\circ(P) \geqslant 2$. Dans $\mathbb{C}$, montrer que l'ensemble $X_{P'}$ des racines du polynôme dérivé P' est contenu dans l'enveloppe convexe C de l'ensemble X_P des racines de P (th. de Lucas) et que les barycentres de X_P (les racines étant pondérées avec leur multiplicité) et de $X_{P'}$ sont égaux. Si $P \in \mathbb{R}[X]$ a n racines réelles distinctes, montrer que l'on retrouve un résultat classique.

Ex 7 - 6

Soit C une partie convexe de $\mathcal{E}_n = \mathcal{E}_n(\mathbb{R})$. Une fonction f de C dans $\mathbb{R}$ est dite convexe si pour tous $M \in C$, $N \in C$, et tout $\lambda \in [0,1]$, on a
$f(\mathrm{bar}((M,1-\lambda),(N,\lambda))) \leqslant (1-\lambda)f(M) + \lambda f(N)$.
On dit que f est strictement convexe si en outre pour $M \neq N$, $0 < \lambda < 1$, l'inégalité est stricte.

a) Montrer que f est convexe si et seulement si $\Omega_f = \{(M,t) \mid f(M) \leqslant t\}$ est une partie convexe de $\mathcal{E} \times \mathbb{R}$.

b) Si f est strictement convexe, montrer que tout point du graphe de f est un point extrémal de Ω_f.

c) Supposons f définie sur $\mathcal{E}_n$ et strictement convexe. Soit $t \in \mathbb{R}$. Si $C_t = \{M \in \mathcal{E} \mid f(M) \leqslant t\}$ est non vide, montrer que l'ensemble des points extrémaux de C_t est
$$E_t = \{M \in \mathcal{E} \mid f(M) = t\}.$$

d) Supposons $\mathcal{E}_n(\mathbb{R})$ euclidien, muni d'un repère orthonormé $\mathcal{R}$ et supposons f définie sur un voisinage ouvert de C, deux fois différentiable, la matrice $(\frac{\delta^2 f}{\delta x_i \delta x_j})(M)$ étant définie positive, pour tout $M \in C$. Montrer que f est strictement convexe.

Indications

Ex 7 - 1

Utiliser la relation vectorielle qui caractérise le barycentre.

Ex 7 - 2

Les racines $k^{\text{ièmes}}$ de l'unité, sont racines de $X^k - 1$ et ont pour somme 0.

Ex 7 - 3

La relation qui caractérise le barycentre montre que f_σ est une translation ou une homothétie.

Ex 7 - 4

Multiplier vectoriellement la relation qui caractérise le barycentre, par divers vecteurs. Dans le cas du centre du cercle inscrit, les aires des triangles sont proportionnelles aux longueurs des côtés.

Ex 7 - 5

Exprimer le polynôme comme produit de facteurs de degré un, prendre la dérivée logarithmique, rendre les dénominateurs positifs et conclure.

Ex 7 - 6

Il suffit d'appliquer les définitions. Pour c), penser à paramétrer le segment reliant deux points. Cela ramène à une variable.

Solutions des exercices du chapitre 7

Ex 7 - 1

Supposons $\text{caract}(K) \neq 3$, soit $3 \times \mathbf{1} \neq 0$. Alors l'isobarycentre G de ABC existe. Supposons que G soit également l'isobarycentre de $A'B'C'$. On a :

$$(1) \qquad \overrightarrow{GA} + \overrightarrow{GB} + \overrightarrow{GC} = \overrightarrow{0} \quad , \quad \overrightarrow{GA'} + \overrightarrow{GB'} + \overrightarrow{GC'} = \overrightarrow{0} \, ,$$

Par soustraction, on obtient $\overrightarrow{AA'} + \overrightarrow{BB'} + \overrightarrow{CC'} = \overrightarrow{0}$.

Réciproquement, supposons que $\overrightarrow{AA'} + \overrightarrow{BB'} + \overrightarrow{CC'} = \overrightarrow{0}$. L'isobarycentre G de A, B, C vérifie la première des relations (1). En ajoutant membre à membre, on obtient la deuxième des relations (1), qui prouve que G est isobarycentre de A', B', C'.

Le résultat s'étend au cas de deux suites finies $(A_1, \ldots, A_k)$ et $(A'_1, \ldots, A'_k)$.

Ex 7 - 2

Posons $\zeta = \exp \frac{2i\pi}{n}$. Soient $A_0, A_1, \ldots, A_{n-1}$ les sommets du polygone régulier à n côtés inscrit dans le cercle unité, d'affixes $z_0 = 1$, $z_1 = \zeta$, $\ldots$, $z_{n-1} = \zeta^{n-1}$. Puisque

$$\begin{aligned} X^n - 1 &= (X - z_0) \cdots (X - z_{n-1}) \\ &= X^n - (z_0 + \cdots + z_{n-1}) X^{n-1} + \cdots + (-1)^n z_0 \cdots z_{n-1} \ , \end{aligned}$$

on a $z_0 + \cdots + z_{n-1} = 0$ et donc $\overrightarrow{OA_0} + \cdots + \overrightarrow{OA_{n-1}} = \overrightarrow{0}$. Ainsi l'origine O est l'isobarycentre de $A_0, \ldots, A_{n-1}$. Dans $\mathbb{U}_{15}$, les racines primitives sont ζ^k, où k n'est

divisible ni par 3, ni par 5. Donc leur ensemble Λ_{15} est dans $\mathbb{U}_{15}$ le complémentaire de $\mathbb{U}_3 \cup \mathbb{U}_5 = \{1, z^3, \dots, z^{12}\} \cup \{1, z^5, z^{10}\}$. D'après ce qui précède on a :

$$0 = 1 + z + \cdots + z^{14} \quad , \quad 0 = 1 + z^5 + z^{10} \quad , \quad 0 = 1 + z^3 + \cdots + z^{12}.$$

Retranchons les deux dernières relations de la première. Il vient $0 = -1 + \sum z^i$, où la somme est prise sur Λ_{15}, avec $\text{card}\,(\Lambda_{15}) = \varphi(15) = 2 \times 4 = 8$. L'affixe de l'isobarycentre de Λ_{15} est donc $\frac{1}{8}$. Plus généralement, pour tout $n \in \mathbb{N}^*$ l'isobarycentre de l'ensemble Λ_n des racines $n^{\text{ièmes}}$ primitives a pour affixe $\frac{\tau(n)}{\varphi(n)}$, où τ est la fonction de Moebius et φ est la fonction d'Euler (voir Ex. 10-4).

Ex 7 - 3

Comme $\alpha + \beta + \gamma + 1 \neq 0$, le barycentre M' existe : f_σ est bien définie. Soient $M \in \mathcal{E}$, $\overrightarrow{x} \in E$ et $N = M + \overrightarrow{x}$. Posons $M' = f_\sigma(M)$, $N' = f_\sigma(N)$ et $\overrightarrow{x'} = \overrightarrow{M'N'}$. Fixons une origine $O \in \mathcal{E}$. La caractérisation du barycentre donne :

$$(1) \qquad \begin{cases} (\alpha+\beta+\gamma+1)\,\overrightarrow{OM'} &= \alpha\overrightarrow{OA} + \beta\overrightarrow{OB} + \gamma\overrightarrow{OC} + \overrightarrow{OM}, \\ (\alpha+\beta+\gamma+1)\,\overrightarrow{ON'} &= \alpha\overrightarrow{OA} + \beta\overrightarrow{OB} + \gamma\overrightarrow{OC} + \overrightarrow{ON}, \end{cases}$$

d'où $(\alpha+\beta+\gamma+1)\,\overrightarrow{M'N'} = \overrightarrow{MN}$, soit encore $\overrightarrow{x'} = \lambda\,\overrightarrow{x}$ où $\lambda = \frac{1}{\alpha+\beta+\gamma+1}$. Ainsi, f_σ est affine d'application linéaire associée $\lambda\,\mathrm{Id}_E$. C'est un élément du groupe H des homothéties et translations.

Si $\alpha + \beta + \gamma = 0$, alors f_σ est une translation car l'application linéaire associée est Id_E. D'après (1), le vecteur $\overrightarrow{a}$ de la translation est

$$\overrightarrow{a} = \overrightarrow{MM'} = \alpha\overrightarrow{OA} + \beta\overrightarrow{OB} + \gamma\overrightarrow{OC}.$$

Il ne dépend que de f_σ et non de l'origine O choisie. En prenant $O = A$,

$$(2) \qquad \overrightarrow{a} = \beta\overrightarrow{AB} + \gamma\overrightarrow{AC}.$$

Si $\alpha + \beta + \gamma \neq 0$, on a $\lambda \neq 1$. Alors f_σ est une homothétie. Son centre est l'unique point fixe I de f_σ. D'après (1) il vérifie $(\alpha+\beta+\gamma)\overrightarrow{OI} = \alpha\overrightarrow{OA} + \beta\overrightarrow{OB} + \gamma\overrightarrow{OC}$. C'est donc le barycentre de (A,α), (B,β), (C,γ).

D'après (2), si $f_\sigma = t_{\vec{a}}$ alors $\overrightarrow{a}$ appartient au sous-espace vectoriel $\mathrm{Vect}(\overrightarrow{AB}, \overrightarrow{AC})$ de E. Réciproquement, soit $\overrightarrow{a}$ dans ce sous-espace. Il existe β, $\gamma \in K$ tels que $\overrightarrow{a} = \beta\overrightarrow{AB} + \gamma\overrightarrow{AC}$. Posons $\alpha = -\beta - \gamma$. Alors f_σ est la translation de vecteur $\overrightarrow{a}$.

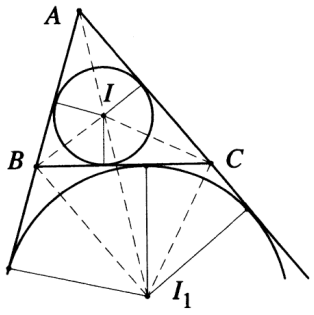
Si $f_\sigma = h_{I,\lambda}$, on a vu que $\lambda = \frac{1}{\alpha+\beta+\gamma+1}$, ce qui détermine $\alpha+\beta+\gamma$ et que I est dans le sous-espace affine $\mathcal{F}$ engendré par A, B, C. Réciproquement, considérons $I \in \mathcal{F}$, $\lambda \in K^*$ et supposons $\lambda \neq 0$. Il existe des masses α, β, γ vérifiant $\alpha+\beta+\gamma = \frac{1}{\lambda} - 1 \neq 0$, telles que $I = \mathrm{bar}[(A,\alpha), (B,\beta), (C,\gamma)]$. D'après a), $f_\sigma = h_{I,\lambda}$.

Ex 7 - 4

Le barycentre M de $(A,\alpha),(B,\beta),(C,\gamma)$ est tel que $\alpha\overrightarrow{MA} + \beta\overrightarrow{MB} + \gamma\overrightarrow{MC} = \overrightarrow{0}$. En multipliant vectoriellement par $\overrightarrow{MA}$, $\overrightarrow{MB}$ et $\overrightarrow{MC}$, on obtient les relations de l'énoncé. La mesure algébrique $\overline{MA}\,\overline{MB}\sin(\overrightarrow{MA}, \overrightarrow{MB})$ de $\overrightarrow{MA} \wedge \overrightarrow{MB}$ est l'aire algébrique du parallélogramme construit sur les deux vecteurs, c'est-à-dire le double de

l'aire algébrique du triangle. Ces trois relations montrent que α, β, γ sont proportionnels aux aires algébriques des triangles correspondants.

Soient I et r le centre et le rayon du cercle inscrit au triangle ABC. Orientons le plan de telle sorte que le repère $(I, \overrightarrow{IB}, \overrightarrow{IC})$ soit direct. L'aire du triangle construit sur $\overrightarrow{IB}, \overrightarrow{IC}$ est $\frac{1}{2}ra$ et celles des triangles ICA et IAB sont $\frac{1}{2}rb$ et $\frac{1}{2}rc$. Les coordonnées barycentriques de I sont donc proportionnelles à a, b, c.



Pour le centre I_1 du cercle exinscrit dans l'angle $(\overrightarrow{AB}, \overrightarrow{AC})$ par exemple, point de concours de la bissectrice intérieure de cet angle et des bissectrices extérieures de $(\overrightarrow{BC}, \overrightarrow{BA})$ et $(\overrightarrow{CA}, \overrightarrow{CB})$, les coordonnées1 barycentriques seront proportionnelles à $-a, b, c$ car c'est le cas pour les aires algébriques des triangles correspondants.

Ex 7 - 5

On peut supposer $P(X)$ unitaire. D'après le th. de d'Alembert, il est scindé : il existe donc $a, b, \ldots, c \in \mathbb{C}$ deux à deux distincts et $\alpha, \beta, \ldots, \gamma \in \mathbb{N}^*$ tels que $P(X) = (X-a)^\alpha (X-b)^\beta \cdots (X-c)^\gamma$. On en déduit l'égalité entre fractions rationnelles

$$\frac{P'(X)}{P(X)} = \frac{\alpha}{X-a} + \frac{\beta}{X-b} + \cdots + \frac{\gamma}{X-c}.$$

Soit z une racine de P'. Si z est racine de P, alors z appartient à l'enveloppe convexe C des racines de P. Si z n'est pas racine de P, alors on obtient :

$$0 = \frac{P'(z)}{P(z)} = \frac{\alpha}{z-a} + \frac{\beta}{z-b} + \cdots + \frac{\gamma}{z-c} = \frac{\alpha(\overline{z}-\overline{a})}{|z-a|^2} + \frac{\beta(\overline{z}-\overline{b})}{|z-b|^2} + \cdots + \frac{\gamma(\overline{z}-\overline{c})}{|z-c|^2},$$

d'où

$$\left(\frac{\alpha}{|z-a|^2} + \frac{\beta}{|z-b|^2} + \cdots + \frac{\gamma}{|z-c|^2}\right) z = \frac{\alpha}{|z-a|^2}\, a + \frac{\beta}{|z-b|^2}\, b + \cdots + \frac{\gamma}{|z-c|^2}\, c.$$

Cela prouve que z est barycentre des racines $a, b, \ldots, c$ de P affectées des masses positives $\frac{\alpha}{|z-a|^2}$, $\frac{\beta}{|z-b|^2}, \ldots, \frac{\gamma}{|z-c|^2}$. Donc z est élément de C.

Si $P(X) = X^n + a_{n-1}X^{n-1} + \ldots + a_0$, on a $\frac{1}{n}(\alpha a + \beta b + \ldots + \gamma c) = -\frac{a_{n-1}}{n}$. Si on dérive $P(X)$, le calcul analogue pour $P'(X)$ conduit à la même valeur, donc le barycentre de X_P est égal au barycentre de $X_{P'}$.

Si $P \in \mathbb{R}[X]$, de degré n, à n racines réelles distinctes $a_1 < \cdots < a_n$, le th. de Rolle montre que pour $i = 1, \ldots, n-1$ il existe $c_i \in]a_i, a_{i+1}[$ tel que $P'(c_i) = 0$. Comme $d^\circ(P') = n-1$, P' n'a pas d'autre racine. Ses racines appartiennent toutes à $[a_1, a_n]$ qui est l'enveloppe convexe de l'ensemble des racines de P.

Ex 7 - 6

a) Soient $(M,t) \in \Omega_f$, $(M',t') \in \Omega_f$ et $\lambda \in [0,1]$. On a :

(1) $\mathrm{bar}[((M,t),(1-\lambda)), ((M',t'),\lambda)] = (\mathrm{bar}[(M,1-\lambda), (M',\lambda)], (1-\lambda)t + \lambda t')$

car les projections de $\mathcal{E} \times \mathbb{R}$ sur $\mathcal{E}$ et $\mathbb{R}$ sont affines. Supposons f convexe. Alors,

$$f(\text{bar}[(M,1-\lambda)\,,\,(M',\lambda)]) \leqslant (1-\lambda)f(M)+\lambda f(M') \leqslant (1-\lambda)t+\lambda t'\,.$$

Ainsi, $\text{bar}[((M,t),(1-\lambda))\,,\,((M',t'),\lambda)] \in \Omega_f$ et Ω_f est convexe.

Réciproquement, supposons Ω_f convexe. Pour tout couple de points $(M,f(M))$ et $(M',f(M'))$ du graphe de f, le segment qui les relie est contenu dans Ω_f. D'après (1), cela signifie que pour tout $\lambda \in [0,1]$, on a :

$$f(\text{bar}[(M,1-\lambda)\,,\,(M',\lambda)]) \leqslant (1-\lambda)f(M)+\lambda f(M')\,.$$

Donc f est convexe.

b) Soient $A \in C$ et $t = f(A)$. Considérons $(M,\alpha) \in \Omega_f$, $(N,\beta) \in \Omega_f$, $\lambda \in]0,1[$, tels que $(A,t) = \text{bar}[((M,\alpha),1-\lambda),((N,\beta),\lambda)]$. On a $M,N \in C$. Supposons $M \neq N$. Les projections de $\mathcal{E}\times\mathbb{R}$ sur $\mathcal{E}$ et $\mathbb{R}$ étant affines,

$$(2) \qquad A = \text{bar}[(M,1-\lambda),(N,\lambda)] \quad \text{et} \quad t = \alpha(1-\lambda)+\beta\lambda\,.$$

Si on suppose f strictement convexe, on a

$$t \;=\; f(A) < (1-\lambda)f(M)+\lambda f(N) \leqslant (1-\lambda)\alpha+\lambda\beta\,.$$

Cela contredit (2). Donc $M = N = A$. On en déduit,

$$t = f(A) = f(M) \leqslant \alpha \quad , \quad t = f(A) = f(N) \leqslant \beta \quad \text{et} \quad t = \alpha(1-\lambda)+\beta\lambda\,,$$

d'où $t = \alpha$ ou $t = \beta$. Ainsi (A,t) est extrémal dans Ω_f.

c) L'intersection Σ_t de Ω_f avec l'hyperplan "horizontal" $\mathcal{H} = \{(M,\lambda) \mid \lambda = t\}$ est une partie convexe de $\mathcal{E}\times\mathbb{R}$, contenue dans Ω_f. Tout point de Σ_t qui est extrémal pour Ω_f est a fortiori extrémal pour Σ_t. D'après b), c'est le cas de tout (A,t) où $A \in C$ et $t = f(A)$. La projection $p : (M,t) \mapsto M$ de $\mathcal{H}$ sur $\mathcal{E}$ est un isomorphisme affine. Le projeté A de $(A,f(A))$ est donc un point extrémal de $C_t = p(\Sigma_t)$. Une fonction convexe définie sur une partie convexe ouverte est continue donc f définie sur $\mathcal{E}_n$ est continue sur $\mathcal{E}_n$. Ainsi $\{M \in \mathcal{E}_n \mid f(M) < t\}$ est une partie ouverte, intérieure à C_t. Or, un point de l'intérieur d'une partie convexe n'est pas extrémal. Donc E_t est l'ensemble des points extrémaux de C_t.

d) Dans $\mathcal{R}$, on peut voir f comme une fonction de $\overrightarrow{OM}$ et de ses coordonnées $x_1,\dots,x_n$. Soient $M \in C$ et $N \in C$, avec $M \neq N$. Pour $t \in [0,1]$, posons

$$\varphi(t) \;=\; f((1-t)\,\overrightarrow{OM}+t\overrightarrow{ON}) \;=\; f(\overrightarrow{OM}+t\,\overrightarrow{MN})\,.$$

On a :

$$\varphi'(t) \;=\; Df(\overrightarrow{OM}+t\,\overrightarrow{MN})\cdot\overrightarrow{MN} \qquad , \qquad \varphi''(t) \;=\; q_t(\overrightarrow{MN})\,,$$

où q_t est la forme quadratique de matrice $((\dfrac{\delta^2 f}{\delta x_i \delta x_j})(\overrightarrow{OM}+t\overrightarrow{MN}))$. Par hypothèse, on a $\varphi''(t) > 0$ pour tout $t \in [0,1]$ donc la fonction φ est strictement convexe sur $[0,1]$. Pour $0 < \lambda < 1$ on a donc :

$$f((1-t)\,\overrightarrow{OM}+t\overrightarrow{ON}) \;=\; \varphi(t) < (1-t)\,\varphi(0)+t\,\varphi(1) \;=\; (1-t)\,f(M)+t\,f(N)\,.$$

Chapitre 8

Géométrie affine euclidienne

8.1 Espaces affines euclidiens

Soient E un espace vectoriel sur $\mathbb{R}$ et $\mathcal{E}$ un espace affine sur E. Si E est muni d'une norme, en posant $d(M,N) = \|\overrightarrow{MN}\|$ on obtient une distance sur $\mathcal{E}$. En effet, d'après la relation de Chasles, pour tous points M, N, P de $\mathcal{E}$, on a :

$d(M,P) = \|\overrightarrow{MP}\| = \|\overrightarrow{MN} + \overrightarrow{NP}\| \leqslant \|\overrightarrow{MN}\| + \|\overrightarrow{NP}\| = d(M,N) + d(N,P)$.

$d(M,N) = \|\overrightarrow{MN}\| = \| -\overrightarrow{NM}\| = \|\overrightarrow{NM}\| = d(N,M)$.

$d(M,N) = 0 \quad \Leftrightarrow \quad \|\overrightarrow{MN}\| = 0 \quad \Leftrightarrow \quad \overrightarrow{MN} = \overrightarrow{0} \quad \Leftrightarrow \quad M = N$.

De plus, pour tout $\overrightarrow{a} \in E$, en posant $M' = t_{\vec{a}}(M)$ et $N' = t_{\vec{a}}(N)$ on a :

$$d(t_{\vec{a}}(M), t_{\vec{a}}(N)) = d(M', N') = \|\overrightarrow{M'N'}\| = \|\overrightarrow{MN}\| = d(M,N).$$

Pour toute homothétie $h_{A,\lambda}$, pour tout $M \in \mathcal{E}$ et pour tout $N \in \mathcal{E}$, on a :

$$d(h_\lambda(M), h_\lambda(N)) = d(A + \lambda\overrightarrow{AM}, A + \lambda\overrightarrow{AN}) = \|\lambda\overrightarrow{MN}\| = |\lambda|\, d(M,N).$$

Réciproquement, on vérifiera facilement que toute distance sur $\mathcal{E}$ telle que toute translation soit une isométrie et telle que toute homothétie de rapport λ multiplie les distances par $|\lambda|$, est associée de cette façon à une norme sur E.

Si E est de dimension finie n, toutes les normes sont équivalentes sur E. Toutes ces distances sur $\mathcal{E}$, qui leur sont canoniquement associées, sont uniformément équivalentes. Il existe donc sur $\mathcal{E}$ une topologie canonique que toute norme sur E permet de définir. Pour cette topologie, les translations et les homothéties sont des homéomorphismes. En fait, on a vu au §1 que $\mathcal{E}$ est isomorphe à l'espace affine $\mathcal{E}_n$ obtenu en faisant agir $\mathbb{R}^n$ sur lui-même par translations. Si on identifie $\mathcal{E}$ muni d'une origine A avec $\mathbb{R}^n$ à l'aide de l'isomorphisme $\varphi_A : \overrightarrow{x} \mapsto A + \overrightarrow{x}$, on retrouve bien sûr la topologie canonique de $\mathbb{R}^n$. Toute norme sur E définit cette topologie. Il est particulièrement intéressant d'utiliser une norme associée à un produit scalaire.

Définition.

On appelle espace (affine) euclidien de dimension n, un espace affine $\mathcal{E}$ sur un espace vectoriel euclidien E de dimension n.

Notons $(\overrightarrow{x}, \overrightarrow{y}) \mapsto (\overrightarrow{x}\,|\,\overrightarrow{y})$ le produit scalaire de E. Il définit sur E la norme

d'expression $\|\overrightarrow{x}\| = \sqrt{(\overrightarrow{x}\,|\,\overrightarrow{x})}$, d'où la distance euclidienne de $\mathcal{E}$:

$$(M,N) \mapsto MN = \sqrt{(\overrightarrow{MN}\,|\,\overrightarrow{MN})}\,.$$

Deux sous-espaces affines $\mathcal{F},\mathcal{G}$ de $\mathcal{E}$ sont dits *orthogonaux*, si leurs directions F,G sont des sous-espaces vectoriels de E orthogonaux, c'est-à-dire tels que $G \subset F^{\perp}$.

On appelle *repère orthonormé* de $\mathcal{E}$, un repère cartésien $(A,\overrightarrow{e_1},\ldots,\overrightarrow{e_n})$ tel que $(\overrightarrow{e_1},\ldots,\overrightarrow{e_n})$ soit une base orthonormée de E.

8.2 Rappels sur le groupe orthogonal

Soit v un endomorphisme de l'espace vectoriel euclidien E. Rappelons que l'adjoint de v est l'unique élément v^* de $\mathcal{L}(E)$ tel que :

$$\forall\,\overrightarrow{x}\in E \quad \forall\,\overrightarrow{y}\in E \qquad (v(\overrightarrow{x})\,|\,\overrightarrow{y}) = (\overrightarrow{x}\,|\,v^*(\overrightarrow{y}))\,.$$

Le produit scalaire s'exprime en fonction de la norme par la formule de polarisation :

$$4\,(\overrightarrow{x}\,|\,\overrightarrow{y}) = \|\overrightarrow{x}+\overrightarrow{y}\|^2 - \|\overrightarrow{x}-\overrightarrow{y}\|^2\,.$$

Soit $v\in\mathcal{L}(E)$. D'après cette formule, les propriétés suivantes sont donc équivalentes.

- $\|v(\overrightarrow{x})\| = \|\overrightarrow{x}\|$ pour tout $x\in E$ (v est isométrique).
- $(v(\overrightarrow{x})|v(\overrightarrow{y})) = (\overrightarrow{x}\,|\,\overrightarrow{y})$ pour tout $\overrightarrow{x}\in E$ et pour tout $\overrightarrow{y}\in E$.
- $v^*v = \mathrm{Id}_E$.
- L'image par v de toute base orthonormée de E est une base orthonormée de E.
- Il existe une base orthonormée de E dont l'image par v est une base orthonormée.
- Dans une base orthonormée de E, la matrice de v est orthogonale.

Un tel endomorphisme de E est appelé un *endomorphisme orthogonal*. L'ensemble $O(E)$ de ces endomorphismes est un sous-groupe du groupe $\mathrm{GL}(E)$ appelé le *groupe orthogonal* de E. Nous allons rappeler quelques propriétés utiles pour la suite.

Lemme 1.

Considérons $v\in O(E)$ et un sous-espace vectoriel F de E. On a $v(F^{\perp}) = v(F)^{\perp}$. En particulier, si F est stable par v, alors $F^{\perp}$ est stable par v.

Démonstration. On a $(v(\overrightarrow{x})|v(\overrightarrow{y})) = (\overrightarrow{x}\,|\,\overrightarrow{y}) = 0$ pour tout $\overrightarrow{y}\in F^{\perp}$, pour tout $\overrightarrow{x}\in F$ et donc $v(F^{\perp})\subset v(F)^{\perp}$. Or v est isométrique et donc injectif. Il en résulte que $\dim(v(F^{\perp})) = \dim(F^{\perp}) = \dim(E)-\dim(F)$, et que $\dim(v(F)^{\perp}) = \dim(E)-\dim(v(F)) = \dim(E)-\dim(F)$. On en déduit que $v(F^{\perp}) = v(F)^{\perp}$.

Si F est stable par v, soit $v(F)\subset F$, on a $v(F)=F$ car v étant injectif, les dimensions de F et de $v(F)$ sont égales. On en déduit que $v(F^{\perp}) = v(F)^{\perp} = F^{\perp}$. ∎

Lemme 2.

Soient E un espace vectoriel de dimension finie sur le corps K et $v\in\mathcal{L}(E)$. Soit F un sous-espace vectoriel de E, distinct de $\{\overrightarrow{0}\}$, stable par v, minimal vis-à-vis de ces propriétés. Alors, le polynôme minimal p_w de la restriction $w = v|_F$ est irréductible dans $K[X]$ et $\dim(F) = \mathrm{d}^{\circ}(p_w)$.

Démonstration. Rappelons que l'ensemble des polynômes à coefficients dans K, qui annulent un endomorphisme $w \in \mathcal{L}(F)$, est un idéal de l'anneau $K[X]$ et donc constitué des multiples $p_w(X)q(X)$ d'un polynôme unitaire $p_w(X)$ (voir 10-2). Ce polynôme $p_w(X)$ qui est le polynôme de plus petit degré, unitaire et donc non nul, annulant w est appelé le *polynôme minimal* de w.

Considérons la décomposition $p_w(X) = p_1(X)^{k_1} \cdots p_s(X)^{k_s}$ de $p_w(X)$ en facteurs irréductibles unitaires. On a $p_w(w) = 0$ dans $\mathcal{L}(F)$, d'où :

$$F = \operatorname{Ker}(p_w(w)) = \operatorname{Ker}\left(p_1(w)^{k_1}\right) \oplus \cdots \oplus \operatorname{Ker}\left(p_s(w)^{k_s}\right) . \quad (1)$$

Les endomorphismes $p_j(w)^{k_j}$ commutent avec w. Les sous-espaces $\operatorname{Ker}\left(p_j(w)^{k_j}\right)$ de F sont donc stables par w. Puisque F est minimal avec cette propriété, F est réduit à l'un de ces sous-espaces $\operatorname{Ker}\left(p_1(w)^{k_1}\right)$, autrement dit, $p_1(X)^{k_1}$ annule w et donc $p_w(X) = p_1(X)^{k_1}$. On a donc $0_F = p_1(w)^{k_1}$ et $p_1(w)$ est un endomorphisme nilpotent de F. On a $\operatorname{Ker}(p_1(w)) \neq \{0\}$, sinon $p_1(w)$ serait inversible et ne serait pas nilpotent et $\operatorname{Ker}(p_1(w))$ est stable par w. Comme F est minimal, on a $\operatorname{Ker}(p_1(w)) = F$. Ainsi $p_1(w) = 0_F$ et $p_1(X)$ est donc le polynôme minimal de w, ce qui prouve que $p_w(X)$ est irréductible. Soit $p_w(X) = X^m + \alpha_{m-1}X^{m-1} + \cdots + \alpha_0$ son expression.

Choisissons $\overrightarrow{x} \neq \overrightarrow{0}$ dans F. Les vecteurs $\overrightarrow{x}, w(\overrightarrow{x}), \ldots, w^{m-1}(\overrightarrow{x})$ engendrent un sous-espace vectoriel de F stable par w, puisque $w^m = -\alpha_{m-1}w^{m-1} - \cdots - \alpha_0 \operatorname{Id}_F$. Comme F est minimal, il est égal à F. Les vecteurs précédents sont donc générateurs pour F. Vérifions qu'ils sont libres. S'il existait $\lambda_0, \ldots, \lambda_{m-1}$, non tous nuls, tels que $\lambda_0 \overrightarrow{x} + \ldots + \lambda_{m-1}w^{m-1}(\overrightarrow{x}) = \overrightarrow{0}$, le polynôme $p(X) = \lambda_0 + \cdots + \lambda_{m-1}X^{m-1}$ serait tel que $p(w)(\overrightarrow{x}) = \overrightarrow{0}$. On aurait $p(w)w^k(\overrightarrow{x}) = w^k p(w)(\overrightarrow{x}) = \overrightarrow{0}$ pour $k = 0, \ldots, m-1$ et donc $p(w) = 0_F$ avec $\mathrm{d}^\circ(p) \leqslant m-1$, contredisant la définition du polynôme minimal $p_w(X)$. Ces vecteurs constituent donc une base de F et $\dim(F) = m = \mathrm{d}^\circ(p_w)$. ∎

Propositon.

Soit E un espace vectoriel euclidien et $v \in O(E)$. Alors E est somme directe orthogonale $E = \oplus F_k$ de sous-espaces vectoriels (F_k) stables par v, non nuls, minimaux. La dimension de ces sous-espaces est 1 ou 2. Les sous-espaces F_k de dimension 1 sont des sous-espaces propres relatif à la valeur propre 1 ou -1. Pour ceux de dimension 2, si on choisit une base orthonormée $(\overrightarrow{\imath}, \overrightarrow{\jmath})$ de F_k, la restriction de v à F_k a pour matrice $\begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix}$, où θ n'est pas multiple de π.

Démonstration. La famille des sous-espaces vectoriels non nuls de E, stables par v n'est pas vide car E en fait partie. Choisissons un tel sous-espace F_1 de dimension minimum. Alors F_1 est évidemment minimal. Les polynômes de $\mathbb{R}[X]$ irréductibles sont de degré 1 ou 2. D'après le lemme 2, la dimension de F_1 est 1 ou 2. D'après le lemme 1, $F_1^\perp$ est stable par v. Si $F_1^\perp \neq \{0\}$, on peut choisir un sous-espace F_2 de $F_1^\perp$, stable, de dimension minimale, qui est donc 1 ou 2. Alors $F = F_1 \oplus F_2$ est stable par v et $F^\perp$ également. Si $F^\perp \neq \{0\}$, on poursuit par récurrence, d'où la première assertion.

Si $\dim(F_k) = 1$, alors F_k est un sous-espace propre de v. Soient λ la valeur propre et $\overrightarrow{x} \in F_k$ avec $\overrightarrow{x} \neq \overrightarrow{0}$. On a $|\overrightarrow{x}| = |v(\overrightarrow{x})| = |\lambda|\,|\overrightarrow{x}|$ donc $|\lambda| = 1$.

Si $\dim(F_k) = 2$, soit $(\overrightarrow{\imath}, \overrightarrow{\jmath})$ une base orthonormée de F_k. Cette base oriente F_k. La restriction w de v à F_k applique $\overrightarrow{\imath}$ sur un vecteur de ce plan de longueur 1 soit

1. Nous utilisons le th. classique suivant, basé sur la relation de Bezout : si $P_1, \ldots, P_k$ sont des polynômes deux à deux premiers entre eux, pour tout $T \in \mathcal{L}(E)$, on a :
$\operatorname{Ker}((P_1 \cdots P_k)(T)) = \operatorname{Ker}(P_1(T)) \oplus \cdots \oplus \operatorname{Ker}(P_k(T))$.

$w(\overrightarrow{\imath}) = \cos\theta\,\overrightarrow{\imath} + \sin\theta\,\overrightarrow{\jmath}$ et applique $\overrightarrow{\jmath}$ sur un vecteur de longueur 1 orthogonal à $w(\overrightarrow{\imath})$, soit $w(\overrightarrow{\jmath}) = -\sin\theta\,\overrightarrow{\imath} + \cos\theta\,\overrightarrow{\jmath}$ ou $w(\overrightarrow{\jmath}) = \sin\theta\,\overrightarrow{\imath} - \cos\theta\,\overrightarrow{\jmath}$. Ce second cas ne peut pas se produire car alors w serait une symétrie par rapport à la droite d'angle polaire $\theta/2$ et aurait des droites de vecteurs propres, ce qui contredirait la minimalité de F_k. Pour la même raison, on ne peut avoir $\theta = 0$ ou π.

Il existe donc une base orthonormée de E dans laquelle v a une matrice bloc diagonale dont les blocs sont soit un scalaire égal à 1 ou -1, soit une matrice de rotation. ∎

8.3 Isométries affines

Proposition.

Soient E et E' des espaces vectoriels euclidiens de même dimension et $\mathcal{E}, \mathcal{E}'$ des espaces affines euclidiens sur E et E'. Soit $(A, \overrightarrow{e_1}, \ldots, \overrightarrow{e_n})$ un repère orthonormé de $\mathcal{E}$ et f une application affine de $\mathcal{E}$ dans $\mathcal{E}'$. Les conditions suivantes sont équivalentes.

(i) *f est isométrique.*

(ii) *L'application linéaire associée v_f est orthogonale.*

(iii) *$(f(A), v_f(\overrightarrow{e_1}), \ldots, v_f(\overrightarrow{e_n}))$ est un repère orthonormé de $\mathcal{E}'$.*

Démonstration. (i) ⇔ (ii) Posons $A' = f(A)$. Par définition des distances sur $\mathcal{E}$ et $\mathcal{E}'$, les bijections $\varphi_A : \overrightarrow{x} \mapsto A + \overrightarrow{x}$ de E sur $\mathcal{E}$ et $\varphi_{A'} : \overrightarrow{x'} \mapsto A' + \overrightarrow{x'}$ de E' sur $\mathcal{E}'$ sont des isométries. On a $f = \varphi_{A'} \circ v_f \circ \varphi_A^{-1}$, d'où l'équivalence de (i) et (ii).

(ii) ⇔ (iii) En effet, v_f est isométrique si et seulement si elle applique une base orthonormée de E sur un système orthonormé de E'. Un tel système étant libre et la dimension de E' étant n, c'est en fait une base de E'. ∎

Corollaire 1.

Soient $\mathcal{E}$ et $\mathcal{E}'$ des espaces affines euclidiens de même dimension n et $\mathcal{R} = (A, \overrightarrow{e_1}, \ldots, \overrightarrow{e_n})$ un repère orthonormé de $\mathcal{E}$. Pour tout repère orthonormé $\mathcal{R}' = (A', \overrightarrow{e'_1}, \ldots, \overrightarrow{e'_n})$ de $\mathcal{E}'$, il existe une application affine isométrique unique telle que :

$$(f(A), v_f(\overrightarrow{e_1}), \ldots, v_f(\overrightarrow{e_n})) = (A', \overrightarrow{e'_1}, \ldots, \overrightarrow{e'_n}).$$

Démonstration. Il existe une application affine f unique telle que $f(\mathcal{R}) = \mathcal{R}'$ (voir 6-4). C'est une isométrie d'après la proposition. ∎

Corollaire 2.

Un espace affine euclidien $\mathcal{E}$ de dimension finie n est isomorphe à l'espace affine canonique $\mathcal{E}_n(\mathbb{R})$, où $\mathbb{R}^n$ est muni du produit scalaire canonique (à isomorphisme isométrique près, il existe un seul espace affine euclidien de dimension finie n).

Démonstration. Soit $\mathcal{R}$ un repère orthonormé de $\mathcal{E}$. D'après le cor. 1, il existe une application affine isométrique unique f appliquant ce repère sur le repère orthonormé de $\mathbb{R}^n$ constitué du vecteur nul pour origine et de la base canonique de $\mathbb{R}^n$. ∎

Exercice. Soit C un cube dans l'espace affine euclidien $\mathcal{E}_3$. Montrer que l'ensemble G des applications affines f de $\mathcal{E}_3$ telles que $f(C) = C$ est un sous-groupe du groupe $\mathcal{I}_3$ des isométries de $\mathcal{E}_3$ et préciser son ordre. Même question si on remplace C par un octaèdre régulier.

Solution. Quitte à changer l'unité de longueur, on peut supposer que les arêtes de C ont pour longueur 1. D'après 7-9, cor., tout $f \in G$ permute les sommets A_i où $1 \leqslant i \leqslant 8$, de C. Si $f(A_1) = A_i$, $f(A_2) = A_j$, $f(A_3) = A_k$, $f(A_4) = A_\ell$, les images des arêtes $[A_1A_2]$, $[A_1A_4]$, $[A_1A_5]$ issues de A_1 sont les trois arêtes $[A_iA_j]$, $[A_iA_k]$, $[A_iA_\ell]$ issues de A_i. D'après la proposition, f est une isométrie et G est un sous-groupe de $\mathcal{I}_3$. Réciproquement, pour tout choix de trois arêtes $[A_iA_j]$, $[A_iA_k]$, $[A_iA_l]$ issues d'un sommet A_i de C, il existe une application affine unique appliquant le repère orthonormé $(A_1, \overrightarrow{A_1A_2}, \overrightarrow{A_1A_4}, \overrightarrow{A_1A_5})$ sur $(A_i, \overrightarrow{A_iA_j}, \overrightarrow{A_iA_k}, \overrightarrow{A_iA_l})$ et on a $f \in \mathcal{I}_3$. Comme C a 8 sommets et pour chaque sommet on a $3! = 6$ choix de repères, $[G : 1] = 8 \times 6 = 48$.

Quitte à changer l'unité de longueur, on peut supposer que les arêtes de C ont pour longueur 2. Choisissons un repère orthonormé de $\mathcal{E}_3$, tel que C soit la boule unité pour la norme $||\overrightarrow{x}||_\infty = \sup(|x_1|, |x_2|, |x_3|)$. Les éléments de G sont les applications affines qui sont isométriques pour la norme euclidienne et isométriques pour la norme $||\cdot||_\infty$. La norme duale de $||\cdot||_\infty$ est $||\cdot||_1$ et celle de la norme euclidienne $||\cdot||_2$ est $||\cdot||_2$. La boule unité Ω de $(\mathbb{R}^3, ||\cdot||_1)$ est un octaèdre régulier (voir 7-6, ex.). Par la transposition $g \mapsto {}^tg$, les applications affines conservant Ω correspondent à celles qui conservent C. Elles constituent un groupe isomorphe à G ($g \mapsto ({}^tg)^{-1}$ est un isomorphisme).

8.4 Symétries orthogonales

Lemme.

Soit E un espace vectoriel euclidien, $v \in \mathcal{L}(E)$ tel que $v^2 = Id_E$. Les conditions suivantes sont équivalentes.

(i) *v est un endomorphisme orthogonal,*

(ii) $v^* = v$,

(iii) $E = E_1 \oplus E_{-1}$ *somme directe orthogonale.*

Démonstration. L'endomorphisme v est annulé par le polynôme simple $X^2 - 1 = (X-1)(X+1)$. Donc E est somme directe des sous-espaces propres $E_1 = \mathrm{Ker}\,(v - \mathrm{Id}_E)$ et $E_{-1} = \mathrm{Ker}\,(v + \mathrm{Id}_E)$ de v (voir (1) en 8-2) et v est la symétrie vectorielle par rapport à E_1 parallèlement à E_{-1}.

(i) $\Leftrightarrow$ (ii) $\quad v \in O(n) \quad \Leftrightarrow \quad v^*v = \mathrm{Id}_E \quad \Leftrightarrow \quad v^* = v \quad$ (car $v^2 = \mathrm{Id}_E$).

(ii) $\Rightarrow$ (iii) En effet, les sous-espaces propres d'un endomorphisme symétrique sont deux à deux orthogonaux de somme directe E (ce résultat classique sera revu en 13-2).

(iii) $\Rightarrow$ (i) Supposons $E_1 \perp E_{-1}$. En utilisant le th. de Pythagore, on voit immédiatement que v est une isométrie et donc élément de $O(E)$. ∎

Soient $\mathcal{E}$ un espace affine de dimension finie n et s une symétrie, c'est à dire une application affine telle que $s^2 = \mathrm{Id}_\mathcal{E}$. Pour tout $M \in \mathcal{E}$, en posant $M' = s(M)$, on a $s(M') = M$. L'isobarycentre A de M et M' est donc invariant par s. D'après 6-8, cor. 2, $\mathcal{E}_1 = \{M \in \mathcal{E} \mid s(M) = M\}$ est le sous-espace affine de $\mathcal{E}$ contenant A, de direction $E_1 = \{\overrightarrow{x} \in E \mid v_s(\overrightarrow{x}) = \overrightarrow{x}\}$. L'image de $M = A + \overrightarrow{AM}$ est $s(M) = A + v_s(\overrightarrow{AM})$. On a $v_s^2 = v_{s^2} = \mathrm{Id}_E$. Si $E_1 = E$, on voit que $v_s = \mathrm{Id}_E$ et $s = \mathrm{Id}_\mathcal{E}$ car s a des points fixes. Si $E_{-1} = E$, on a $v_s = -\mathrm{Id}_E$ et l'ensemble $\mathcal{E}_1$ des points fixes, de direction $E_1 = \{\overrightarrow{0}\}$, est réduit au point A. Alors s est la symétrie par rapport au point A.

Définitions.

Soit $\mathcal{E}$ un espace affine de dimension finie n. Une symétrie s est appelée symétrie hyperplane si $\mathcal{E}_1$ est un hyperplan de $\mathcal{E}$, c'est-à-dire si $\dim(\mathcal{E}_1) = \dim(E_1) = n-1$.

Si $\mathcal{E}$ est euclidien, la symétrie s est dite orthogonale si les sous-espaces propres E_1 et E_{-1} sont orthogonaux entre eux.

Proposition.

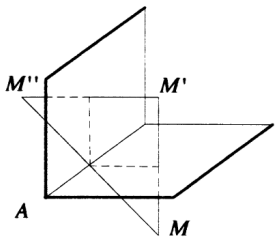
Soient $\mathcal{E}$ un espace affine euclidien de dimension n et $\mathcal{F}$ un sous-espace affine de dimension k de $\mathcal{E}$. Il existe une symétrie orthogonale $s_{\mathcal{F}}$, unique, dont l'ensemble des points fixes est $\mathcal{F}$. Elle est produit de $n-k$ symétries hyperplanes orthogonales deux à deux permutables. Elle est directe si et seulement si $n-k$ est pair.

Démonstration. Si $s = s_{\mathcal{F}}$ existe, le sous-espace propre E_1 de v_s est la direction F de $\mathcal{F}$ et $E_{-1} = E_1^{\perp} = F^{\perp}$. Cela détermine v_s et donc s de manière unique.

Pour montrer l'existence de s, choisissons $A \in \mathcal{F}$, une base orthonormée $(\overrightarrow{e_1}, \dots, \overrightarrow{e_k})$ de F, une base orthonormée $(\overrightarrow{e_{k+1}}, \dots, \overrightarrow{e_n})$ de $F^{\perp}$. Alors $\mathcal{B} = (\overrightarrow{e_1}, \dots, \overrightarrow{e_n})$ et $\mathcal{B}' = (\overrightarrow{e_1}, \dots, \overrightarrow{e_k}, -\overrightarrow{e_{k+1}}, \dots, -\overrightarrow{e_n})$ sont des bases orthonormées de E. D'après 8-3, cor. 1, il existe une application affine isométrique unique s telle que $s(A) = A$ et

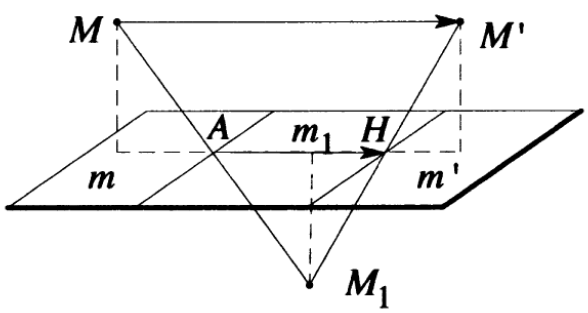
(1) $v_s(\overrightarrow{e_i}) = \overrightarrow{e_i}$ pour $i = 1, \dots, k$, $v_s(\overrightarrow{e_j}) = -\overrightarrow{e_j}$ pour $j = k+1, \dots, n$.

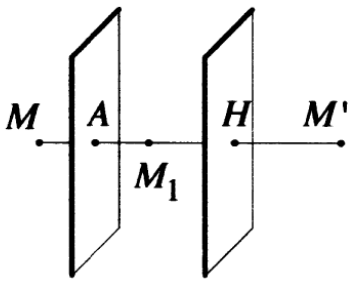
On a $s^2 = \mathrm{Id}_{\mathcal{E}}$. D'après le lemme, s est une symétrie orthogonale et $\mathcal{F}$ est l'ensemble de ses points fixes. Dans la base $\mathcal{B}$ de E, la matrice de $v_s = v$ est produit de $n-k$ matrices diagonales, dont les termes diagonaux sont égaux à 1 sauf l'un d'eux égal à -1. Ces matrices commutent deux à deux et ont pour déterminant -1, d'où la proposition.
(La figure est faite dans $\mathcal{E}_3$, avec $\dim(\mathcal{F}) = 1$.) ∎



Corollaire.

Soient $\mathcal{F}, \mathcal{F}'$ deux sous-espaces affines de $\mathcal{E}$, de même direction $F \subset E$. Alors $s_{\mathcal{F}'} \circ s_{\mathcal{F}}$ est la translation $t_{2\vec{a}}$, où $\overrightarrow{a} \in F^{\perp}$ est tel que $t_{\vec{a}}(\mathcal{F}) = \mathcal{F}'$.





Démonstration. Considérons des bases orthonormées $(\overrightarrow{e_1}, \dots, \overrightarrow{e_k})$ et $(\overrightarrow{e_{k+1}}, \dots, \overrightarrow{e_n})$ de F et de $F^{\perp}$ et $A \in \mathcal{F}$. Posons $s = s_{\mathcal{F}}$ et $s' = s_{\mathcal{F}'}$. L'expression de $v_s = v_{s'}$ dans la base $(\overrightarrow{e_1}, \dots, \overrightarrow{e_n})$ de E, est donnée par (1) ci-dessus. On a $v_{s' \circ s} = v_{s'} \circ v_s = \mathrm{Id}_E$ donc $s' \circ s$ est une translation $t_{\vec{x}}$. On a $s'(s(A)) = s'(A) = A + 2\overrightarrow{AH}$, où H est la projection orthogonale de A sur $\mathcal{F}'$. Ainsi, $\overrightarrow{x} = 2\overrightarrow{AH} \in F^{\perp}$. Posons $\overrightarrow{a} = \overrightarrow{AH}$. Alors $t_{\vec{a}}(\mathcal{F})$ est le sous-espace affine de $\mathcal{E}$ issu de H, de direction F car l'application linéaire associée à $t_{\vec{a}}$ est Id_E, c'est-à-dire $\mathcal{F}'$. (figures dans $\mathcal{E}_3$ avec $\dim(\mathcal{F}) = 0, 1$ ou 2.) ∎

8.5 Symétries glissées

Proposition.

Soient $\mathcal{E}$ un espace affine euclidien, f une application affine isométrique de $\mathcal{E}$ dans $\mathcal{E}$. Les conditions suivantes sont équivalentes.

(i) $v_f^* = v_f$.

(ii) $v_f^2 = Id_E$.

(iii) *Il existe* $\overrightarrow{a} \in E$ *et une symétrie orthogonale* s, *tels que* $f = t_{\vec{a}} \circ s$.

(iv) *Il existe un sous-espace affine* $\mathcal{F}$ *de* $\mathcal{E}$ *et* $\overrightarrow{b} \in F$, *où* F *est la direction de* $\mathcal{F}$, *tels que* $f = t_{\vec{b}} \circ s_{\mathcal{F}}$.

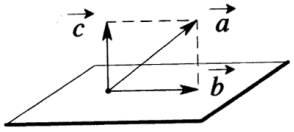
De plus, avec la propriété (iv), $\mathcal{F}$ *et* $\overrightarrow{b} \in F$ *sont uniques et donnent la seule expression de* f *comme produit* $t_{\vec{b}} \circ s_{\mathcal{F}}$ *avec* $t_{\vec{b}}$ *et* $s_{\mathcal{F}}$ *qui commutent.*

Démonstration. (i) $\Leftrightarrow$ (ii) car f étant une isométrie, on a $v_f^* v_f = \mathrm{Id}_E$.

(iv) $\Rightarrow$ (i) Si $f = t_{\vec{b}} \circ s_{\mathcal{F}}$, alors $v_f = v_{s_{\mathcal{F}}}$, d'où l'implication.

(i) $\Rightarrow$ (iii) Si $v_f^* = v_f$ alors $E = E_1 \oplus E_{-1}$, somme directe orthogonale des sous-espaces propres de v_f. Choisissons un sous-espace affine $\mathcal{F}$ de $\mathcal{E}$ de direction E_1. Soit s la symétrie orthogonale par rapport à $\mathcal{F}$. D'après 8-4, on a $v_s = v_f$ et donc $v_{f\circ s} = v_f \circ v_s = v_s^2 = \mathrm{Id}_E$. Il existe donc $\overrightarrow{a} \in E$ tel que $f \circ s = t_{\vec{a}}$, soit $f = t_{\vec{a}} \circ s$.

(iii) $\Rightarrow$ (iv) Si $f = t_{\vec{a}} \circ s$, où $s = s_{\mathcal{F}_0}$, on a $v_f = v_s$ et $E = F \oplus F^\perp$, où F est la direction de $\mathcal{F}_0$. Il existe $\overrightarrow{b} \in F$ et $\overrightarrow{c} \in F^\perp$ uniques tels que $\overrightarrow{a} = \overrightarrow{b} + \overrightarrow{c}$. Considérons le sous-espace affine $\mathcal{F} = t_{\frac{1}{2}\vec{c}}(\mathcal{F}_0)$. Il a la même direction que $\mathcal{F}_0$. D'après 8-4, cor., on a $t_{\vec{c}} = s_{\mathcal{F}} \circ s_{\mathcal{F}_0}$ et donc $f = t_{\vec{b}} \circ t_{\vec{c}} \circ s_{\mathcal{F}_0} = t_{\vec{b}} \circ s_{\mathcal{F}}$, avec $\overrightarrow{b} \in F$. Alors, $f = t_{\vec{b}} \circ s_{\mathcal{F}}$ et $s_{\mathcal{F}} \circ t_{\vec{b}}$ ont la même application linéaire associée $v_f = v_{s_{\mathcal{F}}}$. Pour $A \in \mathcal{F}$, on a $t_{\vec{b}}(A) \in \mathcal{F}$ et donc $t_{\vec{b}} \circ s_{\mathcal{F}}(A) = t_{\vec{b}}(A) = s_{\mathcal{F}} \circ t_{\vec{b}}(A)$. Il en résulte que $t_{\vec{b}} \circ s_{\mathcal{F}} = s_{\mathcal{F}} \circ t_{\vec{b}}$.



Soit $f = t_{\vec{b}'} \circ s_{\mathcal{F}'}$ une autre expression de f où $t_{\vec{b}'}$ et $s_{\mathcal{F}'}$ commutent. Alors $s_{\mathcal{F}}$ et $s_{\mathcal{F}'}$ ont v_f pour application linéaire associée. Ainsi, $\mathcal{F}$ et $\mathcal{F}'$ ont F pour direction. Pour tout $M \in \mathcal{F}'$, on a
$M + \overrightarrow{b'} = (t_{\vec{b}'} \circ s_{\mathcal{F}'})(M) = f(M) = s_{\mathcal{F}'}(M + \overrightarrow{b'}) = M + v_f(\overrightarrow{b'})$
donc $\overrightarrow{b'} \in \mathrm{Ker}\,(v_f - \mathrm{Id}_F) = F$. On a $t_{-\vec{b}'} \circ t_{\vec{b}} = s_{\mathcal{F}'} \circ s_{\mathcal{F}} = t_{2\vec{x}}$ où $\overrightarrow{x}$ donne la "perpendiculaire commune" à $\mathcal{F}$ et $\mathcal{F}'$ (voir cor. 8-4). Ainsi on a $\overrightarrow{b} - \overrightarrow{b'} \in F$ et $\overrightarrow{b} - \overrightarrow{b'} = 2\overrightarrow{x} \in F^\perp$ et donc $\overrightarrow{b} - \overrightarrow{b'} = \overrightarrow{0}$ et $s_{\mathcal{F}'} = s_{\mathcal{F}}$.

On en déduit que l'expression $f = t_{\vec{b}} \circ s_{\mathcal{F}}$, avec $\overrightarrow{b} \in F$, est unique puisque dans ce cas $t_{\vec{b}}$ et $s_{\mathcal{F}}$ commutent. ∎

Définition.

On appelle symétrie glissée toute composée $f = t_{\vec{a}} \circ s_{\mathcal{F}}$ *d'une symétrie orthogonale et d'une translation* $t_{\vec{a}}$.

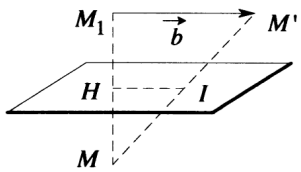
L'unique expression de f *caractérisée par (iv) s'appelle la forme canonique de* f.

Remarques.

a) Nous avons vu au cours de la démonstration que dans la forme réduite $f = t_{\vec{b}} \circ s$ de la symétrie glissée f, le vecteur $\overrightarrow{b}$ est propre pour v_f avec la valeur propre 1.

b) d'après 8-4, prop., $f = t_{\vec{a}} \circ s_{\mathcal{F}}$ est directe si et seulement si $n - \dim(\mathcal{F})$ est pair.

c) Pour déterminer les éléments $\mathcal{F}$ et $\overrightarrow{b}$ de la forme réduite de f, on notera que la direction de $\mathcal{F}$ est le sous-espace propre E_1 de v_f et que pour tout $M \in \mathcal{E}$, si on pose $M' = f(M)$, le milieu I du segment $[MM']$ appartient à $\mathcal{F}$ car $\overrightarrow{HI} = \frac{1}{2}\overrightarrow{b} \in E_1$.



De plus, $\overrightarrow{b} = \overrightarrow{II'}$, où $I' = f(I)$ car
$f(I) = t_{\vec{b}}(s_{\mathcal{F}}(I)) = I + \overrightarrow{b}$.

Exercice. Dans l'espace affine euclidien $\mathcal{E}_3$, muni d'un repère orthonormé $(O, \overrightarrow{\imath}, \overrightarrow{\jmath}, \overrightarrow{k})$, étudier l'application f associant au point $M(x,y,z)$ le point $M'(x',y',z')$ où

$$\begin{cases} x' &= & & - \frac{\sqrt{2}}{2} y & - \frac{\sqrt{2}}{2} z \\ y' &= -\frac{\sqrt{2}}{2} x & - \frac{1}{2} y & + \frac{1}{2} z & + 2 \\ z' &= -\frac{\sqrt{2}}{2} x & + \frac{1}{2} y & - \frac{1}{2} z & - 1 \end{cases}$$

Solution. On a $M' = B + v(\overrightarrow{OM})$, où $B(0,2,-1)$ et v désigne l'endomorphisme de $\mathbb{R}^3$ admettant dans la base $\mathcal{B} = (\overrightarrow{\imath}, \overrightarrow{\jmath}, \overrightarrow{k})$, la matrice A du système ci dessus. D'après 6-4, cor. 3 f est affine et l'application linéaire associée est v.

La matrice A est orthogonale et symétrique. Donc f est une symétrie glissée. Il existe une base orthonormée $\mathcal{B}'$ de E dans laquelle la matrice de v est diagonale. Ses valeurs propres sont 1 ou -1. Comme $\text{tr}\,(v) = \text{tr}\,(A) = -1$, deux valeurs propres sont égales à -1, la troisième est 1. Ainsi f est directe : c'est un déplacement. Ici E_1 est une droite vectorielle. Le calcul montre que $\overrightarrow{w} = -\sqrt{2}\,\overrightarrow{\imath} + \overrightarrow{\jmath} + \overrightarrow{k} \in E_1$. Pour $M = O$, on a $f(M) = B$ donc le milieu $I(0,1,-\frac{1}{2})$ de $[OB]$ appartient à $\mathcal{F}$. Dans l'expression canonique $f = t_{\vec{a}} \circ s_{\mathcal{F}}$ de f, le sous-espace affine $\mathcal{F}$ est la droite issue de I de vecteur directeur $\overrightarrow{w}$. Le vecteur $\overrightarrow{a}$ de la translation $t_{\vec{a}}$ est $\overrightarrow{II'} = \frac{1}{4}\overrightarrow{w} \in E_1$.

8.6 Isométries produits de symétries hyperplanes

Soient $\mathcal{E}$ un espace affine euclidien, E sa direction. Soient $A, B \in \mathcal{E}$, avec $A \neq B$, et $I = \text{bar}\,((A, \frac{1}{2}), (B, \frac{1}{2}))$. Un point $M \in \mathcal{E}$ est à égale distance de A et de B, si

$$0 \;=\; MB^2 - MA^2 \;=\; (\overrightarrow{MB} + \overrightarrow{MA} \,|\, \overrightarrow{MB} - \overrightarrow{MA}) \;=\; (2\overrightarrow{MI} \,|\, \overrightarrow{AB}),$$

L'ensemble $\mathcal{H}$ des points M tels que $MA = MB$ est l'hyperplan $\mathcal{H}$ issu du milieu I de $[AB]$, de direction H orthogonale au vecteur $\overrightarrow{AB} \in E$. On l'appelle *l'hyperplan médiateur* du segment $[AB]$. La symétrie hyperplane orthogonale $s_{\mathcal{H}}$ applique A sur B et c'est la seule.

Lemme.

Considérons un espace affine euclidien $\mathcal{E}$ de dimension n, un repère affine $\mathcal{R} = \{A_0, \ldots, A_n\}$ de $\mathcal{E}$ et $M \in \mathcal{E}$. Si $M' \in \mathcal{E}$ est à la même distance que M de chacun des points A_i de $\mathcal{R}$, alors $M' = M$.

Démonstration. Si on avait $M' \neq M$, alors l'hyperplan médiateur $\mathcal{H}$ de $[MM']$ contiendrait tous les points A_i du repère $\mathcal{R}$. C'est absurde car $\mathcal{R}$ engendre $\mathcal{E}$ et $\dim(\mathcal{H}) = n-1$. ∎

Proposition.

Considérons un espace affine euclidien $\mathcal{E}$ de dimension n, un repère affine $R = \{A_0, \ldots, A_n\}$ de $\mathcal{E}$ et des points $A'_0, \ldots, A'_n$ de $\mathcal{E}$ tels que $A'_iA'_j = A_iA_j$ pour tous $0 \leqslant i < j \leqslant n$. Il existe une isométrie unique f de $\mathcal{E}$ dans $\mathcal{E}$ telle que $f(A_i) = A'_i$ pour $i = 0, \ldots, n$ et f est affine, produit de symétries hyperplanes orthogonales.

Démonstration. Si $A_0 = A'_0$, posons $f_1 = \mathrm{Id}_{\mathcal{E}}$. Si $A_0 \neq A'_0$, soit s_1 la symétrie orthogonale par rapport à l'hyperplan médiateur du segment $[A_0\,A'_0]$ et posons $f_1 = s_1$. Ainsi définie, f_1 est une isométrie affine telle que $f_1(A_0) = A'_0$. La distance de $f_1(A_1)$ à $f_1(A_0) = A'_0$ est égale à $A_0A_1 = A'_0A'_1$.

Si $f_1(A_1) = A'_1$, posons $f_2 = f_1$. Si $f_1(A_1) \neq A'_1$, soit s_2 la symétrie orthogonale par rapport à l'hyperplan médiateur $\mathcal{H}$ de $[f_1(A_1)\,A'_1]$ et posons $f_2 = s_2 \circ f_1$. Comme $\mathcal{H}$ passe par A'_0, ainsi définie, f_2 est telle que $f_2(A_0) = A'_0$ et $f_2(A_1) = A'_1$.

En continuant ainsi, on construit par récurrence une isométrie f produit de symétries hyperplanes orthogonales, telle que $f(A_i) = A'_i$ pour $i = 0, \ldots, n$.

Soit g est une isométrie de $\mathcal{E}$ dans $\mathcal{E}$ telle que $g(A_i) = A'_i$ pour $i = 0, \ldots, n$. Alors $h = f^{-1} \circ g$ laisse fixe $A_0, \ldots, A_n$. Tout $M \in \mathcal{E}$, est à la même distance de $A_0, \ldots, A_n$ que $M' = h(M)$. D'après le lemme, on a $M' = M$ et donc $h = \mathrm{Id}_{\mathcal{E}}$. Ainsi, $g = f$ et f est unique. Elle est affine, produit de symétries hyperplanes orthogonales. ∎

Corollaire.

Soit $\mathcal{E}$ un espace affine euclidien de dimension n. Toute application isométrique f de $\mathcal{E}$ dans $\mathcal{E}$ est affine et elle est produit de symétries hyperplanes orthogonales.

Démonstration. Considérons un repère affine $R = \{A_0, \ldots, A_n\}$ de $\mathcal{E}$, et les points $A'_0 = f(A_0), \ldots, A'_n = f(A_n)$. D'après la proposition, il existe un produit de symétries hyperplanes orthogonales g tel que $g(A_0) = A'_0, \ldots, g(A_n) = A'_n$ et l'unicité dans la proposition montre que $f = g$. Comme g est affine, f est affine. ∎

Exercice. Dans le plan euclidien $\mathcal{E}_2$, on considère deux triangles (non aplatis) ABC et $A'B'C'$. Montrer que dans les cas suivants ces triangles sont isométriques :
- $AB = A'B'$, $BC = B'C'$, $CA = C'A'$,
- $AB = A'B'$, $AC = A'C'$, $\widehat{A} = \widehat{A'}$,
- $BC = B'C'$, $\widehat{B} = \widehat{B'}$, $\widehat{C} = \widehat{C'}$.

Solution. Dans le premier cas, la proposition donne directement le résultat. Dans le second cas, la relation $BC^2 = AB^2 + AC^2 - 2AB\,AC\cos(\widehat{A})$, obtenue en développant $||\overrightarrow{BC}||^2 = ||\overrightarrow{BA} + \overrightarrow{AC}||^2$, montre que $BC = B'C'$. On est ramené au premier cas. Dans le troisième cas, des relations $\dfrac{\sin\widehat{A}}{BC} = \dfrac{\sin\widehat{B}}{CA} = \dfrac{\sin\widehat{C}}{AB}$ et $\widehat{A} + \widehat{B} + \widehat{C} = \pi$, on déduit $CA = C'A'$, $AB = A'B'$. On est ramené au premier cas.

8.7 Groupe des isométries de $\mathcal{E}_n$

Proposition.

Muni de l'opération de composition des applications, l'ensemble $\mathcal{I}$ des isométries de l'espace affine euclidien $\mathcal{E}_n$ de dimension n, est un groupe isomorphe au produit semi-direct $\mathbb{R}^n \times_\varphi O(n)$ où φ est l'action naturelle $(u, \overrightarrow{x}) \mapsto u(\overrightarrow{x})$ du groupe orthogonal $O(n)$ sur $\mathbb{R}^n$.

Démonstration. Toute isométrie de $\mathcal{E}_n$ dans $\mathcal{E}_n$ est affine d'après 8-6 et injective. Elle est donc bijective d'après 6-3, prop. 1. On a donc $\mathcal{I} \subset \mathrm{Aut}(\mathcal{E}_n)$. Par ailleurs, $f \in \mathrm{Aut}(\mathcal{E}_n)$ est une isométrie si et seulement si v_f est une isométrie, c'est-à-dire élément de $O(n)$. Donc $\mathcal{I}$ est l'image réciproque dans $\mathrm{Aut}(\mathcal{E}_n)$ du sous-groupe $O(n)$ de $\mathrm{GL}(n,\mathbb{R})$ par l'homomorphisme de groupes $\nu : f \mapsto v_f$. C'est donc un sous-groupe de $\mathrm{Aut}(\mathcal{E}_n)$. Il contient le sous-groupe distingué T de G constitué des translations. D'après 6-9, $\mathrm{Aut}(\mathcal{E}_n)$ est le produit semi-direct de $\mathbb{R}^n$ par $\mathrm{GL}(n,\mathbb{R})$ associé à l'action naturelle φ de $\mathrm{GL}(n,\mathbb{R})$ sur $\mathbb{R}^n$. Le stabilisateur d'un point $A \in \mathcal{E}_n$ dans $\mathcal{I}$ étant isomorphe à $O(n)$, le lemme 6-10 donne le résultat. ∎

Corollaire.

L'ensemble $\mathcal{I}^+$ des isométries directes de $\mathcal{E}_n$ est un sous-groupe distingué de $\mathcal{I}$. Il est isomorphe au produit semi-direct $\mathbb{R}^n \times_\varphi O^+(n)$, où $O^+(n)$ est l'ensemble des endomorphismes orthogonaux directs de $\mathbb{R}^n$ et φ l'action naturelle $(u, \overrightarrow{x}) \mapsto u(\overrightarrow{x})$ de $O^+(n)$ sur $\mathbb{R}^n$.

Démonstration. $u \in \mathcal{L}(E)$ est orthogonal si et seulement si ${}^t u u = \mathrm{Id}_E$. De ce fait,

$$(\det(u))^2 = \det({}^t u)\det(u) = \det({}^t u\, u) = \det(\mathrm{Id}_E) = 1 \quad \text{donc} \quad \det(u) = \pm 1.$$

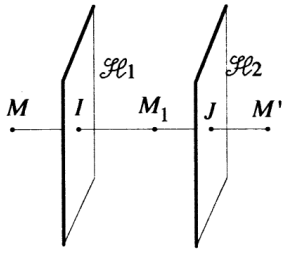
L'application $v \mapsto \det(v)$ est un homomorphisme de groupes de $\mathrm{GL}(E)$ sur $\mathbb{R}^*$. Pour $v \in O(n)$, on a $\det(v) \in \{1,-1\}$. Donc $f \mapsto \det(v_f)$ est un homomorphisme de groupes de $\mathcal{I}$ sur $\{1,-1\}$. Son noyau $\mathcal{I}^+ = \{f \in \mathcal{I} \mid \det(v_f) = 1\}$ est donc un sous-groupe distingué de $\mathcal{I}$. Comme dans la proposition, le lemme 6-10 donne le résultat. ∎

Définition.

Les éléments de $\mathcal{I}^+$ sont appelés des déplacements. Ce sont les éléments f de $\mathcal{I}$ tels que $\det(v_f) = 1$, c'est-à-dire ceux qui conservent l'orientation de $\mathcal{E}_n$.
Si $\det(v_f) = -1$, on dit que $f \in \mathcal{I}$ est un antidéplacement.

Parmi les antidéplacements figurent les symétries orthogonales hyperplanes et plus généralement les isométries qui sont produit d'un nombre impair de telles symétries. Les déplacements sont produit d'un nombre pair de symétries hyperplanes orthogonales.

Toute translation $t_{\vec{a}}$ est un déplacement car l'application linéaire associée est Id_E, de déterminant 1. D'ailleurs, on peut (d'après 8-4, cor.), décomposer $t_{\vec{a}}$ en produit $s_{\mathcal{H}_2} \circ s_{\mathcal{H}_1}$ de deux symétries hyperplanes orthogonales, où $\mathcal{H}_1$ peut être choisi arbitrairement parmi les hyperplans perpendiculaires au vecteur $\overrightarrow{a}$ et où $\mathcal{H}_2$ se déduit de $\mathcal{H}_1$ par la translation de vecteur $\overrightarrow{IJ} = \frac{1}{2}\overrightarrow{a}$.



8.8 Décomposition canonique d'une isométrie

Lemme.

Soient E un espace vectoriel euclidien et $v \in O(E)$. Alors
$\mathrm{Ker}\,(v - Id_E) = [\mathrm{Im}\,(v - Id_E)]^\perp$.

Démonstration. Soient $\overrightarrow{x} \in \mathrm{Ker}\,(v - \mathrm{Id}_E)$ et $\overrightarrow{y} \in \mathrm{Im}\,(v - \mathrm{Id}_E)$. Il existe $\overrightarrow{z} \in E$ tel que $\overrightarrow{y} = v(\overrightarrow{z}) - \overrightarrow{z}$. Utilisons le fait que $v^* = v^{-1}$ car v orthogonale et que v^{-1} laisse $\overrightarrow{x}$ fixe. On a :

$$\begin{aligned}(\overrightarrow{x} \mid \overrightarrow{y}) &= (\overrightarrow{x} \mid v(\overrightarrow{z}) - \overrightarrow{z}) = (\overrightarrow{x} \mid v(\overrightarrow{z})) - (\overrightarrow{x} \mid \overrightarrow{z}) \\ &= (v^{-1}(\overrightarrow{x}) \mid \overrightarrow{z}) - (\overrightarrow{x} \mid \overrightarrow{z}) = (\overrightarrow{x} \mid \overrightarrow{z}) - (\overrightarrow{x} \mid \overrightarrow{z}) = 0,\end{aligned}$$

et donc $\mathrm{Ker}\,(v - \mathrm{Id}_E) \subset [\mathrm{Im}\,(v - \mathrm{Id}_E)]^\perp$. Cette inclusion est une égalité car d'après le th. du rang, $\dim(\mathrm{Ker}\,(v - \mathrm{Id}_E)) = n - \dim(\mathrm{Im}\,(v - \mathrm{Id}_E)) = \dim([\mathrm{Im}\,(v - \mathrm{Id}_E)]^\perp)$. ∎

Proposition.

Soit f une isométrie de l'espace affine euclidien $\mathcal{E}_n$. Notons E l'espace vectoriel euclidien, direction de $\mathcal{E}_n$. Il existe une isométrie g de $\mathcal{E}_n$ admettant un point fixe et un vecteur $\overrightarrow{x} \in Ker\,(v_f - Id)$, uniques, tels que $f = t_{\vec{x}} \circ g$. C'est la seule expression $f = t_{\vec{x}} \circ g$ où $g \in Aut\,(\mathcal{E}_n)$ a un point fixe et commute avec $t_{\vec{x}}$.

Démonstration. Soient $A \in \mathcal{E}_n$ et $A' = f(A)$. Posons $\overrightarrow{a} = \overrightarrow{AA'}$. D'après le lemme, il existe $\overrightarrow{x} \in \mathrm{Ker}\,(v_f - \mathrm{Id}_E)$ et $\overrightarrow{y} \in \mathrm{Im}\,(v_f - \mathrm{Id}_E)$ tels que $\overrightarrow{a} = \overrightarrow{x} + \overrightarrow{y}$. Soit $\overrightarrow{z} \in E$ tel que $\overrightarrow{y} = v_f(\overrightarrow{z}) - \overrightarrow{z}$. Vérifions que $B = A + (-\overrightarrow{z})$ est fixe par $g = t_{-\vec{x}} \circ f$.

$$\begin{aligned}g(B) &= f(B) + (-\overrightarrow{x}) = f(A + (-\overrightarrow{z})) + (-\overrightarrow{x}) = f(A) + [-v_f(\overrightarrow{z}) - \overrightarrow{x}] \\ &= A + [\overrightarrow{a} - v_f(\overrightarrow{z}) - \overrightarrow{x}] = A + [\overrightarrow{y} - v_f(\overrightarrow{z})] = A + (-\overrightarrow{z}) = B.\end{aligned}$$

Montrons l'unicité de cette décomposition $f = t_{\vec{x}} \circ g$. Soit $f = t_{\vec{x}'} \circ g'$ une autre expression, où g' admet un point fixe B' et où $\overrightarrow{x'} \in \mathrm{Ker}\,(v_f - \mathrm{Id}_E)$. Puisque $f(B') = B' + \overrightarrow{x'}$ et $f(B) = B + \overrightarrow{x}$, on a $v_f(\overrightarrow{BB'}) = \overrightarrow{BB'} + \overrightarrow{x'} - \overrightarrow{x}$. Cela montre que $\overrightarrow{x'} - \overrightarrow{x} \in \mathrm{Im}\,(v_f - \mathrm{Id}_E)$. On a aussi $\overrightarrow{x'} - \overrightarrow{x} \in \mathrm{Ker}\,(v_f - \mathrm{Id}_E)$ et donc $\overrightarrow{x'} - \overrightarrow{x} = \overrightarrow{0}$ d'après le lemme. Ensuite, la relation $f = t_{\vec{x}} \circ g = t_{\vec{x}'} \circ g'$ donne $g = g'$.

Pour tout $M \in \mathcal{E}_n$, en tenant compte du fait que $\overrightarrow{x}$ est fixe par $v_f = v_g$, on a

$$g \circ t_{\vec{x}}(M) = g(M + \overrightarrow{x}) = g(M) + v_g(\overrightarrow{x}) = g(M) + \overrightarrow{x} = (t_{\vec{x}} \circ g)(M).$$

Cela prouve que $t_{\vec{x}}$ et g commutent.

Réciproquement, si $f = t_{\vec{x}} \circ g$, où g a un point fixe B et où $t_{\vec{x}}$ et g commutent,

$$\begin{aligned}B + \overrightarrow{x} &= g(B) + \overrightarrow{x} = (t_{\vec{x}} \circ g)(B) = (g \circ t_{\vec{x}})(B) \\ &= g(B + \overrightarrow{x}) = g(B) + v_g(\overrightarrow{x}) = B + v_g(\overrightarrow{x}).\end{aligned}$$

On voit que $v_f(\overrightarrow{x}) = \overrightarrow{x}$. L'unicité déjà démontrée, concernant cette propriété, montre que $f = t_{\vec{x}} \circ g$ est la décomposition précédente. ∎

Définition.

Cette unique expression $f = t_{\vec{x}} \circ g$ de l'isométrie f de $\mathcal{E}_n$, où g a un point fixe et où $t_{\vec{x}}$ et g commutent, est appelée la forme canonique de f.

Comme g a un point fixe B, son étude se ramène à celle de $v_g = v_f$ qui est orthogonal. D'après 8-2, il existe une base orthonormée $(\overrightarrow{e_1}, \ldots, \overrightarrow{e_n})$ dans laquelle la matrice M_g de v_g est diagonale par blocs, avec des blocs de dimension un, égaux à 1 ou -1 et des blocs de dimension deux qui sont des matrices de rotation non diagonalisables.

D'après 6-8, cor.3, f a un point fixe unique si et seulement si $\mathrm{Ker}\,(v_f - \mathrm{Id}_E) = \{\overrightarrow{0}\}$. Cela est confirmé par la proposition précédente : si $\mathrm{Ker}\,(v_f - \mathrm{Id}_E) = \{\overrightarrow{0}\}$, dans la décomposition canonique on aura $\overrightarrow{x} = \overrightarrow{0}$ et $f = g$ aura un point fixe, unique car la direction du sous-espace des points fixes est justement $\mathrm{Ker}\,(v_f - \mathrm{Id}_E)$.

Notons encore que toute conjuguée $f' = h \circ f \circ h^{-1}$ de f, où $h \in \mathcal{I}$, sera de "même nature" que f : sa forme canonique sera $f' = t_{v_h(\vec{x})} \circ g'$, où $g' = h \circ g \circ h^{-1}$ admet $h(B)$ pour point fixe et où $v_{g'}$ admet dans la base orthonormée $(v_h(\overrightarrow{e_1}), \ldots, v_h(\overrightarrow{e_n}))$, la même matrice M_g que v_g relativement à la base $(\overrightarrow{e_1}, \ldots, \overrightarrow{e_n})$.

Exercice. Soit f une isométrie de l'espace euclidien $\mathcal{E}_n$. Supposons que f^n, où $n \geqslant 2$, ait un point fixe. Montrer que f a un point fixe.

Solution. Utilisons la décomposition canonique $f = t_{\vec{a}} \circ g$. Notons d'abord que si une isométrie f a un point fixe, alors on a $f = t_{\vec{0}} \circ f$ avec $t_{\vec{0}} = \mathrm{Id}_E$ et f permutables. Donc $f = t_{\vec{0}} \circ f$ est la forme canonique de f.

Supposons que f^n ait un point fixe. Comme $t_{\vec{a}}$ et g commutent, on a $f^n = t_{n\vec{a}} \circ g^n$, avec $t_{n\vec{a}}$ et g^n qui commutent et g^n qui a un point fixe car g en a un. D'après l'unicité de la forme canonique de f^n et la remarque précédente, si f^n a un point fixe, alors $t_{n\vec{a}} = t_{\vec{0}}$ soit $n\overrightarrow{a} = \overrightarrow{0}$. Ainsi $\overrightarrow{a} = \overrightarrow{0}$ et $f = g$ a un point fixe.

Autre démonstration, plus générale, valable pour toute application affine : si A est fixe par f^n, alors $A, f(A), \ldots, f^{n-1}(A)$ sont permutés par f. L'isobarycentre de ces points est fixe par f puisque f est affine.

8.9 Classification des isométries du plan

Soit f une isométrie du plan euclidien $\mathcal{E}_2$. Soit $f = t_{\vec{x}} \circ g$ sa décomposition canonique, où g a un point fixe B et où $\overrightarrow{x} \in \mathrm{Ker}\,(v_g - \mathrm{Id}_E)$. D'après 8-2, il existe une base orthonormée $(\overrightarrow{imath}, \overrightarrow{\jmath})$ de $\mathbb{R}^2$ dans laquelle la matrice M_f de $v_f = v_g$ est diagonale par blocs, les blocs étant de format un égaux à 1 ou -1 ou de format deux et matrice d'une rotation non diagonalisable. Quitte à échanger $\overrightarrow{imath}$ et $\overrightarrow{\jmath}$, la matrice M_f de v_f est l'une des matrices

$$S = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \quad , \quad I_2 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \quad , \quad -I_2 = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} \quad , \quad M_\theta = \begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix}$$

avec $\theta \neq 0 \pmod{\pi}$. On a $\det(v_f) = -1$ uniquement si $v_f = S$. Donc f est un déplacement dans les trois derniers cas et un antidéplacement dans le premier cas où $M_f = S$. Pour $\theta = 0$ ou $\theta = \pi$, l'expression de M_θ serait I_2 ou $-I_2$. On peut donc dire que si f est un déplacement (resp. un antidéplacement), il existe une base orthonormée de $\mathbb{R}^2$ dans laquelle la matrice de v_f est de la forme M_θ (resp. S).

1°/ *Considérons le cas où $f = t_{\vec{x}} \circ g$ est un déplacement.*

Si $M_f = I_2$, alors $v_f = \mathrm{Id}_E$ et f est une translation $t_{\vec{x}}$.

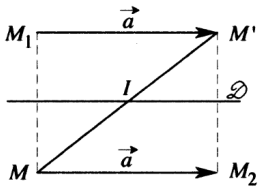
Si $M_f = -I_2$, alors $v_f = -\mathrm{Id}_E$. On a $\overrightarrow{x} \in \mathrm{Ker}\,(v_f - \mathrm{Id}_E) = \{\overrightarrow{0}\}$ et donc $\overrightarrow{x'} = \overrightarrow{0}$. Alors $f = g$ a un point fixe B. On voit que f est la rotation de centre B d'angle π, c'est-à-dire la symétrie par rapport au point B.

Si $M_f = M_\theta$ avec $\theta \neq 0 \pmod{\pi}$. On a $\mathrm{Ker}\,(v_f - \mathrm{Id}_E) = \{\overrightarrow{0}\}$ et donc $\overrightarrow{x'} = \overrightarrow{0}$. Alors $f = g$ a un point fixe B. On voit que f est la rotation de centre B d'angle θ.

Finalement, le groupe $\mathcal{I}^+$ des déplacements est constitué des translations et des rotations. D'après 8-7, c'est un produit semi-direct $\mathbb{R}^2 \times_\varphi \mathbb{U}$ où $\mathbb{U}$ désigne le groupe multiplicatif des nombres complexes $e^{i\theta}$ de module 1, agissant sur $\mathbb{R}^2 = \mathbb{C}$ par les rotations $z \mapsto e^{i\theta}z$.

2°/ *Considérons le cas où $f = t_{\vec{x}} \circ g$ est un antidéplacement.*

Comme g a un point fixe B et v_g a pour matrice S, on voit que g est la symétrie orthogonale $s_{\mathcal{D}}$ par rapport à la droite $\mathcal{D}$, issue de B de direction $D = \mathbb{R}\overrightarrow{\imath}$.
Si $\overrightarrow{x} = \overrightarrow{0}$, alors $f = g = s_{\mathcal{D}}$.
Si $\overrightarrow{x} \neq \overrightarrow{0}$, alors f, est composée de $s_{\mathcal{D}}$ et $t_{\vec{x}}$ où $\vec{x} \in D$. C'est une symétrie glissée. Il y a unicité de cette expression de f, d'après l'unicité de la décomposition canonique de f. Rappelons que pour tout $M \in \mathcal{E}_2$, la droite $\mathcal{D}$ passe par le milieu du segment $[MM']$, où $M' = f(M)$.



Proposition.

Les déplacements du plan euclidien $\mathcal{E}_2$ sont les translations et les rotations autour d'un point. Un déplacement a un point fixe si et seulement si c'est une rotation.

Les antidéplacements sont les symétries orthogonales par rapport à une droite et les symétries glissées. Pour qu'un antidéplacement ait un point fixe, il faut et il suffit que ce soit une symétrie orthogonale par rapport à une droite.

Exercice 1. Soit $n \in \mathbb{N}$, avec $n \geqslant 2$. Dans le groupe des isométries du plan affine euclidien $\mathcal{E}_2$, déterminer f telle que $f^n = r_{A,\theta}$, où $\theta \neq 0 \pmod{2\pi}$.

Solution. Puisque f^n a un point fixe, f a un point fixe (8-8, ex.). Si un point est fixe par f, il est fixe par f^n, c'est donc A. Si f est un antidéplacement c'est une symétrie s par rapport à une droite et s^n est égal a $\mathrm{Id}_{\mathcal{E}_2} \neq r_{A,\theta}$ si n est pair et à s qui n'est pas un déplacement pour n impair. Donc si le problème a des solutions, ce seront des déplacements, laissant A fixe, c'est-à-dire des rotations $r_{A,\alpha}$. La relation $r^n_{A,\alpha} = r_{A,\theta}$ équivaut à $\alpha = \frac{\theta}{n} \pmod{\frac{2\pi}{n}}$. On a donc n solutions.

Exercice 2. On identifie le plan euclidien muni d'un repère orthonormé, avec le plan complexe.

a) Montrer que le groupe $\mathcal{I}^+$ des déplacements est l'ensemble des applications $f_{a,\theta} : z \mapsto e^{i\theta}z + a$, où $a \in \mathbb{C}$ et $\theta \in [0, 2\pi[$.

b) Montrer que $\mathcal{I}^-$ est l'ensemble des applications $g_{a,\theta} : z \mapsto e^{i\theta}\,\overline{z} + a$, où $a \in \mathbb{C}$ et $\theta \in [0, 2\pi[$. Donner l'expression canonique de $g_{a,\theta}$.

Solution. **a)** Le stabilisateur $\mathcal{I}^+_O$ de l'origine (zéro de $\mathbb{C}$) dans $\mathcal{I}^+$ est l'ensemble des rotations de la forme $z \mapsto e^{i\theta}z$. Soit f un déplacement. Posons $O' = f(O)$ et $\overrightarrow{a} = \overrightarrow{OO'}$. Alors $t_{-\vec{a}} \circ f = g \in \mathcal{I}^+_O$, est de la forme $z \mapsto e^{i\theta}z$ et donc $f = t_{\vec{a}} \circ g$ a

pour expression $z \mapsto e^{i\theta}z + a$, avec a l'affixe de $\overrightarrow{a}$. Réciproquement, si f a cette expression, elle est composée de la rotation $r_{O,\theta}$ et de la translation définie par a. C'est un déplacement.

b) Soit $g \in \mathcal{I}^-$. La symétrie $s : z \mapsto \bar{z}$ est élément de $\mathcal{I}^-$ donc $f = g \circ s \in \mathcal{I}^+$ est de la forme $z \mapsto e^{i\theta}z + a$ et $g = f \circ s$ est de la forme $z \mapsto e^{i\theta}\bar{z} + a$.

Tout antidéplacement de $\mathcal{E}_2$ est une symétrie glissée. L'expression canonique de g est donc $g = t_{\vec{x}} \circ s$ où s est une symétrie orthogonale qui commute avec $t_{\vec{x}}$. On a $g \circ g = t_{2\vec{x}} \circ s^2 = t_{2\vec{x}}$ et $g(g(z)) = e^{i\theta}(\overline{e^{i\theta}\bar{z} + a}) + a = z + e^{i\theta}\bar{a} + a$ donc $\overrightarrow{x}$ a pour d'affixe $\frac{1}{2}(e^{i\theta}\bar{a} + a)$ et $s(z) = (t_{-\vec{x}} \circ g)(z) = e^{i\theta}\bar{z} + a - \frac{1}{2}e^{i\theta}\bar{a} - \frac{1}{2}a = e^{i\theta}\bar{z} + \frac{1}{2}(a - e^{i\theta}\bar{a})$. On a $g(0) = a$ donc $(\frac{1}{2}a)$ appartient à l'axe de la symétrie s. C'est un point fixe pour s. Cela se vérifie d'ailleurs sur l'expression de s et conduit directement à l'expression de s car $v_s = v_g$ est $z \mapsto e^{i\theta}\bar{z}$. L'axe de la symétrie s est la droite D issue de A d'affixe $\frac{1}{2}a$, telle que l'angle $(Ox, D) = \frac{\theta}{2} \pmod{\pi}$. Puisque $s(z) - \frac{1}{2}a = e^{i\theta}(\overline{z - \frac{1}{2}a})$, en plaçant l'origine en A, l'expression de s devient $Z \mapsto e^{i\theta}\overline{Z}$.

8.10 Classification des isométries de l'espace

Soit f un élément du groupe $\mathcal{I}_3$ des isométries de l'espace euclidien $\mathcal{E}_3$. D'après 8-2, il existe une base orthonormée $(\overrightarrow{\imath}, \overrightarrow{\jmath}, \overrightarrow{k})$ de $\mathbb{R}^3$ dans laquelle la matrice M_f de $v_f = v_g$ est diagonale par blocs, avec des blocs égaux à 1 ou -1 ou de format deux et matrice d'une rotation non diagonalisable. Quitte à permuter $\overrightarrow{\imath}, \overrightarrow{\jmath}, \overrightarrow{k}$, la matrice M_f est de l'un des types :

$$I_3 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, S = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & -1 \end{pmatrix}, S' = \begin{pmatrix} 1 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & -1 \end{pmatrix}, -I_3 = \begin{pmatrix} -1 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & -1 \end{pmatrix}$$

$$P_\theta = \begin{pmatrix} 1 & 0 & 0 \\ 0 & \cos\theta & -\sin\theta \\ 0 & \sin\theta & \cos\theta \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & M_\theta \end{pmatrix}, P'_\theta = \begin{pmatrix} -1 & 0 & 0 \\ 0 & \cos\theta & -\sin\theta \\ 0 & \sin\theta & \cos\theta \end{pmatrix} = \begin{pmatrix} -1 & 0 \\ 0 & M_\theta \end{pmatrix},$$

où $\theta \neq 0 \pmod{\pi}$. Pour $\theta = 0$, les matrices P_θ et P'_θ sont du type I_3 et S. Pour $\theta = \pi$ elles ont pour expression S' et $-I_3$. Il existe donc une base orthonormée de $\mathbb{R}^3$ dans laquelle la matrice de $v_f = v_g$ est soit P_θ lorsque $\det(v_f) = 1$, c'est-à-dire lorsque f est un déplacement, soit P'_θ lorsque $\det(v_f) = -1$, c'est-à-dire lorsque f est un antidéplacement. Les cas où la matrice est $I_3, S, S', -I_3$, correspondent aux cas particuliers où l'endomorphisme orthogonal v_f est diagonalisable, c'est-à-dire où $v_f^* = v_f$, ce qui se produit lorsque $\theta = 0$ ou $\theta = \pi$.

Remarque 1. On peut démontrer ce résultat sans s'appuyer sur la prop 8-2. On remarquera que le polynôme caractéristique de v_f est de degré 3. D'après le th. des valeurs intermédiaires, il a au moins une racine réelle. Comme v_f est isométrique, cette valeur propre de v_f est 1 ou -1. Si on choisit un vecteur propre $\overrightarrow{\imath}$, de longueur un, relatif à cette valeur propre, l'endomorphisme orthogonal v_f laisse stable le plan vectoriel V orthogonal à $\overrightarrow{\imath}$ et induit sur ce plan euclidien V une isométrie v de V. Il existe une base orthonormée $(\overrightarrow{\jmath}, \overrightarrow{k})$ de V dans laquelle la matrice de v a l'une des formes décrites en 8-9. Finalement, il existe une base orthonormée $\mathcal{B} = (\overrightarrow{\imath}, \overrightarrow{\jmath}, \overrightarrow{k})$ de $\mathbb{R}^3$ dans laquelle la matrice de v_f est de l'une des formes P_θ ou P'_θ.

Si l'espace euclidien est orienté, on supposera la base orthomormée directe, quitte à remplacer $\overrightarrow{\imath}$ par son opposé. Soit $f = t_{\vec{x}} \circ g$ sa décomposition canonique, où g a un point fixe A et où $\overrightarrow{x} \in E_1 = \mathrm{Ker}\left(v_g - \mathrm{Id}_E\right)$.

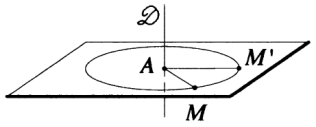
1°/ *Supposons que f soit un déplacement.*

Dans la base orthonormée $\mathcal{B}$ la matrice de v_f est P_θ.

- Si $\theta = 0 \pmod{2\pi}$, alors $v_f = \mathrm{Id}_E$ et f est une translation.

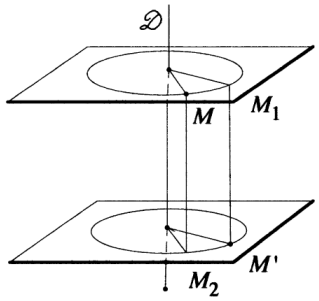
- Si $\theta \neq 0 \pmod{2\pi}$, alors E_1 est la droite vectorielle dirigée par $\overrightarrow{\imath}$. Le vecteur $\overrightarrow{x}$ de la translation $t_{\vec{x}}$ est un élément $\lambda\overrightarrow{\imath}$ de cette droite.

Si $\lambda = 0$, alors $f = g$ admet A pour point fixe et admet donc la droite $\mathcal{D} = A + \mathbb{R}\overrightarrow{\imath}$ pour ensemble de points fixes. Dans le repère orthonormé $(A, \overrightarrow{\imath}, \overrightarrow{\jmath}, \overrightarrow{k})$, on reconnaît la rotation r d'axe $\mathcal{D}$, d'angle θ.



Cas particulier : si $\theta = \pi \pmod{2\pi}$, la rotation r est aussi la symétrie orthogonale par rapport à $\mathcal{D}$. On l'appelle le *demi-tour* d'axe $\mathcal{D}$.

Si $\lambda \neq 0$, alors f est composée de la rotation g, d'axe $\mathcal{D}$ et d'angle θ et de la translation $t_{\vec{x}}$ de vecteur $\overrightarrow{x} \in D = \mathbb{R}\overrightarrow{\imath}$. Les deux termes g et $t_{\vec{x}}$ commutent. C'est la seule expression de f de ce type. Une telle isométrie est appelée le *vissage* d'axe $\mathcal{D}$, d'angle θ, de vecteur $\overrightarrow{x}$.



Si $\theta = \pi \pmod{2\pi}$, alors $g = r_{A,\pi}$ est aussi la symétrie orthogonale par rapport à la droite $\mathcal{D}$ issue de A, dirigée par $\overrightarrow{\imath}$. Le vissage $f = t_{\vec{x}} \circ g$, qui est un déplacement, est aussi la symétrie glissée définie par $\mathcal{D}$ et $\overrightarrow{x}$. Notons que pour tout $M \in \mathcal{E}_3$, le milieu I du segment $[MM']$, où $M' = f(M)$, appartient à $\mathcal{D}$.

Finalement, on peut dire que le groupe $\mathcal{I}^+$ des déplacements de $\mathcal{E}_3$ est l'ensemble des vissages : les translations sont les vissages pour lesquels l'angle de la rotation g est nul, les rotations sont les vissages dont le vecteur de translation $\vec{x}$ est nul. Un déplacement qui a un point fixe I est une rotation autour d'un axe passant par I.

2°/ *Supposons que $f = t_{\vec{x}} \circ g$ soit un antidéplacement.*

Dans la base orthonormée $\mathcal{B}$, la matrice de v_f est P'_θ.

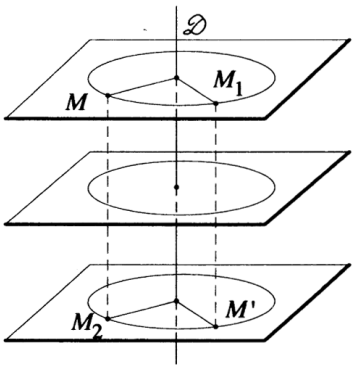
- Si $\theta \neq 0 \pmod{2\pi}$, on a $E_1 = \mathrm{Ker}\left(v_f - \mathrm{Id}_E\right) = \{\overrightarrow{0}\}$ donc $\overrightarrow{x}$ est nul et A est fixe par $f = g$. L'ensemble des points fixes de f est le sous-espace affine de $\mathcal{E}_3$ issu de A, de direction E_1. Il est réduit au point A (voir aussi 6-8, cor. 3). La matrice P'_θ montre que f est le produit de la rotation r autour de l'axe $\mathcal{D}$ issu de A dirigé par $\overrightarrow{\imath}$ et de la symétrie orthogonale s par rapport au plan $\mathcal{P}$ perpendiculaire en A à $\mathcal{D}$. De plus r et s commutent. On peut appeler *rotation-symétrie* ce type d'isométrie.

Si $\theta = \pi \pmod{2\pi}$, on a $P'_\theta = -I_3$. Alors f est la symétrie par rapport au point A. Cette rotation-symétrie particulière s_A est produit du demi-tour autour de $\mathcal{D}$ et de s.

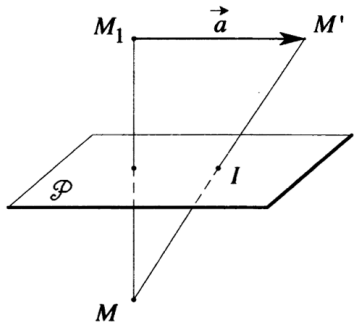
- Si $\theta = 0 \pmod{2\pi}$, la matrice de v_f est S. On a $\dim(E_1) = 2$ et v_f est la symétrie orthogonale par rapport à un plan de direction $E_1 = \mathrm{Ker}\left(v_f - \mathrm{Id}_E\right)$.

Si f a un point fixe A, l'ensemble des points de $\mathcal{E}_3$, fixes par f, est le plan $\mathcal{P}$ issu de A de direction E_1 et $f = g$ est la symétrie orthogonale par rapport $\mathcal{P}$.

Si f n'a pas de point fixe, alors $f = t_{\vec{x}} \circ g$ ou g est la symétrie orthogonale par rapport au plan $\mathcal{P}$ issu du point A, fixe pour g, de direction E_1 et où $\overrightarrow{x} \in E_1$. C'est une symétrie glissée. On notera que pour tout point $M \in \mathcal{E}_3$, le milieu I du segment $[MM']$, où $M' = f(M)$, appartient au plan $\mathcal{P}$ (voir fig.).



Rotation-symétrie

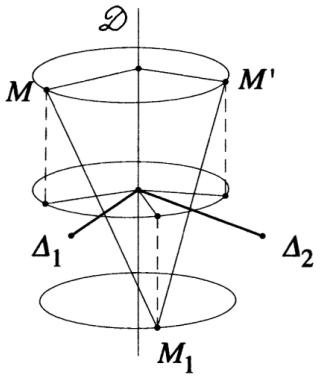


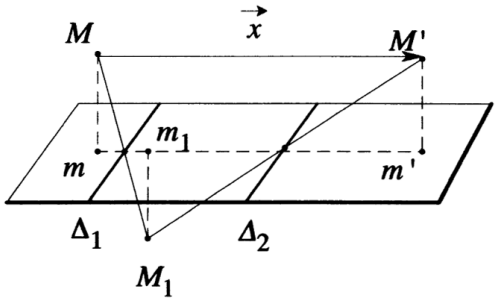
Symétrie glissée

Proposition.

Les déplacements de l'espace euclidien $\mathcal{E}_3$ sont les vissages. Les translations et les rotations autour d'un axe en sont des cas particuliers. Pour qu'un déplacement ait des points fixes, il faut et il suffit que ce soit une rotation autour d'un axe ou $Id_{\mathcal{E}_3}$.

Les antidéplacements sont les symétries orthogonales par rapport à un plan, les symétries planes glissées et les rotation-symétrie. Pour qu'un antidéplacement ait plus d'un point fixe, il faut et il suffit que ce soit une symétrie orthogonale par rapport à un plan. Pour qu'il ait un seul point fixe, il faut et il suffit que ce soit une rotation-symétrie.





Remarque 2. Les demi-tours, rotations d'angle π autour d'un axe, sont des déplacements. Ils engendrent $\mathcal{I}^+$. En effet, tout $f \in \mathcal{I}^+$ a une expression $f = t_{\vec{x}} \circ r_{D,\theta}$.

La rotation $r_{D,\theta}$, est le produit $r_{\Delta_2} \circ r_{\Delta_1}$ de deux demi-tours r_{Δ_2} et r_{Δ_1}, où on choisit la droite Δ_1 arbitrairement parmi les droites qui rencontrent D et sont perpendiculaires à D et où $\Delta_2 = r_{D,\frac{\theta}{2}}(\Delta_1)$.

La translation $t_{\vec{x}}$ est le produit $r_{\Delta_2} \circ r_{\Delta_1}$ de deux demi-tours r_{Δ_2} et r_{Δ_1}, où on choisit la droite Δ_1 arbitrairement parmi les droites de direction orthogonale à $\overrightarrow{x}$ et où $\Delta_2 = t_{\frac{1}{2}\vec{x}}(\Delta_1)$ (voir figures ci-dessus).

Notons que deux demi-tours $r_1 = r_{\Delta_1}$ et $r_2 = r_{\Delta_2}$ commutent si et seulement si $r_1 \circ r_2 \circ r_1^{-1} = r_2$ soit si $r_1(\Delta_2) = \Delta_2$. Cela se produit si $\Delta_1 = \Delta_2$ ou si Δ_1, Δ_2 sont concourantes et orthogonales.

	Déplacements		**Antidéplacements**	
$\dim(E_1)$	3	1	2	0
Il existe des points fixes	$\mathrm{Id}_{\mathcal{E}}$	rotations axiales	symétries planes	rotations-symétries
Il n'existe pas de point fixe	translations	vissages	symétries glissées	

Exercice. Dans l'espace affine euclidien $\mathcal{E}_3$ muni d'un repère orthonormé, $R = (O, \overrightarrow{\imath}, \overrightarrow{\jmath}, \overrightarrow{k})$, étudier les applications affines f et f^2, où f est définie par :

$$\begin{cases} x' &= -\frac{2}{3}x - \frac{2}{3}y + \frac{1}{3}z + 10 \\ y' &= -\frac{2}{3}x + \frac{1}{3}y - \frac{2}{3}z + 2 \\ z' &= \frac{1}{3}x - \frac{2}{3}y - \frac{2}{3}z + 6 \end{cases}.$$

Solution. Dans la base orthonormée $(\overrightarrow{\imath}, \overrightarrow{\jmath}, \overrightarrow{k})$ de l'espace vectoriel euclidien E associé à $\mathcal{E}_3$, la matrice de v_f est $A = \frac{1}{3}\begin{pmatrix} -2 & -2 & 1 \\ -2 & 1 & -2 \\ 1 & -2 & -2 \end{pmatrix}$. Elle est symétrique. Il existe donc une base orthonormée de E qui diagonalise A. Comme A est orthogonale, v_f est isométrique. Les valeurs propres de A sont 1 ou -1. Comme $\mathrm{tr}(A) = -1$, nécessairement A est semblable à $\begin{pmatrix} 1 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & -1 \end{pmatrix}$. Ainsi v_f est la symétrie vectorielle orthogonale par rapport à une droite vectorielle D, sous-espace propre relatif à la valeur propre 1 de v_f. Quant à l'isométrie f, c'est une symétrie glissée car v_f est orthogonale et symétrique. Soit $t_{\vec{a}} \circ s$ la forme canonique de f. Ici s est une symétrie orthogonale par rapport à une droite $\mathcal{D}$ de direction D, c'est-à-dire le demi-tour d'axe $\mathcal{D}$ et f est un déplacement. Pour tout $M \in \mathcal{E}_3$, cette droite $\mathcal{D}$ contient le milieu I de $[MM']$, où $M' = f(M)$. Avec $M = O$ on obtient $M'(10,2,6)$ donc $I(5,1,3)$ appartient à $\mathcal{D}$. Soit $I' = f(I)$. On obtient le vecteur $\overrightarrow{a} = \overrightarrow{II'} = 2\overrightarrow{\imath} - 4\overrightarrow{\jmath} + 2\overrightarrow{k}$. La droite $\mathcal{D}$ est la droite issue de I, dirigée par $\overrightarrow{\imath} - 2\overrightarrow{\jmath} + \overrightarrow{k}$. Puisque $t_{\vec{a}}$ et s commutent, on a $f^2 = t_{2\vec{a}} \circ s^2 = t_{2\vec{a}}$. C'est une autre façon de trouver le vecteur $t_{\vec{a}}$ en calculant par exemple $f^2(O) = P$ d'où $\overrightarrow{OP} = 2\overrightarrow{a}$. On pourrait également déterminer la direction de $\mathcal{D}$ en cherchant les vecteurs propres de v_f relatifs à la valeur propre 1.

8.11 Groupe des similitudes

Définition.

On appelle similitude de l'espace affine euclidien $\mathcal{E}_n$, une application $f : \mathcal{E}_n \to \mathcal{E}_n$ telle qu'il existe $k_f \in \mathbb{R}_+^*$, appelé rapport de f, vérifiant pour tous $M, N \in \mathcal{E}_n$:

(1) $\qquad M'N' = k_f\, MN \qquad$ *où* $\qquad M' = f(M) \quad , \quad N' = f(N)\,.$

Proposition.

Notons S l'ensemble des similitudes, $\mathcal{I}$ le groupe des isométries, H le groupe des homothéties et translations et T le groupe des translations.

(i) *S est un sous-groupe de $Aut(\mathcal{E}_n)$ et on a $T \lhd S$, $H \lhd S$, $\mathcal{I} \lhd S$.*

(ii) *Si $f \in S$ a un point fixe unique A, posons $h = h_{A,k_f}$. Alors $g = h^{-1} \circ f$ est une isométrie et $f = h \circ g = g \circ h$. De plus, g et h sont les seules isométrie et homothétie de rapport positif permutables dont f est la composée.*

(iii) *Soit $f \in S$ tel que $k_f \neq 1$. Alors f admet un point fixe unique A.*

(iv) *Soit A un point de $\mathcal{E}_n$. Alors S est isomorphe à un produit semi-direct $\mathbb{R}^n \times_\alpha S_A$, où S_A est le stabilisateur de A, c'est-à-dire l'ensemble des similitudes de centre A. Il est également isomorphe à un produit semi-direct $\mathcal{I} \times_\beta \mathbb{R}_*^+$.*

Démonstration. (i) Soient $A \in \mathcal{E}_n$ et h l'homothétie h_{A,k_f}. Alors $g = h^{-1} \circ f$ est une isométrie de $\mathcal{E}_n$. D'après 8-6, g est affine et bijective donc $f = h \circ g \in \mathrm{Aut}(\mathcal{E}_n)$.

La relation (1) montre alors que $f^{-1} \in S$ avec $k_{f^{-1}} = \frac{1}{k_f}$. Pour $f, f' \in S$, la relation (1) montre à l'évidence que $f \circ f' \in S$ et que $k_{f \circ f'} = k_f\, k_{f'}$. Ainsi, S est un sous-groupe de $\mathrm{Aut}(\mathcal{E}_n)$ et $\chi : f \mapsto k_f$ est un homomorphisme de S dans le groupe multiplicatif $\mathbb{R}_+^*$. Il en résulte que $\mathcal{I} = \mathrm{Ker}(\chi)$ est un sous-groupe distingué de S. Comme T et H sont des sous-groupes distingués de $\mathrm{Aut}(\mathcal{E}_n)$ (voir 6-9 et 6-10), contenus dans S, ce sont des sous-groupes distingués de S.

(ii) Revenons au début de (i), en plaçant A au point fixe. Alors $f = h \circ g$ et A est fixe par f, g, h. Etablir que $h \circ g = g \circ h$ revient à montrer que $v_h \circ v_g = v_g \circ v_h$, ce qui est vérifié puisque $v_h = k_f\, \mathrm{Id}_E$ est dans le centre de $\mathrm{GL}(n, \mathbb{R})$.

Soit $f = h' \circ g' = g' \circ h'$, une expression de f, où g' est une isométrie et où h' est une homothétie de centre A' de rapport positif. Ce rapport est nécessairement k_f. Comme $g' \circ h' \circ g'^{-1}$ est l'homothétie de centre $g'(A')$, de même rapport que h', le fait que $g' \circ h' \circ g'^{-1} = h'$ implique $g'(A') = A'$. Alors A' est fixe par h', par g' et par f. Il est donc égal à l'unique point fixe A de f. Les homothéties h et h' ont même centre, même rapport k_f. Elles sont donc égales et $g = h^{-1} \circ f$ est égale à g'.

(iii) Supposons $k_f \neq 1$. On a $\mathrm{Ker}\left(v_f - \mathrm{Id}_E\right) = \{\overrightarrow{0}\}$. D'après 6-8, cor. 3, il existe un unique point fixe pour f. Pour voir cela, on peut aussi utiliser le fait que f est une contraction de l'espace métrique complet $\mathcal{E}_n$ pour $k_f < 1$. Elle a donc un point fixe unique A. Pour $k_f > 1$, alors f^{-1} de rapport $\frac{1}{k_f}$ admet un point fixe unique A. Les relations $f(A) = A$ et $A = f^{-1}(A)$ sont équivalentes donc A est fixe pour f et unique.

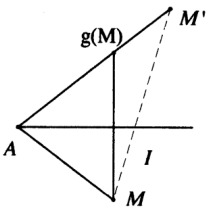
(iv) En utilisant le lemme 6-10, on voit que $S = T \times_\alpha S_A \simeq \mathbb{R}^n \times_\alpha S_A$, où α est l'action $(f, \overrightarrow{x}) \mapsto v_f(\overrightarrow{x})$ de S_A sur $\mathbb{R}^n$.

L'homomorphisme surjectif $\chi : f \mapsto k_f$ de S sur $\mathbb{R}_+^*$ a pour noyau $\mathcal{I}$. Si on fixe $A \in \mathcal{E}_n$, alors $\tau : \lambda \mapsto h_{A,\lambda}$, est un homomorphisme de $\mathbb{R}_+^*$ dans S tel que $\chi \circ \tau = \mathrm{Id}_{\mathbb{R}_+^*}$ donc S est un produit semi-direct de $\mathcal{I}$ par $\mathbb{R}_+^*$ (voir 2-7, ex. 1). ∎

Définition.

Quand f admet un point fixe unique, on l'appelle le centre de la similitude et l'unique expression de $f = h \circ g$, où h et g sont une homothétie et une isométrie permutables, est appelé la forme réduite de f. Evidemment, g a elle-même une décomposition canonique (voir 8-8).

Remarque. Soit f une similitude plane indirecte avec un point fixe A. Posons $k = k_f$. Alors $g = h_{A,k}^{-1} \circ f$ est une isométrie indirecte qui a pour point fixe A. C'est une symétrie par rapport à une droite $\mathcal{D}$ passant par A. Pour tout point $M \in \mathcal{E}_2$, dans le triangle MAM', où $M' = f(M)$, la droite $\mathcal{D}$ est bissectrice de l'angle $(\overrightarrow{AM}, \overrightarrow{AM'})$. Ainsi, pour tout M, le point I de $[MM']$ qui divise ce segment dans le rapport k est un point de $\mathcal{D}$.



Exercice. On identifie le plan affine euclidien $\mathcal{E}_2$, muni d'un repère orthonormé, avec le plan complexe $\mathbb{C}$. Donner l'expression des similitudes.

Solution. Soit $f \in S$. Posons $k = k_f$. Considérons l'homothétie $h : z \mapsto kz$. Nous avons vu en démontrant (i), que $h^{-1} \circ f = g$ est une isométrie. Si f est directe, alors g est directe, d'expression $z \mapsto e^{i\theta}z + \beta$. On en déduit l'expression $f : z \mapsto ke^{i\theta}z + b = az + b$, où $a \in \mathbb{C}^*$, des similitudes directes. Le groupe S^+ des similitudes directes est donc isomorphe au groupe des automorphismes affines de la droite complexe et donc au produit semi-direct $\mathbb{C} \times_\alpha \mathbb{C}_*$, où $\mathbb{C}_*$ agit sur $\mathbb{C}$ par multiplications (voir 6-9, prop., (iv)). Si $a \neq 1$, $s_{a,b}$ admet un unique point fixe d'affixe $\frac{b}{1-a}$. Exemple : $f : z \mapsto (i-1)z + 2 - i$ a pour point fixe A d'affixe 1, pour rapport $k = |i-1| = \sqrt{2}$ et pour angle $\theta = \mathrm{Arg}(i-1) = \frac{3\pi}{4}$.

Dans le groupe S, les similitudes indirectes constituent la classe $S^+\sigma$, modulo le sous-groupe distingué S^+, de la symétrie orthogonale $\sigma : z \mapsto \bar{z}$. C'est donc l'ensemble des applications de la forme $f : z \mapsto a\bar{z} + b$, où $a \in \mathbb{C}_*, b \in \mathbb{C}$. Pour $|a| \neq 1$, notons que l'unique point fixe de f est aussi le point fixe de la similitude directe $f \circ f : z \mapsto a\bar{a}z + a\bar{b} + b$. Il a pour affixe $\frac{a\bar{b}+b}{1-|a|^2}$.

8.12 Sous-groupes finis du groupe des déplacements

Proposition.

Soit G un sous-groupe fini, d'ordre $n \geqslant 2$, du groupe $\mathcal{I}^+$ des déplacements de l'espace affine euclidien $\mathcal{E} = \mathcal{E}_3$. Alors, G est isomorphe à $\mathbb{U}_n$ ou à $D_{n/2}$ (n est alors pair) ou bien à l'un des trois groupes des déplacements qui conservent l'un des cinq polyèdres réguliers, c'est-à-dire isomorphe à $\mathcal{A}_4$, $\mathcal{S}_4$ ou $\mathcal{A}_5$.

Soit $A \in \mathcal{E}$. Tout $g \in G$ permute les points de l'orbite (finie) de A et laisse donc fixe l'isobarycentre O de ces points. D'après 8-10, prop., tout $g \in G \setminus \{\mathrm{Id}_\mathcal{E}\}$ est donc une rotation autour d'un axe $\mathcal{D}_g$ passant par O. Les points P_g et P'_g où $\mathcal{D}_g$ coupe la sphère S de centre O de rayon 1 sont appelés les pôles de g. L'ensemble $X \subset S$ des pôles des éléments g de $G \setminus \{\mathrm{Id}_\mathcal{E}\}$ est invariant par g_0 pour tout $g_0 \in G$. En effet, pour tout $g \in G \setminus \{\mathrm{Id}_\mathcal{E}\}$, on a $g_0 g g_0^{-1} \in G \setminus \{\mathrm{Id}_\mathcal{E}\}$ et $g_0 g g_0^{-1}$ laisse fixe tout point de $g_0(\mathcal{D}_g)$. Ses pôles sont donc $g_0(P_g) \in X$ et $g_0(P'_g) \in X$.

Ainsi, le groupe G (d'ordre n) opère naturellement sur l'ensemble fini X. On a $1 \leqslant \mathrm{card}\,(G \setminus \{\mathrm{Id}_\mathcal{E}\}) = n-1$ et donc $2 \leqslant \mathrm{card}\,(X) \leqslant 2(n-1)$. Le nombre d'orbites est

(1) $k = \frac{1}{[G:1]} \sum_{g \in G} \text{card}\,(\text{fix}(g)) = \frac{1}{n}\,[\,\text{card}\,(X) + 2(n-1)\,]$ (formule de Burnside).

En effet, $\text{Id}_{\mathcal{E}} \in G$ laisse fixe tout point de X et tout $g \in G \setminus \{\,\text{Id}_{\mathcal{E}}\}$ a deux points fixes P_g, P'_g. De (1) on déduit $2 \leqslant k \leqslant 4(1 - \frac{1}{n}) < 4$, soit $k = 2$ ou 3. $\mathbb{U}$

1°) *Supposons que* $k = 2$. D'après (1), on a $\text{card}\,(X) = 2$. Ainsi, tous les éléments de $G \setminus \{\,\text{Id}_{\mathcal{E}}\}$ ont les mêmes pôles : les deux éléments P, P' de X. Ayant le même axe, ils laissent stable le plan $\mathcal{H}$ perpendiculaire en O à la droite (PP'). Tout $g \in G$ induit donc une isométrie $f(g)$ de $\mathcal{H}$. Il est clair que $g \mapsto f(g)$ est un isomorphisme de G sur $f(G)$. Comme $f(G)$ est un sous-groupe fini du groupe des rotations de centre O, il est cyclique, isomorphe à $\mathbb{U}_n$ (voir Ex. 8-4)

2°) *Supposons que* $k = 3$. Soient X_1, X_2, X_3 les trois orbites, avec $\text{card}\,(X_1) \geqslant \text{card}\,(X_2) \geqslant \text{card}\,(X_3)$. Pour $1 \leqslant i \leqslant 3$, l'ordre m_i du stabilisateur G_P d'un point $P \in X_i$, ne dépend que de X_i (2-3, prop. (iii)) et vérifie $\text{card}\,(X_i) = \frac{[G:1]}{m_i}$. On a donc $2 \leqslant m_1 \leqslant m_2 \leqslant m_3$ (on a $2 \leqslant m_1$ car $P \in X_1$ étant pôle d'un $g \in G \setminus \{\,\text{Id}_{\mathcal{E}}\}$, on a $\{\,\text{Id}_{\mathcal{E}}, g\} \subset G_P$). D'après (1), on a $\text{card}\,(X) = n + 2$. L'équation des classes donne $n + 2 = \text{card}\,(X_1) + \text{card}\,(X_2) + \text{card}\,(X_3) = \frac{n}{m_1} + \frac{n}{m_2} + \frac{n}{m_3}$, soit :

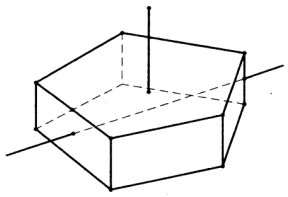
(2) $$1 + \tfrac{2}{n} = \tfrac{1}{m_1} + \tfrac{1}{m_2} + \tfrac{1}{m_3}.$$

On en déduit $1 < \frac{3}{m_1}$ et donc $m_1 = 2$. Ainsi, (2) s'écrit :

(3) $$\tfrac{1}{2} + \tfrac{2}{n} = \tfrac{1}{m_2} + \tfrac{1}{m_3}.$$

On en déduit $\frac{1}{2} < \frac{2}{m_2}$ et donc $m_2 = 2$ ou 3.

a) *Supposons que* $m_2 = 2$. Comme $\text{card}\,(X_2) = \frac{[G:1]}{m_2}$, l'ordre n de G est pair. On a $\text{card}\,(X_1) = \frac{n}{2} = \text{card}\,(X_2)$ et $\text{card}\,(X_3) = \text{card}\,(X) - n = 2$, d'où $X_3 = \{P, P'\}$. Le stabilisateur G_P de P est cyclique, d'ordre $\frac{n}{2}$, isomorphe à $\mathbb{U}_{n/2}$ (raisonner comme en 1°), lorsque $k = 2$). Pour tout $g \in G \setminus G_P$ on a $g \cdot P \neq P$ donc $g \cdot P \in X_3$ est égal P' et de même, $g \cdot P' = P$. La rotation g est donc un demi-tour autour d'un axe Δ perpendiculaire à $[PP']$ en son milieu O. Ainsi, tout $g \in G \setminus G_P$ est d'ordre 2. C'est notamment le cas de ag, où $a \in G_P$ est un générateur de $G_P \simeq \mathbb{U}_{n/2}$. Cela prouve que G est isomorphe à $D_{n/2}$ (voir Ex. 8-3). Notons qu'il existe des polyèdres de $\mathcal{E}$ dont le groupe des déplacements qui les conservent est G (figure faite pour $n = 10$).



b) *Supposons que* $m_2 = 3$. Alors (3) donne :

(4) $$\tfrac{1}{6} + \tfrac{2}{n} = \tfrac{1}{m_3}.$$

On en déduit $\frac{1}{6} < \frac{1}{m_3}$ soit $m_3 \leqslant 5$, avec $3 = m_2 \leqslant m_3$. Ainsi, $m_3 = 3, 4$ ou 5.

(i) *Supposons que* $m_3 = 3$. D'après (4), on a $n = 12$,

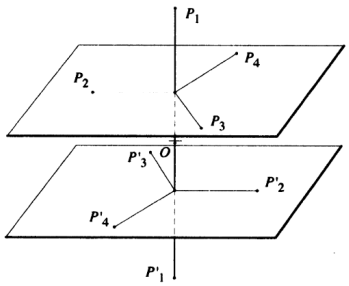
$\text{card}\,(X_1) = \frac{[G:1]}{m_1} = \frac{12}{2} = 6$, $\text{card}\,(X_2) = \frac{[G:1]}{m_2} = \frac{12}{3} = 4$, $\text{card}\,(X_3) = \frac{[G:!1]}{m_3} = \frac{12}{3} = 4$.

Tout $g \in G$ laisse stable X_2 et induit une permutation s_g de X_2. L'homomorphisme $s : g \mapsto s_g$ de G dans $\mathcal{S}_4$ est injectif. En effet, considérons $g \in \text{Ker}\,(s)$. On a $s_g = \text{Id}_{X_2}$. Comme g laisse fixe deux points P, Q de X_2, c'est une rotation autour de l'axe (PQ). Si on avait $g \neq \text{Id}_{\mathcal{E}}$, alors P et Q seraient les seuls points de S fixes par g, ce qui contredirait le fait que g laisse fixes les quatre points de X_2. Ainsi, $s(G)$ est un sous-groupe d'ordre 12 de $\mathcal{S}_4$. C'est le groupe alterné $\mathcal{A}_4$ (seul sous-groupe d'ordre 12 de $\mathcal{S}_4$ d'après 4-4, cor. 1). Donc G est isomorphe à $\mathcal{A}_4$ lui même isomorphe au groupe des déplacements qui conservent un tétraèdre régulier (Ex. 8-9).

(ii) *Supposons que* $m_3 = 4$. D'après (4), on a $n = 24$, d'où :

$\text{card}\,(X_1) = \frac{[G:1]}{m_1} = \frac{24}{2} = 12$, $\text{card}\,(X_2) = \frac{[G:1]}{m_2} = \frac{24}{3} = 8$, $\text{card}\,(X_3) = \frac{[G:1]}{m_3} = \frac{24}{4} = 6$.

Soit $P \in X_i$, où $1 \leqslant i \leqslant 3$. Le point P', symétrique de P par rapport à O , a le même stabilisateur que P . Comme m_1, m_2, m_3 sont distincts, P' appartient nécessairement à l'orbite X_i. Dans chaque orbite X_i, on peut donc associer les points par couples de points symétriques P, P'. Considérons $P_1 \in X_2$. On a $[G_{P_1} : 1] = m_2 = 3$. Soit $g \in G_{P_1}$, avec $g \neq \text{Id}_{\mathcal{E}}$. L'ordre de g est 3 . C'est une rotation autour de (P_1P_1') , d'angle $\pm\frac{2\pi}{3}$. Considérons $P_2 \in X_2 \setminus \{P_1, P_1'\}$. Alors P_2 , $P_3 = g\cdot P_2$, $P_4 = g^2\cdot P_2$ sont les sommets d'un triangle équilatéral dans un plan $\mathcal{H}$ perpendiculaire à (P_1P_1') . Leurs symétriques P_2', P_3', P_4' par rapport à O , appartiennent au plan symétrique $\mathcal{H}'$. Les plans $\mathcal{H}$ et $\mathcal{H}'$ sont distincts, sinon tout $g \in G$, qui laisse stable $X_2 = \{P_1, P_1', \ldots, P_4, P_4'\}$, devrait laisser le plan $\mathcal{H}$ invariant, ainsi que sa perpendiculaire (P_1P_1'). On voit que G laisserait stable $\{P_1, P_1'\}$, ce qui est exclu compte tenu des cardinaux des trois orbites. Dans X_2 les segments $[P_1P_2], [P_1P_3], [P_1P_4]$ et leurs symétriques ont la même longueur. Or, ces raisonnements ne s'appliquent pas seulement au couple P, P' de l'orbite X_2 mais à chacun des couples. On voit donc que les points de X_2 sont les sommets d'un cube Γ que G laisse invariant et dont les 4 couples (P_1P_1') , …, (P_4P_4') constituent les grandes diagonales. Tout $g \in G$ détermine une permutation s_g de ces 4 droites, d'où un homomorphisme $s : g \mapsto s_g$ de G dans $\mathcal{S}_4$.

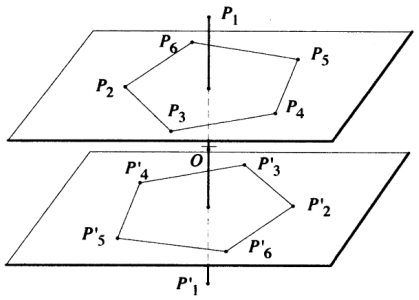


Vérifions que l'homomorphisme $s : g \mapsto s_g$ est injectif de G dans $\mathcal{S}_4$. Considérons $g \in \text{Ker}\,(s)$. Pour tout $i = 1, \ldots, 4$, g laisse stable $\{P_i, P_i'\}$. Supposons qu'il existe i tel que $g(P_i) = P_i'$. Alors g est un demi-tour par rapport à une droite Δ perpendiculaire en O à (P_iP_i') . Comme g laisse fixe deux points seulement de la sphère S et que dans X_2 on a huit points, nécessairement il existe deux autres couples (P_k, P_k') et (P_l, P_l') que g échange. Comme (O, P_i, P_k, P_l) est un repère affine, $g = s_O$. C'est absurde car s_O est un antidéplacement. Donc g laisse fixes les huit points de X_2 et $g = \text{Id}_{\mathcal{E}}$. Ainsi, s est un homomorphisme injectif de G , d'ordre 24 dans $\mathcal{S}_4$ d'ordre 24 . C'est donc un isomorphisme de G sur le groupe des déplacements qui conservent le cube Γ , groupe isomorphe à $\mathcal{S}_4$ (voir Ex. 8-10).

(iii) *Supposons que* $m_3 = 5$. D'après (4), on a $n = 60$, d'où :

$\text{card}\,(X_1) = \frac{[G:1]}{m_1} = \frac{60}{2} = 30$, $\text{card}\,(X_2) = \frac{[G:1]}{m_2} = \frac{60}{3} = 20$, $\text{card}\,(X_3) = \frac{[G:1]}{m_3} = 12$.

Puisque m_1, m_2, m_3 sont distincts, on peut, comme dans le cas précédent, associer dans chaque orbite X_i , les points par couples de points symétriques P, P' . Considérons $P_1 \in X_3$. On a $[G_{P_1} : 1] = m_3 = 5$. Soit $g \in G_{P_1}$, avec $g \neq \text{Id}_{\mathcal{E}}$. L'ordre de g est 5 . C'est une rotation autour de (P_1P_1') , d'angle $\pm\frac{2\pi}{5}$. Considérons $P_2 \notin \{P_1, P_1'\}$. Alors P_2 , $P_3 = g\cdot P_2$, $P_4 = g\cdot P_3$, $P_5 = g\cdot P_4$, $P_6 = g\cdot P_5$ sont les sommets d'un pentagone régulier dans un plan $\mathcal{H}$ perpendiculaire à (P_1P_1') . Leurs symétriques $P_2', \ldots, P_6'$ par par rapport à O , appartiennent au plan symétrique $\mathcal{H}'$. Comme dans le cas précédent, les plans $\mathcal{H}$ et $\mathcal{H}'$ sont distincts. Ces propriétés étant valables pour chacun des couples (P_i, P_i') de X_3 , les points de X_2 sont les sommets d'un icosaèdre régulier Γ que G laisse invariant. Or le groupe des déplacements conservant Γ est d'ordre 60 (admis ici), isomorphe à $\mathcal{A}_5$. Donc G est égal à ce groupe. ∎



Exercices du chapitre 8

Ex 8 - 1

On identifie le plan affine euclidien $\mathcal{E}_2$, muni d'un repère orthonormé, avec $\mathbb{C}$. On appelle inversion de centre $O \in \mathcal{E}_2$, de puisance $k > 0$, l'application f de $\mathcal{E}_2 \setminus \{O\}$ dans lui-même associant à $M \in \mathcal{E}_2 \setminus \{O\}$ le point M' de la droite (OM) tel que $\overline{OM}\,\overline{OM'} = k$.

a) Donner l'expression $z \mapsto f(z)$ de f. Montrer que f est involutive et qu'elle conserve les angles.

b) Donner l'image par f d'une droite Δ, d'un cercle Γ.

c) Soient A et B les points d'affixes $a > 0$ et $-a$. Pour tout cercle C du faisceau $\mathcal{F}$ à points de base A et B, soient M et N les point d'intersection de C avec le diamètre D de C parallèle à $(x'x)$. Quand C décrit $\mathcal{F}$, quel est l'ensemble H des points M et N ?

d) Donner une équation cartésienne, un paramétrage rationnel, une génération géométrique de la courbe L inverse de H par l'inversion de centre O et de puissance $\overline{OA}^2$. Montrer que L est l'un des ovales de Cassini de foyers I et I', inverses des foyers F et F' de H.

e) Etudier l'image S de H par l'inversion de centre A, de puissance $\overline{AB}^2$.

Ex 8 - 2

Dans le plan affine euclidien $\mathcal{E}_2$, soit P un polygone convexe régulier à n côtés (où $n \geqslant 3$), de sommets $A_0, ..., A_{n-1}$.

Montrer que l'ensemble D_n des applications affines de $\mathcal{E}_2$ dans $\mathcal{E}_2$ telles que $f(P) = P$ est un sous-groupe fini du groupe $\mathcal{I}$ des isométries de $\mathcal{E}_2$. Dans D_n, déterminer le stabilisateur d'un sommet A_i de P. En déduire le cardinal de D_n.

Décrire les éléments de D_n et montrer que D_n est engendré par r, s tels que :

$r^n = \mathrm{Id}_{\mathcal{E}_2}$, $s^2 = \mathrm{Id}_{\mathcal{E}_2}$, $(sr)^2 = \mathrm{Id}_{\mathcal{E}_2}$.

Ex 8 - 3

Soit G un groupe engendré par deux éléments a, b tels que

(1) $o(a) = n$, $b^2 = e$, $(ab)^2 = e$, où $n \geqslant 3$. Montrer que $H = \{e, a, ..., a^{n-1}\}$ est un sous-groupe distingué de G et que G est un produit semi-direct de H par $K = \{e, b\}$. En déduire que G est unique, à isomorphisme près.

Ex 8 - 4

Soit G un sous-groupe fini du groupe $\mathcal{I}$ des isométries du plan euclidien $\mathcal{E}_2$. Montrer que G est isomorphe à $\mathbb{Z}/n\mathbb{Z}$ ou à D_n.

Ex 8 - 5

Soit ABC un triangle non aplati du plan euclidien. Quelle est la composée f des rotations r_A, r_B, r_C d'angles $(\overrightarrow{AB}, \overrightarrow{AC})$, $(\overrightarrow{BC}, \overrightarrow{BA})$, $(\overrightarrow{CA}, \overrightarrow{CB})$, de centres A, B, C ? Si ABC est équilatéral, quel est le point fixe de f ?

Quelle est la composée g des symétries orthogonales $s_{(BC)}$, $s_{(CA)}$, $s_{(AB)}$? Donner son expression canonique.

Ex 8 - 6

Soient C un cercle du plan euclidien et $\Delta, \Delta', \Delta''$ trois directions de droites, distinctes. Pour tout $M \in C$, on considère le point $M_1 \in C$ où la droite issue de M de direction Δ recoupe C, puis $M_2 \in C$ où la droite issue de M_1 de direction Δ' recoupe C, puis $M_3 \in C$ où la droite issue de M_2 de direction Δ'' recoupe C. A partir de M_3, on reprend le procédé, comme pour M. Etudier la suite des points de C ainsi, définie.

Ex 8 - 7

L'espace euclidien $\mathcal{E}_3$ est muni d'un repère orthonormé $(A,\vec{\imath},\vec{\jmath},\vec{k})$. Donner l'expression de la symétrie othogonale f par rapport au plan $\mathcal{P}$ issu de $B(2,0,-2)$, de direction orthogonale à $\vec{v} = 2\vec{\imath}+\vec{\jmath}-\vec{k}$.

Ex 8 - 8

L'espace affine euclidien $\mathcal{E}_3$ est muni d'un repère orthonormé $(A,\vec{\imath},\vec{\jmath},\vec{k})$. Montrer que l'application f définie par

$$\begin{cases} x' &= \frac{2}{3}x - \frac{1}{3}y + \frac{2}{3}z + 2 \\ y' &= \frac{2}{3}x + \frac{2}{3}y - \frac{1}{3}z \\ z' &= -\frac{1}{3}x + \frac{2}{3}y + \frac{2}{3}z + 1 \end{cases}$$

est une isométrie. Préciser sa nature, sa décomposition canonique.

Etudier de même g définie par

$$\begin{cases} x' &= \frac{7}{9}x - \frac{4}{9}y - \frac{4}{9}z \\ y' &= -\frac{4}{9}x + \frac{1}{9}y - \frac{8}{9}z - 2 \\ z' &= -\frac{4}{9}x - \frac{8}{9}y + \frac{1}{9}z + 2 \end{cases}$$

Ex 8 - 9

Dans l'espace euclidien $\mathcal{E}_3$, étudier la composée $f' \circ f$ de deux demi-tours f et f' d'axes $\mathcal{D}$ et $\mathcal{D}'$.

Ex 8 - 10

Soit $T = A_1A_2A_3A_4$ un tétraèdre régulier de l'espace euclidien $\mathcal{E}_3$. On note G l'ensemble des applications affines f de $\mathcal{E}_3$ dans $\mathcal{E}_3$ telles que $f(T) = T$.

a) Montrer que tout $f \in G$ induit une permutation $s_f \in \mathcal{S}_4$ des sommets de T. Montrer que G est un sous-groupe fini du groupe $\mathcal{I}$ des isométries de $\mathcal{E}_3$, isomorphe au groupe $\mathcal{S}_4$.
Montrer que f est un déplacement si et seulement si s_f est paire.

b) Montrer que les éléments de G correspondant aux permutations $[1,2][3,4]$, $[1,3][2,4]$, $[1,4][2,3]$, Id constituent un sous-groupe distingué de G.
En déduire que les droites joignant les milieux de deux arêtes opposées de T sont deux à deux perpendiculaires.

c) Soit $f \in G$ d'ordre 2. Etudier les orbites de $\{\mathrm{Id}, f\}$ sur les sommets de T. Caractériser f.

d) Décrire les stabilisateurs des sommets. Montrer qu'ils sont conjugués dans G. Montrer que tout sous-groupe d'ordre 3 de G est contenu dans le stabilisateur d'un sommet. Quels sont les éléments d'ordre 3 de G ?

e) Préciser la nature des éléments de G.

Ex 8 - 11

Soit $\Gamma = ABCDA'B'C'D'$ un cube de l'espace euclidien $\mathcal{E}_3$ ($ABCD$ est une face et $\overrightarrow{AA'} = \overrightarrow{BB'} = \overrightarrow{CC'} = \overrightarrow{DD'}$). Considérons $G = \{ f \in \mathcal{A}(\mathcal{E}_3) \mid f(\Gamma) = \Gamma \}$.

a) Montrer que G est un sous-groupe du groupe $\mathcal{I}$ des isométries de $\mathcal{E}_3$. Etudier l'orbite du sommet A, son stabilisateur G_A. Préciser l'ordre de G.

b) Soit H un sous-groupe d'ordre 3 de G. Montrer que H est contenu dans le stabilisateur d'un sommet. Combien de sous-groupes d'ordre 3 existe-t-il dans G ? Est-ce conforme aux th. de Sylow ?

c) Montrer que tout $f \in G$ définit une permutation σ_f des quatre grandes diagonales $[AC']$, $[BD']$, $[CA']$, $[DB']$. Montrer que $\varphi : f \mapsto \sigma_f$ est un homomorphisme surjectif de G sur le groupe $\mathcal{S}_4$ des permutations des diagonales.
Montrer que $\mathrm{Ker}\,(\varphi)$ est le centre de G.

d) Montrer que $G^+ = G \cap \mathcal{I}^+$ est un sous-groupe distingué de G isomorphe au groupe symétrique $\mathcal{S}_4$. En déduire que G est isomorphe à $\mathcal{S}_4 \times \mathbb{Z}/2\mathbb{Z}$.

e) Préciser la nature des divers éléments de G.

Indications

Ex 8 - 1

a) Si $X+iY=f(x+iy)$, alors
$$X=k\frac{x}{x^2+y^2}\ ,\ Y=k\frac{y}{x^2+y^2}\,.$$

b) Si $O\notin\Delta$, alors $f(\Delta)$ est un cercle Δ' passant par O, privé du point O. L'image de Δ' est Δ. L'image d'un cercle qui ne passe pas par O, est un autre cercle ne passant pas par O.

c) Si P est le projecté orthogonal de M sur $(x'x)$, on a $\overline{PM}^2=\overline{PA}\ \overline{PA'}$, d'où l'équation de H (c'est une hyperbole équilatère).

d) et **e)** Avec les formules a), une équation globale ou paramétrée de L (resp. S) se déduit de celles de H.

Ex 8 - 2

Utiliser 7-9, cor. ; D_n est engendré par la rotation $r=r_{O,2\pi/n}$ et la symétrie orthogonale s par rapport à $(x'x)$.

Ex 8 - 3

Montrer que tout $x\in G$ possède une expression unique de la forme a^m ou a^mb, avec $0\leqslant m\leqslant n-1$.

Ex 8 - 4

Il existe un point fixe pour tous les éléments de G. Si $G\subset\mathcal{I}^+$, les éléments de G sont des rotations $z\mapsto e^{i\theta}z$. Dans $\mathbb{C}^*$, les éléments $e^{i\theta}$ forment un sous-groupe fini.

Ex 8 - 5

f est un déplacement d'angle π et g est une symétrie glissée. (Considérer $g(C)$ et $g(I)$ où I est le symétrique de A par rapport à (BC)).

Ex 8 - 6

On passe de M à M_3 en composant des symétries orthogonales.

Ex 8 - 7

Paramétrer la droite issue de M et dirigée par $\overrightarrow{v}$. Déterminer l'intersection avec $\mathcal{P}$.

Ex 8 - 8

f est un vissage. La direction de l'axe est le sous-espace propre $\mathrm{Ker}\,(v_f-\mathrm{Id})$.
g est une symétrie glissée. Si $t_{\vec{a}}\circ s_{\mathcal{P}}$ est sa forme canonique, le milieu de $[MM']$, où $M'=f(M)$, appartient à $\mathcal{P}$.

Ex 8 - 9

Si $\mathcal{D}$ et $\mathcal{D}'$ ne sont pas coplanaires, considérer leur perpendiculaire commune (II') et la parallèle à $\mathcal{D}$ issue de I'.

Ex 8 - 10

Utiliser 7-9, cor. Les symétries orthogonales par rapport aux plans médiateurs des arêtes sont éléments de G.

Ex 8 - 11

a) Utiliser 7-9, cor.

b) Utiliser l'équation des classes.

c) La symétrie orthogonale par rapport au plan de deux diagonales échange les deux autres.

d) La restriction de φ à G^+ est un isomorphisme de G^+ sur $\mathcal{S}_4$.

e) On voit bien les éléments de G si on pose le cube sur un plan horizontal, sur une face, sur une arête puis sur un sommet.

Solutions des exercices du chapitre 8

Ex 8 - 1

a) Les affixes $z = x + iy$ de M et $Z = X + iY$ de $M' = f(M)$ sont telles que $Z\bar{z} = k$. En effet, z et Z ont même argument et $|z|\,|Z| = OM \times OM' = k$. La relation $X + iY = \frac{k}{\overline{x+iy}} = k\,\frac{x+iy}{x^2+y^2}$ donne :

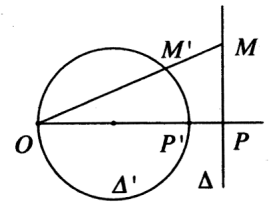
$$X = k\,\frac{x}{x^2+y^2} \quad , \quad Y = k\,\frac{y}{x^2+y^2}. \tag{1}$$

Pour tout $z \in \mathbb{C}^*$ on a $f(f(z)) = \frac{k}{\overline{f(z)}} = z$ donc $f^2 = \mathrm{Id}_{\mathcal{E}_2 \setminus \{O\}}$ et f est involutive.

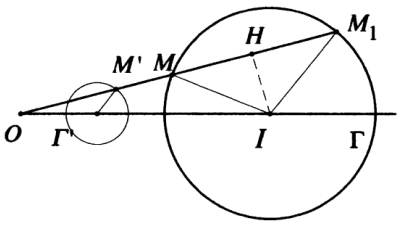
La symétrie orthogonale $z \mapsto \bar{z}$ et $z \mapsto \frac{1}{z}$ qui est holomorphe sur $\mathbb{C}^*$ conservent les angles en valeur absolue donc f également (mais elle change leur signe).

b) Soit Δ une droite. Si Δ passe par O, il est clair que $\Delta \setminus \{O\}$ est invariante par f. Supposons que $O \notin \Delta$ Notons P le projeté de O sur Δ et P' l'inverse de P. Choisissons l'axe des abscisses dirigé par $\overrightarrow{OP}$. La droite Δ a pour équation $x = a$, d'où l'équation de la courbe inverse : $\frac{kX}{X^2+Y^2} = a$, soit encore $X^2 + Y^2 - \frac{k}{a}X = 0$. C'est le cercle Δ' de diamètre $[OP']$ (privé du point O).

Géométriquement, les triangles OPM et $OM'P'$ sont semblables car $\overline{OM}\,\overline{OM'} = \overline{OP}\,\overline{OP'} = k$. Donc l'angle $(\overrightarrow{M'O}, \overrightarrow{M'P'})$ est droit, M' varie sur le cercle Δ' de diamètre $[OP']$. Si M décrit Δ, le point M' décrit $\Delta' \setminus \{O\}$. Comme f est involutive, on a $f(\Delta' \setminus \{O\}) = \Delta$. L'inverse d'un cercle Δ' passant par O (privé du point O), est donc une droite Δ perpendiculaire au diamètre $[OP']$ du cercle.



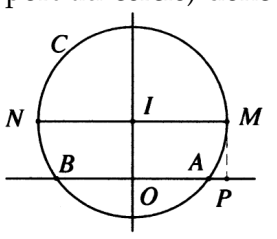
Soit Γ un cercle, de centre I, de rayon r, ne passant pas par O. Son image $\Gamma' = f(\Gamma)$ est un cercle homothétique de Γ dans une homothétie de centre O. En effet, quand M décrit Γ, $\overline{OM}\,\overline{OM_1} = \overline{OH}^2 - \overline{HM}^2 = \overline{OI}^2 - r^2 = p$. Comme $\overline{OM}\,\overline{OM'} = k$, on a $\overline{OM'} = \frac{k}{p}\,\overline{OM_1}$. Analytiquement, l'utilisation des relations (1) donne aussi ce résultat.



c) On a $\overline{PA}\,\overline{PB} = \overline{PM}^2 = \overline{PI}^2 - \overline{IA}^2$ (puissance de P par rapport au cercle) donc $(x+a)(x-a) = y^2$. Ainsi, quand C décrit le faisceau, M et N varient sur l'hyperbole équilatère H d'équation :

$$x^2 - y^2 = a^2. \tag{2}$$

Tout point de H est obtenu quand C décrit le faisceau $\mathcal{F}$ car l'ordonnée y de I, M, N décrit tout $\mathbb{R}$.



d) Substituons $x = \dfrac{a^2X}{X^2+Y^2}$ et $y = \dfrac{a^2Y}{X^2+Y^2}$ dans l'équation (2) de H. On obtient l'équation de l'inverse L de H, appelée *lemniscate de Bernoulli* (privée de O) :

$$(X^2+Y^2)^2 - a^2(X^2-Y^2) = 0\,.$$

Paramétrons l'hyperbole H. On en déduira un paramétrage de L. Coupons H par des droites d'équation $y = -x+t$, où $t \neq 0$, parallèles à une asymptote. Un point d'intersection est rejeté à l'infini. On a donc un seul point d'intersection M avec H. Son abscisse vérifie $x^2-(-x+t)^2 = a^2$, d'où ses coordonnées x et $y = -x+t$:

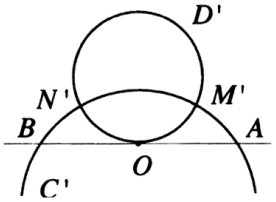
$$x = \frac{t^2+a^2}{2t} \qquad , \qquad y = \frac{t^2-a^2}{2t}\cdot$$

De ce paramétrage rationnel de H on déduit en utilisant (1), un paramétrage de L,

$$X = a^2\,\frac{t(t^2+a^2)}{t^4+a^4} \qquad , \qquad Y = a^2\,\frac{t(t^2-a^2)}{t^4+a^4}\cdot$$

Pour obtenir une définition géométrique de L, il suffit d'examiner la figure inverse de celle qui définissait H. L'image du cercle C est un cercle C' passant par A et B (invariants dans l'inversion). L'image de la droite D est un cercle D' tangent en O à l'axe des abscisses et orthogonal à C'.

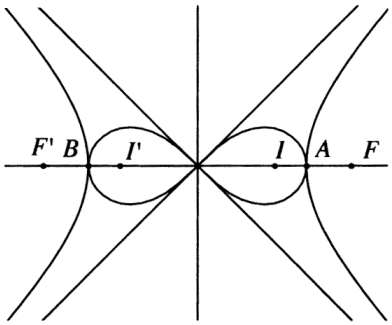
Ainsi, L est l'ensemble des points communs M' et N' à deux cercles C' et D' qui varient en restant orthogonaux entre eux, l'un décrivant le faisceau à points de base A et B, l'autre le faisceau des cercles tangents à $(x'x)$ en O.



Quitte à changer l'unité de longueur, on peut supposer que $a = 1$. Les foyers F et F' de H ont pour abscisses $\sqrt{2}$ et $-\sqrt{2}$. Soient I et I' les inverses de F et F'.

$$\begin{aligned} z \in L \;&\Leftrightarrow\; \tfrac{1}{\bar z} \in H \;\Leftrightarrow\; \tfrac{1}{z} \in H \;\Leftrightarrow\; |\,|\tfrac{1}{z}+\sqrt{2}\,| - |\tfrac{1}{z}-\sqrt{2}\,|\,| = 2 \\ &\Leftrightarrow\; |1+\sqrt{2}\,z\,|^2 + |1-\sqrt{2}\,z\,|^2 - 2\,|1+\sqrt{2}\,z\,|\,|1-\sqrt{2}\,z\,| = 4|z|^2 \\ &\Leftrightarrow\; 2+4|z|^2-4|\tfrac{1}{\sqrt{2}}+z\,|\,|\tfrac{1}{\sqrt{2}}-z\,| = 4|z|^2 \\ &\Leftrightarrow\; |z+\tfrac{1}{\sqrt{2}}\,|\,|z-\tfrac{1}{\sqrt{2}}\,| = \tfrac{1}{2}\,. \end{aligned}$$

Ainsi, L est l'ensemble des points M' du plan tels que le produit des distances aux points I et I' est constant. C'est la définition classique de la famille des ovales de Cassini, dont la lemniscate fait partie. On notera que si M tend vers l'infini sur H, dans une direction asymptotique $y = x$ ou $y = -x$, son image $M' \in L$ tend vers O dans cette même direction, ce qui donne les tangentes en O à L (en prolongeant par continuité la courbe en O).

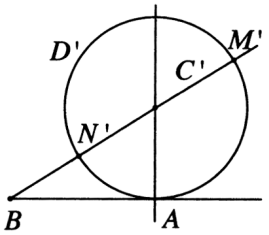


e) Plaçons l'origine en A. L'équation de H devient

$$(x+a)^2 - y^2 = a^2 \qquad \text{soit} \qquad x^2+2ax-y^2 = 0\,.$$

La courbe image S dans l'inversion de puissance $4a^2$ a pour équation

$$X(X^2+Y^2) - 2a\,(Y^2-X^2) = 0\,.$$



On l'appelle la *strophoïde droite*. Le cercle C et la droite D de la définition de H deviennent une droite C' issue de B et le cercle D' tangent en A à l'axe $(x'x)$. Ces deux courbes varient en restant orthogonales entre elles, autrement dit, le cercle D' est centré sur la droite C'. C'est la génération classique de la strophoïde S.

Par la même méthode, le lecteur peut étudier l'inverse par rapport à O de la parabole P d'équation $y^2 - 2px = 0$ (privée de O). C'est la *cissoïde*. Elle présente en O un point de rebroussement qui dans l'inversion correspond aux branches infinies de P de direction horizontale. Elle admet une direction asymptotique verticale, due au fait que la parabole a une tangente verticale en O.

Quant aux images par une inversion de centre O, de toutes les coniques de foyer O, c'est la famille des limaçons de Pascal (conchoïdes de cercles). C'est évident si on donne les coniques par leur équation polaire $\rho = \frac{p}{1+e\cos(\theta-\theta_0)}$. Les courbes inverses ont une équation de la forme $\rho = a\cos(\theta-\theta_0)+b$. Les paraboles de foyer O ont pour images les cardioïdes de point de rebroussement en O (les demi-tangentes correspondent aux branches infinies de la parabole).

Ex 8 - 2

Prenons pour origine du plan $\mathcal{E}_2$ l'isobarycentre O des sommets de P. Choisissons l'axe $x'x$ et l'unité de longueur de façon à avoir $\overrightarrow{OA_0}$ unitaire. En identifiant $\mathcal{E}_2$ avec le plan complexe, les sommets de P sont les points d'affixes $1, \zeta, \ldots, \zeta^{n-1}$, où $\zeta = \exp(2i\pi/n)$. D'après 7-9, cor., D_n est un sous-groupe du groupe des isomorphismes affines de $\mathcal{E}_2$. Tout $f \in D_n$ induit une permutation s_f des sommets de D_n et $f \mapsto s_f$ est un homomorphisme injectif du groupe D_n dans $\mathcal{S}_n$. Donc D_n est fini. En outre, tout $f \in D_n$ laisse fixe l'isobarycentre O des sommets de D_n.

Alors, $A_i = f(A_0)$, $A_j = f(A_1)$, $A_k = f(A_{n-1})$ sont des sommets de P. Comme f est affine bijective, c'est un homéomorphisme de $\mathcal{E}_2$. Elle applique la frontière de P sur la frontière de P. Ainsi, les segments $f([A_0A_1]) = [A_iA_j]$, $f([A_0A_{n-1}]) = [A_iA_k]$ sont nécessairement les deux arêtes de P issues de A_i. D'après 8-6, prop., il existe une isométrie unique appliquant le triangle $A_0A_1A_{n-1}$ sur le triangle $A_iA_jA_k$. Cette application affine est égale à f car elles ont les mêmes valeurs sur le repère affine $A_0A_1A_{n-1}$. Ainsi, tout $f \in D_n$ est une isométrie.

Soit $f \in D_n$ tel que $f(A_0) = A_0$. Comme f est un homéomorphisme, il applique le segment $[A_0A_1]$ de la frontière de P sur un autre segment reliant A_0 à un autre sommet et sans point à l'intérieur de D_n. Ce ne peut être que $[A_0A_1]$ ou $[A_0A_{n-1}]$. La symétrie orthogonale s par rapport à $(x'x)$ et $\mathrm{Id}_{\mathcal{E}_2}$ sont des éléments de D_n qui fixent A_0 et appliquent A_1 sur A_{n-1} ou A_1. Ce sont les seuls car en donnant l'image du repère affine (O, A_0, A_1) on détermine, de manière unique, une application affine. Ainsi, le stabilisateur de A_0 est $K = \{\mathrm{Id}_{\mathcal{E}_2}, s\}$. L'orbite de A_0 est l'ensemble des n sommets. En effet, la symétrie orthogonale par rapport à la médiatrice de $[A_iA_{i+1}]$ est un élément de D_n qui applique A_i sur A_{i+1}. Par composition de telles symétries, on peut donc appliquer A_0 sur tout autre sommet. Puisque $n = \mathrm{card}(\mathrm{orb}(A_0)) = \frac{[D_n:1]}{[K:1]}$, on en déduit que $[D_n : 1] = 2n$. Il existe $2n$ éléments évidents de D_n : les n rotations éléments du

groupe cyclique $H = \{\mathrm{Id}_{\mathcal{E}_2}, r, \ldots, r^{n-1}\}$, où $r = r_{O,2\pi/n}$ et les isométries indirectes $s, sr, \ldots, sr^{n-1}$ qui sont des symétries car elles laissent O fixe. Ce sont donc les $2n$ éléments de D_n. Si n est impair, les symétries précédentes sont les n symétries par rapport aux médiatrices des côtés (qui sont aussi les bissectrices des angles aux sommets). Si n est pair, on a $\frac{n}{2}$ symétries par rapport aux médiatrices et $\frac{n}{2}$ symétries par rapport aux bissectrices. Ainsi, $D_n = \{\mathrm{Id}_{\mathcal{E}_2}, r, \ldots, r^{n-1}, s, sr, \ldots, sr^{n-1}\}$ est engendré par r et s et on a $o(r) = n$, $s^2 = \mathrm{Id}_{\mathcal{E}_2}$, $(sr)^2 = \mathrm{Id}_{\mathcal{E}_2}$.

Ex 8 - 3

Les éléments du groupe $G = \langle a, b\rangle$, sont e et les mots $x_1 \cdots x_l$, où $l \in \mathbb{N}^*$ et $x_i \in \{a, b, a^{-1}, b^{-1}\}$ pour $i = 1, \ldots, l$. Puisque $a^n = e$ et $b^2 = e$, on a $a^{-1} = a^{n-1}$ et $b^{-1} = b$. Tout élément de G peut donc s'écrire $x = x_1 \cdots x_k$ où $k \in N^*$ et $x_1, \ldots, x_k \in \{a, b\}$. Montrons, par récurrence sur k, que $x = a^m$ ou que $x = a^m b$, avec $0 \leqslant m \leqslant n-1$. Pour $k = 1$, c'est évident. Soit $k > 1$. Supposons cette propriété vraie à l'ordre $k-1$ et considérons $x = x_1 \cdots x_k = (x_1 \cdots x_{k-1})x_k$. D'après l'hypothèse de récurrence, $x_1 \cdots x_{k-1}$ s'écrit a^m ou $a^m b$. Si $x_k = b$, on obtient $x = a^m b$ ou a^m. Si $x_k = a$, on a $x = a^{m+1}$ ou $a^m ba$. Or, on a $abab = e$ et donc $ba = a^{-1}b^{-1} = a^{n-1}b$ et donc $a^m ba = a^{m+n-1}b$. En remplaçant l'exposant de a par le reste de la division par n, on voit que dans tous les cas $x = x_1 \cdots x_k$, de la forme annoncée.

Soient $H = \{e, a, \ldots, a^{n-1}\}$ et $K = \{e, b\}$ les sous-groupes de G engendrés par a et par b. Le groupe G n'est pas commutatif (sinon on aurait $e = abab = a^2b^2 = a^2$ contredisant $o(a) = n \geqslant 3$). Donc $b \neq H$ et $H \cap K = \{e\}$. Dans $G = H \cup Hb$, le sous-groupe H est d'indice 2. Il est donc distingué (1-8, cor.). On a $G = HK$ d'après ce qui précède. D'après 2-7, prop., G est isomorphe au produit direct $H \times_\varphi K$, où $\varphi \in \mathrm{Hom}(K, \mathrm{Aut}(H))$ est l'action de K sur H définie par $\varphi(e) = \mathrm{Id}_H$ et $\varphi(b) : a^k \mapsto ba^k b^{-1} = a^{-k}$ (puisque $b^2 = e$, $baba = e$ on a $bab^{-1} = a^{-1}$).

On sait que $\theta : \overline{k} \mapsto a^k$ est un isomorphisme de $\mathbb{Z}/n\mathbb{Z}$ sur le groupe cyclique H. De même, $\mathbb{Z}/2\mathbb{Z}$ est isomorphe à K. Ainsi le produit semi-direct $H \times_\varphi K$ est isomorphe à $\Gamma = (\mathbb{Z}/n\mathbb{Z}) \times_\alpha (\mathbb{Z}/2\mathbb{Z})$, où $\alpha \in \mathrm{Hom}(\mathbb{Z}/2\mathbb{Z}, \mathrm{Aut}(\mathbb{Z}/n\mathbb{Z}))$ est l'action définie par $\alpha(\overline{0}) = \mathrm{Id}$ et $\alpha(\overline{1}) : \overline{k} \mapsto -\overline{k}$. Cela montre que tous les groupes engendrés par deux éléments vérifiant (1) sont isomorphes à Γ. D'après l'exercice précédent, D_n vérifie ces conditions. Les conditions (1) caractérisent donc D_n à isomorphisme près.

Ex 8 - 4

Soit $A_1 \in \mathcal{E}_2$ et soit $\{A_1, \ldots, A_k\}$ son orbite sous l'action du groupe fini G. Tout $g \in G$ permute $A_1, \ldots, A_k$. Il laisse donc fixe l'isobarycentre O de ces points. Choisissons un repère orthonormé $(O, \vec{\imath}, \vec{\jmath})$ d'origine O et identifions $\mathcal{E}_2$ avec $\mathbb{C}$.

Supposons $G \subset \mathcal{I}^+$, d'ordre n. Tout $g \in G$ est une rotation de centre O, de la forme $z \mapsto e^{i\theta_g} z$. Ainsi, $\{e^{i\theta_g}\ ;\ g \in G\}$ est un sous-groupe fini du groupe $\mathbb{C}^*$. On a donc $G = \mathbb{U}_n \simeq \mathbb{Z}/n\mathbb{Z}$ (voir Ex. 3-6).

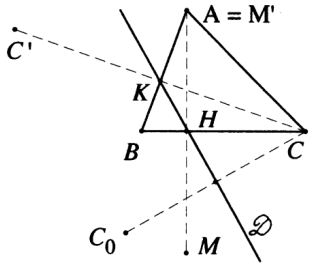
Si G contient un antidéplacement s, alors s qui laisse fixe O est une symétrie orthogonale par rapport à une droite $\mathcal{D}$ passant par O. Alors $G = G^+ \cup sG^+$, avec $G^+ = \{\mathrm{Id}_{\mathcal{E}_2}, r, \ldots, r^{n-1}\}$ cyclique d'après ce qui précède, engendré par une rotation r d'angle $2\pi/n$. Puisque rs est un antidéplacement qui a un point fixe O, c'est une symétrie orthogonale et donc $(rs)^2 = \mathrm{Id}_{\mathcal{E}_2}$. L'exercice précédent montre que $G \simeq D_n$.

Ex 8 - 5

$f = r_C \circ r_B \circ r_A$ est un déplacement. L'application linéaire associée v_f, composée de trois rotations vectorielles dont la somme des angles est π, est $v_f = -\mathrm{Id}$. Ainsi, f est une rotation d'angle π, c'est-à-dire une symétrie par rapport à un point.

Si ABC est équilatéral, on a $r_A(B) = C$, $r_B(C) = A$, $r_C(A) = B$ donc B est fixe par f et f est la symétrie par rapport au point B.

Puisque $g = s_{(AB)} \circ s_{(CA)} \circ s_{(BC)}$ est un antidéplacement, s'il avait un point fixe, g serait une symétrie orthogonale s_Δ par rapport à une droite Δ. Alors $s_{(CA)} \circ s_{(BC)}$ qui est une rotation de centre C, d'angle $2(\overrightarrow{CB}, \overrightarrow{CA}) \neq 0 \pmod{2\pi}$ serait égale à $s_{(AB)} \circ s_\Delta$ qui est une translation si $\Delta // (AB)$ ou une rotation de centre situé sur (AB) (et sur Δ). C'est impossible. Donc g est une symétrie glissée. Soit $g = t_{\vec{a}} \circ s_\mathcal{D}$ son expression canonique. Pour tout $M \in \mathcal{E}_2$, la droite $\mathcal{D}$ contient le milieu de $[MM']$, où $M' = g(M)$. Si on prend M symétrique de A par rapport à (BC), on voit que le pied H de la hauteur issue de A appartient à $\mathcal{D}$. Si on prend M au point C, le pied K de la hauteur issue de C appartient à $\mathcal{D}$. Si le triangle n'est pas rectangle en B, on a $H \neq K$ et $\mathcal{D}$ est la droite (HK). Le vecteur $\overrightarrow{a}$ est $\overrightarrow{C_0C'}$, où C_0 (resp. C') est le symétrique de C par rapport à la droite (HK) (resp. (AB)). C'est aussi $\overrightarrow{M_0A}$, où M_0 est le symétrique de M par rapport à (HK).



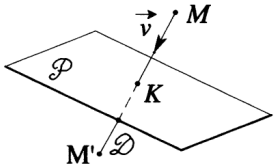
Si ABC est rectangle en B, alors $\mathcal{D}$ passe par B. Si $B' = g(B)$, alors $\overrightarrow{a} = \overrightarrow{BB'}$, donne la direction de $\mathcal{D}$.

Ex 8 - 6

Soient $\mathcal{D}, \mathcal{D}', \mathcal{D}''$ les droites issues du centre O du cercle C et orthogonales à $\Delta, \Delta', \Delta''$ respectivement. On a $M_1 = s_\mathcal{D}(M)$, $M_2 = s_{\mathcal{D}'}(M_1)$, $M_3 = s_{\mathcal{D}''}(M_2)$ donc $M_3 = f(M)$ où $f = s_{\mathcal{D}''} \circ s_{\mathcal{D}'} \circ s_\mathcal{D}$. Alors f est un antidéplacement et O est fixe par f donc f est une symétrie orthogonale par rapport à une droite $\mathcal{D}_0$. On a donc $M_6 = f^2(M) = M$. La suite (M_k) est périodique, avec période 6. Si M est un point d'intersection de C avec $\mathcal{D}_0$, on aura même $M_3 = M$ et la suite a pour période 3.

Ex 8 - 7

Le plan $\mathcal{P}$ a une équation de la forme $2x + y - z - m = 0$. Il passe par $B(2, 0, -2)$ donc $m = 6$. Les points de la droite $\mathcal{D}$ issue du point $M(x, y, z)$, dirigée par $\overrightarrow{v}$, ont des coordonnées de la forme suivante (paramétrage de la droite),



$$X = x + 2t \quad , \quad Y = y + t \quad , \quad Z = z - t\,.$$

Les coordonnées du point K où $\mathcal{D}$ rencontre $\mathcal{P}$, vérifient l'équation de $\mathcal{P}$, d'où la valeur du paramètre pour ce point : $t_0 = 1 - \frac{2}{6}x - \frac{1}{6}y + \frac{1}{6}z$. Le point M' symétrique de M est tel que $\overrightarrow{MM'} = 2\overrightarrow{MK} = 2t_0\overrightarrow{v}$, d'où $\overrightarrow{OM'} = \overrightarrow{OM} + 2t_0\overrightarrow{v}$ et

$$\left\{\begin{array}{rcrcrcl} x' & = & -\frac{1}{3}x & - & \frac{2}{3}y & + & \frac{2}{3}z + 4 \\ y' & = & -\frac{2}{3}x & + & \frac{2}{3}y & + & \frac{1}{3}z + 2 \\ z' & = & \frac{2}{3}x & + & \frac{1}{3}y & + & \frac{2}{3}z - 2 \end{array}\right. .$$

Ex 8 - 8

D'après 6-4, cor. 3, f est affine. Dans la base orthonormée $\mathcal{B} = (\vec{\imath}, \vec{\jmath}, \overrightarrow{k})$, la matrice A de l'application linéaire v_f est orthogonale donc f est une isométrie. En ajoutant à la première colonne les deux autres, on voit rapidement que $\det(A) = 1$ donc f est un déplacement. Comme $v_f \neq \mathrm{Id}$, f n'est pas une translation. C'est donc une rotation ou un vissage, autour d'un axe $\mathcal{D}$. Si on étudie l'équation $f(M) = M$, on peut voir que f n'a pas de point fixe. C'est donc un vissage. Ce qui suit le montrera également.

La recherche des vecteurs propres de v_f pour la valeur propre 1 donne la direction D de $\mathcal{D}$. C'est la droite vectorielle dont $\overrightarrow{w} = (\frac{1}{\sqrt{3}}, \frac{1}{\sqrt{3}}, \frac{1}{\sqrt{3}})$ est vecteur unitaire. Pour connaître l'angle θ, considérerons un vecteur du plan vectoriel P orthogonal à D, par exemple $\overrightarrow{u} = (\frac{1}{\sqrt{2}}, 0, -\frac{1}{\sqrt{2}})$. On a $\overrightarrow{u} \wedge v_f(\overrightarrow{u}) = \frac{\sqrt{3}}{2}\overrightarrow{w}$ donc $\sin\theta = \frac{\sqrt{3}}{2}$. Par ailleurs, A étant semblable à $\begin{pmatrix} 1 & 0 & 0 \\ 0 & \cos\theta & -\sin\theta \\ 0 & \sin\theta & \cos\theta \end{pmatrix}$, on a $1 + 2\cos\theta = \mathrm{tr}(A) = 2$ et donc $\cos\theta = \frac{1}{2}$. Ainsi, dans le plan vectoriel P orienté par $\overrightarrow{w}$, la mesure de θ est $\frac{\pi}{3}$.

Le vecteur $\overrightarrow{a} = (\alpha, \alpha, \alpha) \in D$ du vissage, est caractérisé par le fait que $t_{-\vec{a}} \circ f$ a des points fixes. Par exemple, la méthode du pivot de Gauss donne :

$$\begin{cases} x &= \frac{2}{3}x - \frac{1}{3}y + \frac{2}{3}z + 2 - \alpha \\ y &= \frac{2}{3}x + \frac{2}{3}y - \frac{1}{3}z - \alpha \\ z &= -\frac{1}{3}x + \frac{2}{3}y + \frac{2}{3}z + 1 - \alpha \end{cases} \Leftrightarrow \begin{cases} x + y - 2z &= 6 - 3\alpha \\ y - z &= 3\alpha \\ 0 &= -1 + \alpha \end{cases}$$

Le système n'a de solution que si $\alpha = 1$. Il a alors pour solutions $(x = z + 2\ ,\ y = z + 1\ ,\ z)$, où $z \in \mathbb{R}$, équation paramétrique de l'axe du vissage. Comme $\alpha = 1$, on obtient $\overrightarrow{a} = (1, 1, 1)$. L'expression canonique de f est $f = t_{\vec{a}} \circ r_{\mathcal{D},\pi/3}$.

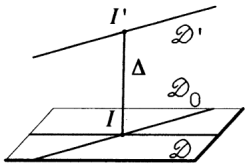
La matrice B de l'application linéaire v_g est orthogonale et symétrique. D'après 8-5, g est un symétrie orthogonale ou une symétrie glissée. Comme $\mathrm{tr}(B) = 1$, il existe une base orthonormée de $\mathbb{R}^3$ dans laquelle la matrice de v_g est $\begin{pmatrix} -1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$. Donc v_g est une symétrie vectorielle orthogonale par rapport à un plan P que l'on détermine en cherchant les vecteurs fixes. Le calcul montre que ce sous-espace propre à pour équation $x + 2y + 2z = 0$, d'où, en tirant x de cette relation, l'expression $y\overrightarrow{v} + z\overrightarrow{w}$, où $\overrightarrow{v} = (-2, 1, 0)$ et $\overrightarrow{w} = (-2, 0, 1)$, des vecteurs de P. Pour déterminer la décomposition canonique $g = t_{\vec{a}} \circ s$ de la symétrie glissée, on peut chercher $\overrightarrow{a} = \alpha\overrightarrow{v} + \beta\overrightarrow{w}$ dans P tel que $t_{-\vec{a}} \circ g$ ait des points fixes. L'ensemble des points fixes sera le plan $\mathcal{P}$ de la symétrie plane orthogonale s. En étudiant, par la méthode de Gauss, le système obtenu, on voit qu'il a des solutions si et seulement si $\alpha = -2$, $\beta = 2$. Dans ce cas, $\overrightarrow{a} = -2\overrightarrow{v} + 2\overrightarrow{w} = -2\vec{\jmath} + 2\overrightarrow{k}$. Ses solutions (x, y, z) donnent les éléments du plan $\mathcal{P}$ d'équation $x + 2y + 2z = 0$.

Si on veut éviter cette résolution de système, il suffit de se souvenir que pour tout $M \in \mathcal{E}$, l'image $M' = f(M)$ est telle que le milieu I de $[MM']$ appartient à $\mathcal{P}$. Par exemple, avec $M = O$ on obtient $I \in \mathcal{P}$ de coordonnées $(0, -1, 1)$, puis $I' = f(I)$ de coordonnées $(0, -3, 3)$, d'où le vecteur $\overrightarrow{a} = \overrightarrow{II'}$ de coordonnées $(0, -2, 2)$ de la translation. Si on calcule $t_{-\vec{a}} \circ f(0) = J$, alors le plan $\mathcal{P}$ est le plan médiateur de $[OJ]$, d'où son équation $x + 2y + 2z = 0$.

Ex 8 - 9

D'après 8-10, rem. 2, si $\mathcal{D}$ et $\mathcal{D}'$ sont parallèles, $g = f' \circ f$ est une translation $t_{2\vec{a}}$ où $\overrightarrow{a}$ donne la plus courte distance de $\mathcal{D}$ à $\mathcal{D}'$. Si $\mathcal{D}$ et $\mathcal{D}'$ sont concourantes en un point A, alors g est la rotation autour de la droite perpendiculaire en A au plan de $\mathcal{D}$ et $\mathcal{D}'$, d'angle $2(\mathcal{D}, \mathcal{D}')$. (L'angle $(\mathcal{D}, \mathcal{D}')$ est défini modulo π et $2(\mathcal{D}, \mathcal{D}')$ modulo 2π.)

Considérons le cas où $\mathcal{D}$ et $\mathcal{D}'$ ne sont pas coplanaires. Soient Δ la perpendiculaire commune à $\mathcal{D}$ et $\mathcal{D}'$ et I et I' les points d'intersection de Δ avec $\mathcal{D}$ et $\mathcal{D}'$. Soit $\mathcal{D}_0$ la droite parallèle à $\mathcal{D}'$ issue de I. Alors $g = s_{\mathcal{D}'} \circ s_{\mathcal{D}} = s_{\mathcal{D}'} \circ s_{\mathcal{D}_0} \circ s_{\mathcal{D}_0} \circ s_{\mathcal{D}} = t_{\vec{a}} \circ r_{\Delta,\theta}$, où $\overrightarrow{a} = 2\overrightarrow{II'}$ et $\theta = 2(\mathcal{D}, \mathcal{D}_0)$. Comme $\overrightarrow{a}$ appartient à la direction de l'axe Δ de la rotation $r_{\Delta,\theta}$, c'est l'expression canonique d'un vissage.

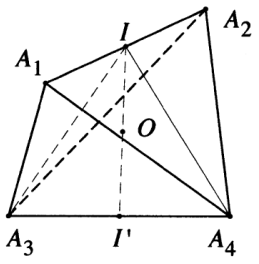


Ex 8 - 10

a) L'ensemble $\{A_1, A_2, A_3, A_4\}$ des sommets de T est un repère affine de $\mathcal{E}_3$. D'après 7-9, cor., G est un sous-groupe de $\mathrm{Aut}(\mathcal{E}_3)$. Tout $f \in G$ laisse stable l'ensemble $\{A_1, A_2, A_3, A_4\}$ des sommets de T. Il induit une permutation s_f de ces sommets et $\varphi : f \mapsto s_f$ est un homomorphisme de groupes injectif de G dans $\mathcal{S}_4$. Comme T est régulier, d'après 8-6, prop. pour toute permutation $s \in \mathcal{S}_4$ des sommets, il existe une isométrie g, unique telle que $s_g = s$. Cela montre que φ est surjective et que tout $f \in G$ est une isométrie. Ainsi G est un sous-groupe de $\mathcal{I}$, isomorphe à $\mathcal{S}_4$.

Soit $f \in G$. Alors s_f est un produit de transpositions $s_f = t_1 \cdots t_k$. Si $t_1 = [i, j]$. L'élément de $\varphi^{-1}(t_1) \in G$ correspondant est la symétrie orthogonale hyperplane $s_1 = s_{ij}$ par rapport au plan médiateur de $[A_i, A_j]$. C'est un antidéplacement. De même, $t_2, \ldots, t_k$ correspondent par φ à des symétries orthogonales hyperplanes $s_2, \ldots, s_k$. Puisque $\varphi(f) = t_1 \cdots t_k$, on a $f = s_1 \cdots s_k$. C' est un déplacement si et seulement si k est pair, c'est-à-dire si $s_f = t_1 \cdots t_k$ est une permutation paire.

b) f telle que $s_f = [1,2][3,4]$ est la composée $s \circ s'$ des symétries orthogonales s, s' par rapport aux plans médiateurs $\mathcal{P}$ et $\mathcal{P}'$ de $[A_1A_2]$ et $[A_3A_4]$. Comme $\mathcal{P}$ contient A_3 et A_4, les droites (A_1A_2) et (A_3A_4) sont orthogonales. Les plans $\mathcal{P}$ et $\mathcal{P}'$ qui ont pour vecteurs normaux $\overrightarrow{A_1A_2}$ et $\overrightarrow{A_3A_4}$ sont donc perpendiculaires, d'intersection la droite reliant les milieux I et I' de $[A_1A_2]$ et $[A_3A_4]$. La composée $s \circ s'$ est donc la rotation $r_{(II')}$ autour de (II') d'angle π, c'est-à-dire le demi-tour autour de (II').



De même, $[1,3][2,4]$ et $[1,4][2,3]$ sont associés aux demi-tours $r_{(JJ')}$ et $r_{(KK')}$ autour des droites (JJ') et (KK') reliant les milieux des arêtes $[A_1A_3]$, $[A_2A_4]$ et $[A_1A_4]$, $[A_2A_3]$. La restriction de $\mathrm{Id}_{\mathcal{E}_3}$ est Id. Ces quatre permutations constituent un sous-groupe distingué H de $\mathcal{S}_4$, isomorphe au petit groupe de Klein. Par l'isomorphisme φ, il est associé à un sous-groupe distingué de G. On a $r_{(II')} \circ r_{(JJ')} = r_{(KK')}$, conformément à la table de multiplication dans le groupe de Klein (Ex 1-4). La composée de deux demi-tours par rapport aux droites (II') et (JJ') concourantes en O est la rotation autour de la droite perpendiculaire en O au plan

des deux droites, d'angle double de l'angle des droites (8-10, rem.). Cette composée étant un demi-tour, l'angle des deux droites est $\frac{\pi}{2}$. Les droites (II'), (JJ'), (KK') sont donc perpendiculaires deux à deux.

c) Si $o(f) = 2$, alors $H = \{\mathrm{Id}, f\}$ est un sous-groupe de G. Pour son action sur les sommets, une orbite a pour cardinal $\mathrm{card}\,(\mathrm{orb}(A_i)) = \frac{[H:1]}{[H_{A_i}:1]} = 1$ ou 2. Si on a une orbite $\{A_i, A_j\}$ à deux éléments, les autres sommets étant fixes, alors f est la symétrie orthogonale s_{ij} par rapport au plan médiateur de $[A_iA_j]$. Si on a deux orbites à deux éléments $\{A_i, A_j\}$ et $\{A_k, A_l\}$, alors $s_f = [i,j]\,[k,l]$ et f est le demi-tour par rapport à la droite reliant les milieux des arêtes $[A_iA_j]$ et $[A_kA_l]$. Ainsi, les seuls éléments d'ordre 2 de G sont ceux que nous avons déjà rencontrés.

d) Si f laisse fixe A_1, alors s_f permute $\{A_2, A_3, A_4\}$. Le stabilisateur G_1 de A_1 a au plus $[\mathcal{S}_3 : 1] = 6!$ éléments. Or, on connaît 6 éléments de G_1. En effet, en notant B_1 l'isobarycentre de A_2, A_3, A_4, la perpendiculaire au plan $(A_2A_3A_4)$, issue de A_1 est (A_1B_1). Alors, Id, $r = r_{(A_1B_1),2\pi/3}$, r^2 sont des éléments de G_1 ainsi que les symétries planes s_{23}, s_{34}, s_{42}. Donc G_1 est isomorphe à $\mathcal{S}_3$.

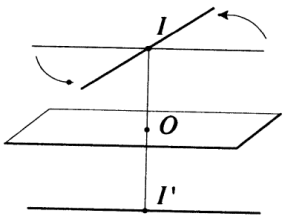
Comme l'action de G sur $E = \{A_1, A_2, A_3, A_4\}$ est transitive, les stabilisateurs des sommets sont conjugués dans G (2-2, prop. (iii)).

Soit H un sous-groupe d'ordre 3 de G. Les orbites pour son action sur E ont un cardinal diviseur de $[H : 1]$ et donc égal à 1 ou 3. Comme $G \neq \{\mathrm{Id}\}$, il existe une orbite $\{A_j, A_k, A_l\}$ à 3 éléments et un point fixe A_i. On a donc $H \subset G_i$ et d'après e), $H = \{\mathrm{Id}, r, r^2\}$, unique sous-groupe d'ordre 3 de $G_i \simeq \mathcal{S}_3$. Les éléments d'ordre 3 de G sont donc les rotations $r_{(A_iB_i),\pm 2\pi/3}$ déjà rencontrées.

e) $G^+ = G \cap \mathcal{I}^+$ est un sous-groupe distingué de G car $\mathcal{I}^+ \triangleleft \mathcal{T}$. Soit $s \in G$ une symétrie plane orthogonale. Alors la classe à gauche $sG^+ = G^-$ de G est équipotente à G^+ et c'est l'ensemble des antidéplacements de G. On a donc $\frac{1}{2}\,4! = 12$ déplacements et 12 antidéplacements dans G. On connaît les 12 déplacements : les 4×2 rotations $r_{(A_iB_i),\pm 2\pi/3}$, les 3 demi-tours $r_{(II')}, r_{(JJ')}, r_{(KK')}$ et Id.

Dans G^- il existe 6 symétries planes orthogonales par rapport aux plans médiateurs des arêtes. Les autres éléments de G^- laissent fixent l'isobarycentre O de T. Ce sont des symétrie-rotation, d'angle $\pi/2$.

Soit $s_{\mathcal{H}}$ la symétrie orthogonale par rapport au plan médiateur $\mathcal{H}$ de $[I, I']$. Alors on a deux symétries-rotations $r_{(II'),\pi/2} \circ s_{\mathcal{H}}$ et $r_{(II'),-\pi/2} \circ s_{\mathcal{H}}$ de G^-. Il existe aussi quatre symétries-rotations associées aux axes (JJ') et (KK'), d'où les 12 éléments de G^-.



Ex 8 - 11

a) D'après 7-9, cor., tout $f \in G$ est un automorphisme affine de $\mathcal{E}_3$. Il laisse invariant l'ensemble des sommets de Γ. Il induit une permutation s_f des sommets et $f \mapsto s_f$ est un homomorphisme injectif de G dans $\mathcal{S}_8$. Prenons la longueur du côté comme unité de longueur. Alors, $(A, \overrightarrow{AB}, \overrightarrow{AD}, \overrightarrow{AA'})$ est un repère orthonormé. Par l'isomorphisme affine f, l'image du plan $\mathcal{P}$ d'une face comme $ABCD$ est un plan qui contient les sommets images. Comme Γ est contenu dans l'un des demi-espaces délimité par $\mathcal{P}$, de même $f(\Gamma) = \Gamma$ est contenu dans l'un des demi-espaces délimités par l'image de $\mathcal{P}$. Ainsi, l'image d'une face de Γ est une autre face de Γ. On en déduit que f applique le repère $(A, \overrightarrow{AB}, \overrightarrow{AD}, \overrightarrow{AA'})$ sur un repère analogue d'origine $f(A)$, c'est-à-dire sur un repère orthonormé. Donc f est une isométrie de $\mathcal{E}_3$.

Soit $f \in G_A$. D'après ce qui précède, l'image du repère $\mathcal{R} = (\mathcal{A}, \overrightarrow{AB}, \overrightarrow{AD}, \overrightarrow{AA'})$ est un autre repère issu du sommet A dont les vecteurs sont une permutation de $\overrightarrow{AB}, \overrightarrow{AD}, \overrightarrow{AA'}$. Réciproquement, pour tout repère $\mathcal{R}'$ de ce type, il existe une isométrie f de $\mathcal{E}_3$ unique telle que $f(\mathcal{R}) = \mathcal{R}'$. Comme f est affine, elle conserve le parallélisme et applique donc le cube Γ sur lui-même. Ainsi G_A est d'ordre $3! = 6$. On connaît 6 éléments de G_A (et donc tous les éléments de G_A), à savoir Id, les symétries planes orthogonales par rapport aux 3 plans analogues au plan $(\overrightarrow{AA'}, \overrightarrow{AC})$, les composées de deux telles symétries qui sont deux rotations r, r^2 d'axe (AC) et d'angles $\frac{2\pi}{3}$ et $\frac{4\pi}{3}$. Comme tout $f \in G$ laisse fixe l'isobarycentre O de l'ensemble des sommets, s'il laisse fixe un sommet, il laisse fixe le sommet symétrique par rapport à O et tout point de la droite qui les joint (grande diagonale du cube). Les stabilisateurs de deux sommets opposés sont donc égaux.

L'action de G sur l'ensemble E des sommets est transitive : la symétrie orthogonale par rapport au plan médiateur d'une arête, par exemple $[AB]$, applique A sur B. Comme l'ensemble des arêtes est un graphe connexe, en composant diverses symétries on peut appliquer le sommet A sur tout autre sommet. L'orbite de A est E, d'où

$$8 = \mathrm{card}\,(E) = \frac{[G:1]}{[G_A:1]} = \frac{[G:1]}{6} \quad \text{et} \quad [G:1] = 48.$$

b) Dans l'action de H, d'ordre 3, sur E, les orbites sont d'ordre 1 ou 3 et constituent une partition de E. Si tous les sommets étaient fixes par H, alors H serait réduit à $\{\mathrm{Id}\}$, ce qui n'est pas le cas. Dans E (de cardinal 8), il existe donc une orbite à 3 éléments et 5 points fixes ou bien 2 orbites à 3 éléments et 2 points fixes. Ainsi, H laisse fixes au moins deux sommets et d'après ce qui précède, laisse fixes deux sommets opposés. Si, par exemple, ces sommets sont A et C', on a $H \subset G_A \simeq \mathcal{S}_3$ et H est l'unique sous-groupe d'ordre 3 de G_A, soit $\{\mathrm{Id}, r, r^2\}$. Les éléments d'ordre 3 de G sont les 8 rotations d'angle $\pm\frac{2\pi}{3}$ d'axes l'une des 4 grandes diagonales du cube. Il y a 4 sous-groupes d'ordre 3. C'est conforme aux th. de Sylow : $[G:1] = 48 = 2^4 \times 3$ donc le nombre de 3-sous-groupes de Sylow doit diviser 2^4 et être congru à 1 modulo 3, ce qui laisse comme possibilités 4 ou 16.

c) Soit $f \in G$. Comme $f \circ r_{(AC'),2\pi/3} \circ f^{-1}$ est un autre élément d'ordre 3 de G, c'est une rotation autour d'une des grandes diagonales de Γ. C'est aussi la rotation d'angle $2\pi/3$ autour de $f(AC')$. Donc f applique toute grande diagonale de Γ sur une autre grande diagonale. Comme il en est de même pour f^{-1}, on voit que f définit une permutation σ_f des grandes diagonales. Deux de ces diagonales, par exemple $[AC'], [BD']$, passent par le centre O et définissent un plan. La symétrie orthogonale par rapport à ce plan échange les deux autres diagonales ($[CA'], [DB']$

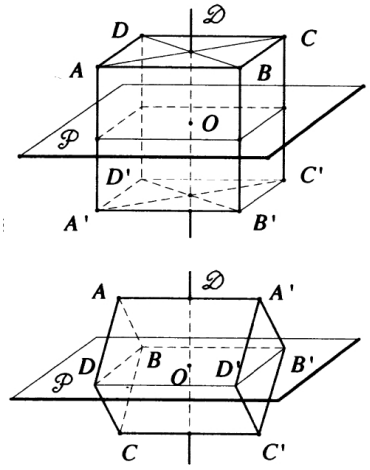
dans notre exemple). Donc toute transposition de $\mathcal{S}_4$ est dans l'image de $\varphi : f \mapsto \sigma_f$.

Les transpositions engendrent $\mathcal{S}_4$ donc $\varphi(G) = \mathcal{S}_4$. Par factorisation de φ, on obtient un isomorphisme $\overline{\varphi}$ de $G/\mathrm{Ker}\,(\varphi)$ sur $\mathcal{S}_4$ donc $[G : \mathrm{Ker}\,(\varphi)] = [\mathcal{S}_4 : 1] = 24$ et $[\mathrm{Ker}\,(\varphi) : 1] = 2$. Or, $\mathrm{Ker}\,(\varphi)$ contient Id et la symétrie s_O par rapport au centre du cube. Donc $\mathrm{Ker}\,(\varphi) = \{\mathrm{Id}, s_O\}$. De plus, tout élément f du centre $Z(G)$ de G est tel que $f \circ r_{(AC'),2\pi/3} \circ f^{-1} = r_{(AC'),2\pi/3}$ donc f laisse invariante la droite (AC'). Il en est de même des autres grandes diagonales, ce qui montre que $Z(G) \subset \mathrm{Ker}\,(\varphi)$. Par ailleurs, $s_O \in Z(G)$ car dans un repère orthonormé $(O, \vec{\imath}, \vec{\jmath}, \vec{k})$ d'origine O, l'application linéaire associée à s_O a pour matrice $-\mathrm{Id}_{\mathcal{E}_3}$ élément du centre de $\mathrm{GL}(3,\mathbb{R})$. Donc $Z(G) = \{\mathrm{Id}, s_O\} = \mathrm{Ker}\,(\varphi)$.

d) Le groupe $\mathcal{I}^+$ des déplacements est distingué dans $\mathcal{I}$ donc $G^+ = G \cap \mathcal{I}^+$ est distingué dans G. On a $G \cap \mathcal{I}^- = G^- = s_O G^+$ car $s_O \in G^-$ et $s_O^2 = \mathrm{Id}$. Chacune des classes à gauche G^+ et $s_O G^+$ possède donc $\frac{1}{2}[G : 1] = 24$ éléments. On a $\mathrm{Ker}\,(\varphi) \cap G^+ = \{\mathrm{Id}\}$ car $s_O \in G^-$ La restriction de φ à G^+ est donc un homomorphisme injectif de G^+ dans $\mathcal{S}_4$ et $[\varphi(G^+) : 1] = 24 = [\mathcal{S}_4 : 1]$. Donc $\varphi(G^+) = \mathcal{S}_4$ et G^+ est isomorphe à $\mathcal{S}_4$. Les sous-groupes $Z(G) = \{\mathrm{Id}, s_O\}$ et G^+ sont distingués, d'intersection $\{\mathrm{Id}\}$, d'ordres 2 et 24 donc on a $G = G^+ \times Z(G) \simeq \mathcal{S}_4 \times \mathbb{Z}/2\mathbb{Z}$.

e) Notons $\mathcal{P}$ le plan "horizontal" issu du centre O du cube et $\mathcal{D}$ la droite "verticale" issue de O. Si $s_{\mathcal{P}}$ est la symétrie orthogonale par rapport à $\mathcal{P}$ et $r_{\mathcal{D}}$ est le demi-tour d'axe $\mathcal{D}$, alors $s_{\mathcal{P}} \circ r_{\mathcal{D}} = r_{\mathcal{D}} \circ s_{\mathcal{P}}$ est la symétrie par rapport au point O.

Posons le cube sur une face. Il apparaît un groupe cyclique d'ordre 4 de déplacements $\{\mathrm{Id}, r, r^2, r^3\}$, où $r = r_{\mathcal{D},\pi/2}$. Composons avec $s_{\mathcal{P}}$. On obtient les antidéplacements
$\{s_{\mathcal{P}}, s_{\mathcal{P}} \circ r = r \circ s_{\mathcal{P}}, s_O, s_{\mathcal{P}} \circ r^3 = r^3 \circ s_{\mathcal{P}}\}$.
On a 3 couples de faces opposées, d'où 10 déplacements (Id, 3×3 rotations) et 10 antidéplacements (s_O, 3 symétries-plans , 3×2 symétries-rotations).



Posons le cube sur une arête. Il apparait un groupe d'ordre 2 de déplacements $\{\mathrm{Id}, r_{\mathcal{D}}\}$, d'où 6 nouveaux déplacements (demi-tours). Composons avec $s_{\mathcal{P}}$. On trouve $\{s_{\mathcal{P}}, s_O\}$, d'où 6 nouveaux antidéplacements (symétries planes).

Posons le cube sur un sommet C'. Les sommets B, D, A' et B', C, D' constituent des triangles équilatéraux symétriques par rapport à O (voir fig. p. 173). Il apparaît un groupe d'ordre 3 $\{\mathrm{Id}, r_{\mathcal{D},2\pi/3}, r_{\mathcal{D},4\pi/3}\}$ de déplacements. Il apparaît ainsi $8 = 4 \times 2$ nouveaux déplacements. En composant avec $s_{\mathcal{P}}$ et $r_{\mathcal{D},\pm\pi/6}$ on obtient 2 symétries-rotations (en composant $s_{\mathcal{P}}$ et $r_{\mathcal{D},\pi}$ on retrouve s_O déjà comptée), d'où $8 = 4 \times 2$ nouveaux antidéplacements.

Finalement, nous avons décrit 24 déplacements et 24 antidéplacements, c'est-à-dire les 48 éléments du groupe.

Troisième partie

ANNEAUX

Chapitre 9

Généralités sur les anneaux

9.1 Les objets de cette catégorie mathématique

Définition.

Un anneau est un ensemble A muni de deux lois de composition internes, une addition et un produit, vérifiant les conditions suivantes :

a) Muni de I'addition, A est un groupe commutatif, que nous noterons $(A,+)$.
b) Le produit est associatif et distribue I' addition, c'est-à-dire vérifie identiquement

$$(x+x')y = xy + x'y \quad , \quad x(y+y') = xy + yy' \ .$$

Si le produit admet un élément neutre (noté généralement 1), on dit que A est un anneau *avec unité* ou encore que A est *unifère*. Un élément $x$de A est appelé une *unité* de A, ou est dit *inversible*, s'il existe $y \in A$ tel que $xy = 1 = yx$. Cet inverse y de x est alors unique et noté x^{-1}. L'ensemble A_* des éléments inversibles de A est un groupe multiplicatif d'élément neutre 1. La plupart des anneaux considérés auront une unité.

L'anneau A est dit *intègre* si $A \neq 0$ et si la condition$xy = 0$ implique $x = 0$ ou $y = 0$ (tout $x \in A$ non nul est régulier pour le produit). Si A n'est pas intègre, il existe $x \neq 0$ et $y \neq 0$ tels que $xy = 0$. On dit alors que x, y sont des *diviseurs de zéro*.

Si le produit est commutatif, on dit que l'anneau A est *commutatif*.

Soit K un anneau commutatif unifère. On dit que l'anneau A est une *algèbre* sur K (ou que A est une K-algèbre) s'il existe une application $(\lambda, x) \mapsto \lambda x$ de $K \times A$ dans A vérifiant pour tout $\lambda \in K$, tout $x \in A$, tout $y \in A$,

$$\lambda(x+y) = \lambda x + \lambda y \quad , \quad \lambda(xy) = (\lambda x)y = x(/\lambda y).$$

Supposons A commutatif et unifère. Deux éléments a et b de A sont dits *associés* s'il existe $u \in A$, tel que $b = ua$. On définit ainsi une relation d'équivalence sur A.

Soit $x \in A$. Pour $n \in \mathbb{N}$, considérons la somme $nx = x + \cdots + x$ de n termes égaux à x. L'application $f_0 : n \mapsto nx$ de $\mathbb{N}$ dans le groupe $(A,+)$, est telle que $f_0(m+n) = f_0(m) + f_0(n)$ pour tout $m \in \mathbb{N}$ et tout $n \in \mathbb{N}$. La propriété universelle du groupe symétrisé $\mathbb{Z}$de $\mathbb{N}$, montre qu'il existe un homomorphisme f du groupe $\mathbb{Z}$dans le groupe additif $(A,+)$ prolongeant f_0 (1-12). Comme tout sous-groupe additif de $\mathbb{Z}$, le noyau de f est monogène, de la forme $\mathrm{Ker}\,(f) = p\mathbb{Z}$ où p est le générateur positif de ce sous-groupe (1-13, prop. 1). Si $p \neq 0$, c'est l'ordre de x dans $(A,+)$ (1-14, prop.).

Supposons A unifère et prenons $x = 1$. On appelle p la *caractéristique* de A. Nous la noterons $\mathrm{caract}(A)$. Pour $n \in \mathbb{Z}$, on notera n l'élément $n1$ de A. L'anneau A est de caractéristique zéro si f est injectif soit si : $\forall n \in \mathbb{Z}\ (n\,1 = 0 => n = 0)$.

Si f n'est pas injectif, p est le plus petit entier strictement positif tel que $p1 = 0$ (ordre de 1 dans le groupe additif $(A, +)$). On a $p \geqslant 2$ car $1 \neq 0$.

Si A est intègre et si $p \neq 0$ alors p est un nombre premier. En effet, si $p = qr$, avec $q, r \in \mathbb{N}$, la relation $0 = p1 = (q1)(r1)$ donne $q1 = 0$ ou $r1 = 0$. Alors p divise q ou p divise r. Comme $p = qr$ il en résulte $q = p$ ou $r = p$. Ainsi p est premier.

Soient $x, y \in A$ qui commutent (tels que $xy = yx$). Par récurrence sur $n \in \mathbb{N}^*$,

$$(x+y)^n = \sum_{k=0}^{n} C_n^k \, x^k \, y^{n-k} \qquad \text{(formule du binôme).}$$

Pour $1 \leqslant k \leqslant p-1$, l'entier $k!\, C_p^k = p(p-1)\cdots(p-k+1)$ est divisible par p. En effet, si p est premier, tous les diviseurs premiers de $k!$ sont strictement inférieurs à p donc p est premier avec $k!$ et p divise C_p^k. Il en résulte que dans un anneau A, commutatif, intègre, unifère, de caractéristique $p \neq 0$, si $x, y \in A$ commutent, on a

$$(x+y)^p = x^p + y^p \, .$$

Exemples.

a) $\mathbb{Z}$est un anneau commutatif, intègre, avec unité. Le groupe de ses unités est $\mathbb{Z}_* = \{1, -1\}$. Deux éléments de $\mathbb{Z}$sont associés s'ils sont égaux ou opposés.

b) Soit $n \in \mathbb{N}$, avec $n \geqslant 2$. Sur le groupe additif $\mathbb{Z}/n\mathbb{Z}$, il existe un produit défini par $\overline{x}\,\overline{y} = \overline{xy}$ qui en fait un anneau commutatif avec unité (voir 9-7). Sa caractéristique est n. Si $\mathbb{Z}/n\mathbb{Z}$ est intègre, n est premier. La réciproque est vraie (voir 9-11, cor. 1).

c) Le produit $A \times B$ de deux anneaux muni des opérations définies par

$$(a, b) + (a', b') = (a + a', b + b') \quad , \quad (a, b)(a', b') = (aa', bb'),$$

est un anneau. On l'appelle l'anneau produit de A et de B. Si A et B sont unifères, alors $(1, 1)$ est une unité de $A \times B$. Pour que $(u, v) \in A \times B$ soit inversible dans $A \times B$, il faut et il suffit que u et v le soient dans A et B respectivement. Le groupe des unités de $A \times B$ est donc $(A \times B)_* = A_* \times B_*$. Tout cela se généralise à un produit $\prod_{i \in I} A_i$ d'une famille d'anneaux. Comme cas particulier on obtient l'exemple suivant.

d) Soit X un ensemble. L'ensemble $\mathcal{F}(X, A) = A^X$ des applications de X dans l'anneau A est un anneau (avec unité si A est unifère) quand on définit l'addition et le produit de deux fonctions f, g par $(f+g)(x) = f(x) + g(x)$ et $(fg)(x) = f(x)g(x)$ où $x \in A$.

e) Soit C un groupe commutatif. On vérifiera que l'ensemble $\mathrm{End}\,(C)$ des endomorphismes du groupe C, muni de l'addition habituelle des applications et du produit de composition des applications, est un anneau unifère. Le groupe A_* des unités de l'anneau $\mathrm{End}\,(C)$ est le groupe $\mathrm{Aut}\,(C)$ des automorphismes du groupe C.

Par exemple, si C est le groupe additif $\mathbb{Z}$(resp. $\mathbb{Z}/n\mathbb{Z}$ où $n \geqslant 2$) alors $\mathrm{End}\,(C)$ est un anneau isomorphe à l'anneau $\mathbb{Z}$(resp. $\mathbb{Z}/n\mathbb{Z}$) et $\mathrm{Aut}\,(C)$ est isomorphe à $\mathbb{Z}_* = \{1, -1\}$ (resp. $(\mathbb{Z}/n\mathbb{Z})_* = \{k \mid 0 \leqslant k \leqslant n-1 \, , \; k \wedge n = 1\}$ (9-2, ex. 2).

Proposition.

Soient A un anneau commutatif unifère et $n \in \mathbb{N}^*$. L'ensemble $\mathcal{M}_n(A)$ des matrices carrées à coefficients dans A, muni de l'addition et du produit usuels est un anneau unifère. Pour $n \geqslant 2$, il n'est ni commutatif, ni intègre. Le groupe $\mathcal{M}_n(A)^*$ des unités de $\mathcal{M}_n(A)$ est l'ensemble $\mathrm{GL}(n, A)$ des matrices $M \in \mathcal{M}_n(A)$ dont le déterminant $\det(M)$ est inversible dans l'anneau A.

Démonstration. En identifiant $\mathcal{M}_n(A)$ avec A^{n^2}, l'addition de $\mathcal{M}_n(A)$ coïncide avec celle du groupe $A^{n^2} = A \times \cdots \times A$ (produit n^2 fois de $(A,+)$ par lui-même). Donc $\mathcal{M}_n(A)$ est un groupe additif. Comme dans le cas où A est un corps commutatif en algèbre linéaire, on vérifie que le produit des matrices est associatif, distribue l'addition, a pour élément neutre la matrice diagonale I_n, dont les termes diagonaux sont égaux à 1. En effet les vérifications de ces propriétés n'utilisent que l'associativité du produit de A et sa distributivité pour l'addition, propriétés valables dans l'anneau A.

Pour les mêmes raisons, $\det(MN) = \det(M)\det(N)$, pour tous $M, N \in \mathcal{M}_n(A)$. Si M est inversible dans $\mathcal{M}_n(A)$) on a donc $\det(M)\det(M^{-1}) = \det(I_n) = 1$ ce qui prouve que $\det(M)$ est inversible dans l'anneau A.

Toujours pour les raisons précédentes, la comatrice C_M de M, qui est la transposée de la matrice des déterminants mineurs de M affectés du signe donné par la règle de Sarrus, est telle que $M\,C_M = C_M\,M = \det(M)I_n$. Ainsi, si $\det(M)$ est inversible dans l'anneau A, alors M est inversible dans l'anneau $\mathcal{M}_n(A)$ d'inverse $\det(M)^{-1}\,C_M$ (matrice obtenue en multipliant tous les coefficients de C_M par $\det(M)^{-1}$).

Finalement, $M \in \mathcal{M}_n(A)$ est inversible si et seulement si $\det(M) \in A_*$.

Pour $n \geqslant 2$ cet anneau n'est ni commutatif, ni intègre. Par exemple pour $n = 2$,

$$\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}\begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \quad , \quad \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} .$$

$$\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} .$$

Corollaire.

Considérons un système de n équations linéaires dont les n inconnues $x_1, \cdots, x_n$ sont éléments de l'anneau commutatif unifère A. Si le déterminant $\det(M)$ de la matrice $M \in \mathcal{M}_n(A)$ du système est une unité de l'anneau A, alors les formules de Cramer sont applicables.

Démonstration. Puisque M est inversible, le système $MX = B$ est équivalent à $X = M^{-1}B$, avec $M^{-1} = (\det(M))^{-1}1C_M$. Cela conduit aux mêmes formules (de Cramer) que dans le cas où A est un corps commutatif.

Exercice1. On dispose de $n \geqslant 2$ billes b_i. Soit k un diviseur de $n-1$. Pour chaque bille b_i, on sait que si l'on retire b_i, les billes restantes peuvent être partagées en k lots de même masse, composés chacun de $s = \frac{n-1}{k}$ billes. Montrer que toutes les billes ont la même masse.

Solution. Pour $i = 1, \cdots, n$, notons x_i la masse de la bille b_i. Soit p la masse totale des n billes. On nous dit que pour $i = 1, \cdots n$, il existe un lot $x_{i_1}, \cdots x_{i_s}$, ne contenant pas x_i, de masse $\frac{1}{k}[\mu - x_i]$, d'où

$$kx_{i_1} + \cdots kx_{i_s} + x_i = \mu .$$

Ce système de n équations linéaires aux n inconnues $x_1, \cdots, x_n$, admet pour solution évidente $x_1 = \cdots = x_n = \frac{\mu}{n}$. Il suffit de vérifier que dans $\mathbb{R}$ ce système est de Cramer, c'est-à-dire que le déterminant $\det(M) = \sum_{s\in\mathcal{S}_n} \varepsilon(s)\, a_{1,s(1)} \cdots a_{n,s(n)}$ est non nul. Or $\sum_{s\in\mathcal{S}_n} \varepsilon(s)\overline{a}_{1,s(1)} \cdots \overline{a}_{n,s(n)}$, valeur modulo k de $\det(M)$, est le déterminant de la matrice $(\overline{a_{i,j}})$ qui est la matrice unité de $\mathcal{M}_n(\mathbb{Z}/k\mathbb{Z})$. La classe de $\det(M)$ dans $\mathbb{Z}/k\mathbb{Z}$ est $\overline{1} \neq \overline{0}$. On a donc $\det(M) \neq 0$.

Exercice 2. Résoudre dans $\mathbb{Z}$ le système $\begin{cases} 4x & + & 9y & \equiv & 4 & (\mathrm{mod}\,12) \\ 3x & + & 8y & \equiv & 7 & (\mathrm{mod}\,12) \end{cases}$.

Solution. Dans l'anneau $\mathbb{Z}/12\mathbb{Z}$, étudions le système $\begin{cases} \overline{4}\overline{x} & + & \overline{9}\overline{y} & = & \overline{4} \\ \overline{3}\overline{x} & + & \overline{8}\overline{y} & = & \overline{7} \end{cases}$.

$d = \begin{vmatrix} \overline{4} & \overline{9} \\ \overline{3} & \overline{8} \end{vmatrix} = \overline{5}$, est inversible, d'inverse $d^{-1} = \overline{5}$. Les formules de Cramer donnent,

$\overline{x} = d^{-1} = \begin{vmatrix} \overline{4} & \overline{9} \\ \overline{7} & \overline{8} \end{vmatrix} = \overline{5} \times (\overline{32} - \overline{63}) = \overline{1}$, $\overline{y} = d^{-1} = \begin{vmatrix} \overline{4} & \overline{4} \\ \overline{3} & \overline{7} \end{vmatrix} = \overline{5} \times \overline{4} \times (\overline{7} - \overline{3}) = \overline{8}$.

Les solutions du système sont $x = 1 + 12\,p$, $y = 8 + 12\,q$ où $p \in \mathbb{Z}$, $q \in \mathbb{Z}$.

9.2 Les morphismes dans cette catégorie mathématique

Définition.

Soient A et B deux anneaux. On appelle homomorphisme (ou morphisme) de A dans B une application f de A dans B qui conserve les deux lois de composition, c'est-à-dire vérifiant pour tout $x \in A$ et tout $y \in A$,

$$(1) \qquad f(x+y) = f(x) + f(y) \qquad , \qquad (2) \qquad f(xy) = fx)f(y)\ .$$

On note $\mathrm{Hom}(A, B)$ *l'ensemble des morphismes de l'anneau A dans l'anneau B.*

En particulier, tout $f \in \mathrm{Hom}\,(A, B)$ est un homomorphisme du groupe commutatif $(A, +)$ dans le groupe commutatif $(B, +)$. On a donc $f(0) = 0$ et $f(-x) = -f(x)$ pour tout $x \in A$. Le noyau $\mathrm{Ker}\,(f) = \{x \in A \mid f(x) = 0\}$ est un sous-groupe de $(A, +)$ et f est injectif si et seulement si $\mathrm{Ker}\,(f) = \{0\}$. D'après 1-6, lemme, pour toute partie non vide X de A, on a :

$$f^{-1}(f(X)) = X + \mathrm{Ker}\,(f)\ .$$

Si A et B sont unifères et si $f(1) = 1$, on aura $f(A_*) \subset B_*$.

Soient $A, B, \mathbb{C}$ des anneaux. Considérons $f \in \mathrm{Hom}\,(A, B)$, $g \in \mathrm{Hom}\,(B, \mathbb{C})$. Alors $g \circ f$ appartient à $\mathrm{Hom}\,(A, \mathbb{C})$.

Un homomorphisme de A dans A est appelé un *endomorphisme* de l'anneau A. On note $\mathrm{End}\,(A)$ l'ensemble des endomorphismes de l'anneau A.

Dans une catégorie mathématique donnée, on appelle isomorphisme d'un objet A de cette catégorie sur un autre objet B, un homomorphisme f de A vers B tel qu'il existe un homomorphisme g de B vers A vérifiant $g \circ f = \mathrm{Id}_A$ et $f \circ g = \mathrm{Id}_B$. Dans la catégorie des anneaux, cela signifie simplement que f est un homomorphisme bijectif de A sur B car alors $g = f^{-1}$ respectera les deux opérations et sera un homomorphisme de B sur A (pour le voir, appliquer $g = f^{-1}$ aux deux membres de (1) et (2)).

Un isomorphisme de A sur A est appelé un *automorphisme* de l'anneau A. L'ensemble $\mathrm{Aut}\,(A)$ des automorphismes de l'anneau A est un groupe pour l'opération de composition des applications, d'élément neutre Id_A.

Exercice 1. Dans $\mathcal{M}_2(\mathbb{R})$ soient $I_2 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ et $J = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$. Montrer que K$= \{xI_2 + yJ\,;\ x \in \mathbb{R},\ y \in \mathbb{R}\}$ est un anneau isomorphe à $\mathbb{C}$ (et un corps).

Solution. Associons à tout $z = x + iy \in \mathbb{C}$, l'application $f_z : z' \mapsto zz'$ de $\mathbb{C}$ dans $\mathbb{C}$. Identifions $\mathbb{C}$ avec $\mathbb{R}^2$. Alors $f_z : (x', y') \mapsto (xx' - yy', yx' + xy')$ est élément de $\mathcal{L}(\mathbb{R}^2)$ de matrice $M_z = \begin{pmatrix} x & -y \\ y & x \end{pmatrix} = xI_2 + yJ$ dans la base canonique. On a :

$$\forall z_1 \in \mathbb{C} \quad \forall z_2 \in \mathbb{C} \qquad f_{z_1+z_2} = f_{z_1} + f_{z_2} \qquad , \qquad f_{z_1 z_2} = f_{z_1}\, f_{z_2}$$

donc $\varphi : z \mapsto f_z$ est un homomorphisme d'anneaux et $\varphi(1) = f_1 = \mathrm{Id}_{\mathbb{C}}$. Il est injectif car $f_z = 0$ implique $0 = f_z(1) = z$. Les algèbres $\mathcal{L}(\mathbb{R}^2)$ et $\mathcal{M}_2(\mathbb{R})$ étant isomorphes, $z \mapsto M_z$ est un homomorphisme injectif de $\mathbb{C}$ dans K. Il est surjectif car tout $xI_2 + yJ \in K$ est égal à M_z, où $z = x + iy$.

Exercice 2. Soient A un anneau avec unité, $(A, +)$ le groupe additif de A.

a) Soit $a \in A$. Considérons $f_a : x \mapsto ax$. Montrer que $f_a \in \mathrm{End}\,(A, +)$ et que $\Phi : a \mapsto f_a$ est un homomorphisme d'anneaux, injectif, de A dans End $(A, +)$.

b) Si $A = \mathbb{Z}$ ou si $A = \mathbb{Z}/n\mathbb{Z}$, montrer que Φ est un isomorphisme d'anneaux. Déterminer le groupe des unités de l'anneau $B = \mathrm{End}\,(A, +)$.

Solution. a) Puisque A est un anneau, pour tout $x \in A$ et pour tout $y \in A$,

$$f_a(x + y) = a(x + y) = ax + ay = f_a(x) + f_a(y)\,.$$

Donc $f_a \in \mathrm{End}\,(A, +)$. Pour tout $a \in A$, tout $b \in A$, tout $x \in A$ on a

$$f_{a+b}(x) = (a + b)x = ax + bx = f_a(x) + f_b(x),$$
$$f_{ab}(x) = (ab)x = a(bx) = f_a(f_b(x))\,.$$

Cela montre que $\Phi(a + b) = f_{a+b} = f_a + f_b$, et $\Phi(ab) = f_{ab} = f_a \circ f_b = \Phi(a)\,\Phi(b)$. Ainsi, Φ est un homomorphisme d'anneaux. De plus $\Phi(1) = f_1 = \mathrm{Id}_A$.
Cet homomorphisme est injectif car :

$$\begin{aligned} a \in \mathrm{Ker}\,(\Phi) \quad &\Leftrightarrow \quad \forall x \in A \ \ ax = 0 \\ &\Rightarrow \qquad a = a1 = 0\,. \end{aligned}$$

b) Si $A = \mathbb{Z}$ ou $\mathbb{Z}/n\mathbb{Z}$, montrons que Φ est surjectif. Soit $f \in \mathrm{End}\,(A)$. Les groupes $(\mathbb{Z}, +)$ et $(\mathbb{Z}/n\mathbb{Z}, +)$ sont monogènes, engendrés par l'unité 1 de l'anneau. Il existe donc $k \in \mathbb{Z}$ tel que $f(1) = k1$. On a $f = \Phi(k\,1) = f_{k1}$ car pour tout $x1 \in A$ on a :

$$f(x1) = f(1 + \cdots + 1) = f(1) + \cdots + f(1) = k1 + \cdots + k1 = xk1 = f_{k1}(x1)\,.$$

Donc Φ est un isomorphisme.

Les unités de l'anneau A sont associées par Φ aux unités de l'anneau End $(A, +)$, c'est-à-dire aux éléments de Aut $(A, +)$.

Si $A = \mathbb{Z}$, il existe deux automorphismes de $(\mathbb{Z}, +)$ qui sont $\mathrm{Id}_{\mathbb{Z}}$ et $-\mathrm{Id}_{\mathbb{Z}}$ associés aux unités 1 et -1 de $\mathbb{Z}$.

Si $A = \mathbb{Z}/n\mathbb{Z}$, les automorphismes du groupe cyclique $(\mathbb{Z}/n\mathbb{Z}, +)$ sont de la forme $\overline{x} \mapsto \overline{k}\overline{x}$ où $k \in \{0, 1, \ldots, n-1\}$ avec $k \wedge n = 1$. L'ordre $[(\mathbb{Z}/n\mathbb{Z})_* : 1] = [\mathrm{Aut}\,(\mathbb{Z}/n\mathbb{Z}, +) : 1]$ est donc $\varphi(n)$ où φ désigne la fonction d'Euler.

Ce résultat a été vu dans l'étude des groupes cycliques : si α est un automorphisme de $(\mathbb{Z}/n\mathbb{Z}, +)$, alors l'image $\overline{k} = \alpha(\overline{1})$ du générateur $\overline{1}$ est un autre générateur de $(\mathbb{Z}/n\mathbb{Z}, +)$, c'est-à-dire un élément de $(\mathbb{Z}/n\mathbb{Z})_*$. La donnée de $\alpha(\overline{1})$ détermine α. L'application $\alpha \mapsto \alpha(\overline{1})$ de Aut $(\mathbb{Z}/n\mathbb{Z}, +)$ sur $(\mathbb{Z}/n\mathbb{Z})_*$ est donc l'isomorphisme réciproque de Φ.

9.3 Les sous-anneaux

Définition.

On appelle sous-anneau d 'un anneau A, une partie B de A telle que :
a) $(B,+)$ *est un sous-groupe du groupe commutatif* $(A,+)$,
b) B *est stable par produit :* $\forall x \in B\ \forall y \in B\ xy \in B$.

Alors B est lui-même un anneau quand on restreint à B les opérations de A.
Notons que $\{0\}$ et A sont des sous-anneaux particuliers de A.
D'après a) on a $0 \in B$ et $x - y \in B$ pour tout $x \in B$, tout $y \in B$.
Si A est commutatif (resp. intègre), alors B est commutatif (resp. intègre).
Si A est unifère et si $1 \in B$, alors la caractéristique de B est égale à celle de A.

Exemples.

a) Les sous-groupes additifs du groupe $(\mathbb{Z},+)$ sont les parties $k\mathbb{Z}$, où $k \in \mathbb{N}$. Ces sous-groupes sont des sous-anneaux de $\mathbb{Z}$. C'est donc la famille des sous-anneaux de $\mathbb{Z}$.

b) Dans une algèbre, on appelle sous-algèbre un sous-anneau qui est stable par la multiplication par les scalaires. Par exemple, dans l'algèbre $\mathcal{M}_n(\mathrm{K})$ des matrices carrées à coefficients dans un corps commutatif K, il existe des sous-algèbres souvent considérées qui sont autant de sous-anneaux. C'est le cas des matrices diagonales (resp. triangulaires supérieures, triangulaires inférieures, bloc-diagonales de la forme $\begin{pmatrix} A & 0 \\ 0 & B \end{pmatrix}$, où $A \in \mathcal{M}_p(\mathrm{K})$, $B \in \mathcal{M}_q(\mathrm{K})$, avec $p \in \mathbb{N}_*$, $q \in N_*$ donnés tels que $p+q=n$, etc.).

Proposition.

Soit $f : A \to B$ *un homomorphisme d'anneaux.*
Si A_1 *est un sous-anneau de* A*, alors* $f(A_1)$ *est un sous-anneau de* B.
Si B_1 *est un sous-anneau de* B*, alors* $f^{-1}(B_1)$ *est un sous-anneau de* A.
En particulier, $\mathrm{Ker}(f)) = f^{-1}(\{0\})$ *et* $\mathrm{Im}(f) = \{f(x)\,;\quad x \in A\}$ *sont des sous-anneaux de* A *et de* B *respectivement.*

Démonstration. $f(A_1)$ et $f^{-1}(B_1)$ sont des sous-groupes additifs de B et A car f est un homomorphisme de groupes additifs de $(A,+)$ dans $(B,+)$. Ce sont des sous-anneaux car ils sont stables par produits :
Soient $y, y' \in f(A_1)$ alors $\exists x, x' \in A_1\ f(x) = y$, $f(x') = y'$ d'où $yy' = f(xx') \in f(A_1)$.
Soient $x, x' \in f^{-1}(B_1)$ alors $f(x) \in B_1$ et $f(x') \in B_1$ d'où $f(xx') = f(x)f(x') \in B_1$ c'est à dire $xx' \in f^{-1}(B_1)$.

Exercice. Montrer que $A = \mathbb{Z} + 2i\mathbb{Z}$ est un sous-anneau de $\mathbb{C}$ (ses éléments sont appelés les entiers de Gauss). Déterminer le groupe des unités de A .

Solution. On a $1 \in \mathbb{Z} + i\mathbb{Z}$. Soient $m, n, m', n' \in \mathbb{Z}$.

$$\begin{aligned} (m+in)+(m'+in') &= (m+m')+i(n+n') \in \mathbb{Z}+i\mathbb{Z}\,, \\ (m+in)(m'+in') &= mm-nn'+i(mn'+nm') \in \mathbb{Z}+i\mathbb{Z}\,. \end{aligned}$$

Ainsi, A est un sous-anneau de $\mathbb{C}$. Pour que $z = m + in \in A$ soit une unité de A, il faut et il suffit qu'il existe $z' = m' + in' \in A$ tel que $1 = zz'$, d'où $|z|^2|z'|^2 = 1$. Cela nécessite que les entiers $|z|^2$ et $|z'|^2$ soient égaux à 1 et nécessite un choix de z dans $\{1\,,\ i,\ -1\,,\ -i\}$. Or chacun de ces éléments z de A convient puisque $z\bar{z} = 1$.

9.4 Sous-anneau engendré par une partie non vide

Proposition.

Soient A un anneau et $B_1, \ldots, B_k$ des sous-anneaux de A et plus généralement une famille $(B_i)_{i\in I}$ de sous-anneaux. Alors $B \bigcap_{i\in I} B_i$ est un sous-anneau de A.

Démonstration.. On sait que l'intersection $(B, +)$ des sous-groupes $(B_i, +)$ de $(A, +)$ est un sous-groupe de $(A, +)$. Par ailleurs, pour tous x , $y \in B$, on a :
$\forall i \in I \quad x$, $y \in B_i$, d'où $\forall i \in I \quad xy \in B_i$ c'est à dire $xy \in B$. ∎

Corollaire.

Soit X une partie non vide de l 'anneau A. Il existe un plus petit sous-anneau de A contenant X, à savoir l'intersection B de tous les sous-anneaux de A contenant X. Ses éléments sont les sommes finies de produits finis d'éléments de $X \cup (-X)$.

Démonstration.. D'après la proposition, B est un sous-anneau de A. Il contient X. Il est minimum car contenu dans tout sous-anneau de A contenant X. L'ensemble des sommes finies $\sum x_{i_1}, \cdots x_{i_k}$ de produits en nombre fini d'éléments de $X \cup (-X)$ est visiblement un sous-anneau de A, contenant X et contenu dans B. Il est égal à B car B est le plus petit sous-anneau possédant ces propriétés. ∎

Définition.

On appelle B le sous-anneau engendré par la partie X de A.

Exercice. Soient A un anneau et $a \in A$. Quel est le sous-anneau A_0 de A engendré par a ? Si A est unifère, quel est le sous-anneau A_1 engendré par $\{a, 1\}$?

Solution. L'ensemble $\mathbb{Z}[X]$ des polynômes à coefficients dans $\mathbb{Z}$ est un anneau (voir 10-1). L'application $f : \mathbb{Z}[X] \to A$ associant à $p(X) = k_0 + k_1X + \cdots + k_rX^r$ l'élément $p(a) = k_0 + k_1a + \cdots + k_ra^r$ de A, où on note k_0 l'élément k_01 de A, est un homomorphisme d'anneaux de $\mathbb{Z}[X]$ dans A. L'ensemble J des polynômes $p \in \mathbb{Z}[X]$ sans terme constant est un sous-anneau de l'anneau $\mathbb{Z}[X]$ (et même un idéal au sens du paragraphe suivant). L'image $f(J)$ de J est un sous-anneau de A qui contient a image du polynôme X. Il contient donc le sous- anneau A_0 engendré par a. Par ailleurs, tout élément $p(a) = k_1a + \cdots + k_ra^r$ de $f(J)$ appartient à A_0. Donc $A_0 = f(J)$.
De même, on voit que A_1 est l'ensemble des éléments $p(a) = k_0 + k_1a + \cdots + k_ra^r$.

9.5 Idéaux d'un anneau

Définitions.

On appelle idéal à gauche de l'anneau A, un sous-groupe de $(A, +)$ tel que :
(1) $\forall a \in A \quad \forall x \in I \qquad ax \in I$.
On appelle idéal à droite de A un sous-groupe de $(A, +)$ tel que :
(2) $\forall a \in A \quad \forall x \in I \qquad xa \in I$.
On appelle idéal bilatère de A un sous-groupe de $(A, +)$ qui vérifie (1) et (2).

Évidemment, si l'anneau A est commutatif, les trois notions sont identiques. On dit alors tout simplement, "un idéal" de A.

Dans un anneau A, il existe au moins deux idéaux bilatères, à savoir $\{0\}$ et A. Supposons A unifère. Pour que $I \neq \emptyset$ soit un idéal à gauche, il suffit que

$$\forall x \in I \quad \forall y \in I \quad x+y \in I \quad \text{et} \quad \forall a \in A \quad \forall x \in I \quad ax \in I\,.$$

car alors $0 = 0x \in I$ et $-x = (-1)x \in I$ pour tout $x \in I$. Ainsi I est un sous-groupe de $(A,+)$.

Supposons A unifère. Si un idéal à gauche (resp. à droite) I de A contient l'unité 1 de A, alors $I = A$ car alors $a = a1 \in I$ pour tout $a \in A$. Plus généralement, si I contient un élément inversible u de A, alors $1 = u^{-1}u \in I$ et donc $I = A$.

Un idéal de A est un sous-anneau de A car (1) ou (2), montre que $xy \in I$ pour tout $x \in I$ et tout $y \in I$. La réciproque est fausse : par exemple $\mathbb{Z}$ est un sous-anneau de $\mathbb{R}$ mais n'est pas un idéal de $\mathbb{R}$.

Proposition.

Soit $f : A \longrightarrow B$ un morphisme d'anneaux.

(i) *Soit J un idéal à gauche (resp. à droite, bilatère) de B. Alors $f^{-1}1(J)$ est un idéal à gauche (resp. à droite, bilatère) de A.*
En particulier, le noyau $\mathrm{Ker}\,(f) = f^{-1}(\{0\})$ de f est un idéal bilatère de A.

(ii) *Supposons f surjectif. L'image $f(I)$ de tout idéal à gauche (resp. à droite, bilatère) I de A, est un idéal à gauche (resp. à droite, bilatère) de B.*

(iii) *Supposons f surjectif. L'application $\alpha : J \mapsto f^{-1}(J)$ est une bijection, de l 'ensemble $\mathcal{J}$ des idéaux bilatères de B sur l'ensemble $\mathcal{F}$ des idéaux bilatères de A contenant $\mathrm{Ker}\,(f)$ et α respecte l'inclusion.*

Démonstration. (i) $f^{-1}(J)$ est un sous-groupe additif de A. Pour $x \in f^{-1}(J)$ et $a \in A$ on a $f(x) \in J$, d'où $f(ax) = f(a)f(x) \in J$ et donc $ax \in f^{-1}(J)$.

(ii) Nous laissons la vérification au lecteur.

(iii) D'après (i), si J est un idéal bilatère de B, alors $f^{-1}(J)$ est un idéal bilatère de A. Il contient $\mathrm{Ker}\,(f) = f^{-1}(\{0\})$. Ainsi α est une application de $\mathcal{J}$ dans $\mathcal{F}$. Si $J, J' \in \mathcal{J}$ sont tels que $J \subset J'$ on a $f^{-1}(J) \subset f^{-1}(J')$ donc α respecte l'ordre. Pour tout $J \in \mathcal{J}$ on a $f[f^{-1}(J)] = J$ car f est surjective donc α est injective. Elle est surjective car pour tout $I \in \mathcal{F}$, on a $\mathrm{Ker}\,(f) \subset I$ et donc $f^{-1}(f(I)) = I + \mathrm{Ker}\,(f) = I$. ∎

9.6 Intersection et somme d'idéaux

Proposition.

Soit $(I_k)_{k\in K}$ une famille d'idéaux à gauche de l'anneau A.

(i) $\bigcap_{k\in K} I_k$ *est un idéal à gauche de A.*

(ii) *L'ensemble $\sum_{k\in K} I_k$ des éléments $x \in A$ qui sont somme finie $x_{i_1} + \cdots + x_{i_k}$ d'éléments de $\bigcup_{k\in K} I_k$, est un idéal à gauche de A. C'est le plus petit idéal à gauche de A contenant I_k pour tout $k \in K$.*

En particulier, la somme $I + J = \{x+y\,;\ x \in I, y \in J\}$ de deux idéaux à gauche I et Jde A, est un idéal à gauche de A.

Démonstration.. Les vérifications sont laissées au lecteur. ∎

Corollaire.

Soit A un anneau unifère. Pour toute partie non vide X de A, il existe un plus petit idéal à gauche I de A contenant X, à savoir l 'intersection de tous les idéaux à gauche de A contenant X. De plus, I est l 'ensemble des éléments de A de la forme $a_1x_1 + \cdots + a_px_p$ où $p \in N^*$, $x_1, \ldots, x_p \in X$ et $a_1, ..., a_p \in A$.

Démonstration.. La première assertion est une conséquence de (i). L'ensemble des éléments de la forme $a_1x_1 + \cdots + a_px_p$ est un idéal à gauche de A qui contient X (prendre $p = 1$ et $a_1 = 1$). Il contient donc I (plus petit idéal à gauche contenant X). Par ailleurs, on a $x_1, \ldots, x_p \in I$ donc tous les éléments de la forme précédente appartiennent à I. ∎

Définition.

Dans un anneau unifère A, ce plus petit idéal à gauche de A contenant une partie $X \neq \emptyset$ de A est appelé l 'idéal à gauche engendré par X.

Il existe des énoncés analogues pour les idéaux à droite, d'où une notion d'idéal à droite engendré par X, dont les éléments sont de la forme $x_1a_1 + \cdots + x_pa_p$.

Pour les idéaux bilatères, il en va de même. L'idéal bilatère engendré par X est l'ensemble des $a_1x_1b_1 + \cdots + a_px_pb_p$, où $p \in N^*$, $x_1, \ldots, x_p \in X$ et $a_1, \ldots, a_p, b_1, \ldots, b_p \in A$.

Si I et I' sont deux idéaux à gauche (resp. à droite, bilatères), l'idéal à gauche (resp. à droite, bilatère) engendré par $I \cup I'$ est $I + I' = \{x + x' ;\ x \in I ,\ x' \in I'\}$.

Exercice. Soient I, J, K des idéaux bilatères d'un anneau A.

a) Montrer que $IJ = \{\sum_{i=1}^{k} x_iy_i\ , y, \ ;\ k \in N_*\ , x_i \in I, y_i \in J\}$ est un idéal bilatère de A contenu dans $I \cap J$.

b) Si $I + J = A$ et si A est commutatif unifère, montrer que $IJ = I \cap J$.

c) Montrer que $I(J+\mathrm{K}) = IJ + IK$.

Solution. a) Soient, $x = \sum_{i=1}^{k} x_iy_i$ et $x' = \sum_{i=1}^{\ell} x'_iy'_i$ des éléments de IJ. On a

$$x - x' = x_1y_1 + \cdots + x_ky_k + (-x'_1)y_1 + \cdots + (x'_\ell)y_\ell \in IJ$$

donc IJ est un sous-groupe de $(A, +)$. Pour tout $y \in A$ on a :

$$yx = \sum_{i=1}^{k} (yx_i)y_i \quad , \quad xy = \sum_{i=1}^{k} (x_iy_i)y \quad \text{avec} \quad yx_i \in I\ ,\ y_iy \in J$$

car I et J sont des idéaux bilatères. Donc IJ est un idéal bilatère de A. On a $IJ \subset I$ et $IJ \subset J$, d'où $IJ \subset I \cap J$. En général $IJ \neq I \cap J$ (Voir Ex. 11-4).

b) Si $I + J = A$ et si A est abélien unifère, on a :

$$I \cap J = (I + J)(I \cap J) = I(I \cap J) + J(I \cap J) \subset IJ + JI = IJ \subset I \cap J\,.$$

c) On a $IJ \subset I(J + K)$ et $IK \subset I(J + K)$ donc $IJ + IK \subset I(J + K)$. Tout élément de $I(J + K)$ est somme d'éléments de la forme $x_i(y_i + z_i)$, où $x_i \in I\,, y_i \in J\,, z_i \in K$. Or on a $x_i(y_i + z_i) = x_iy_i + x_iz_i \in IJ + IK$ et donc $I(J + K) \subset IJ + IK$.

9.7 Quotient d'un anneau par un idéal bilatère

Lemme.

Soient A un anneau, I un sous-groupe du groupe additif $(A,+)$. La relation d'équivalence de congruence modulo le sous-groupe I,

$$x \equiv y \Leftrightarrow y - x \in I\,,$$

est compatible avec le produit de A, si et seulement si I est un idéal bilatère de A.

Démonstration.. L'équivalence est compatible avec les multiplications à gauche, si pour $x, y \in A$, la condition $x \equiv y$ implique que $ax \equiv ay$ pour tout $a \in A$, soit si pour tout $z \in I$ et tout $a \in A$, on a$az \in I$, c'est-à-dire si I est idéal à gauche.

De même, l'équivalence est compatible avec le produit du côté droit si et seulement si I est un idéal à droite de A, d'où le lemme. ∎

Proposition.

Soient A un anneau et I un idéal bilatère de A. Le quotient A/I, muni des opérations

$$\overline{x} + \overline{y} = \overline{x+y} \qquad , \qquad \overline{x}\,\overline{y} = \overline{xy}$$

est un anneau. Si A a une unité, alors $\overline{1}$ est une unité pour A/I.
L'application canonique $\varphi : x \mapsto \overline{x}$ est un homomorphisme d'anneaux surjectif de A sur A/I, de noyau I et le couple $(A/I, \varphi)$ a la propriété universelle suivante (factorisation des homomorphismes) :

(P) Si un homomorphisme f de A dans un anneau B est nul sur I, alors il existe un homomorphisme unique $\overline{f} : A/I \to B$ tel que $\overline{f} \circ \varphi = f$.
De plus, on a $\mathrm{Im}\left(\overline{f}\right) = \mathrm{Im}\,(f)$ et $\mathrm{Ker}\left(\overline{f}\right) = \mathrm{Ker}\,(f)\,/\,I$.

Démonstration.. D'après 1-8, A/I est un groupe additif. D'après le lemme, le produit est bien défini sur A/I et les axiomes des anneaux sont vérifiés (voir 1-2).

Soit $f \in \mathrm{Hom}\,(A,B)$ nul sur I. D'après 1-9, on définit un homomorphisme de groupes additifs en posant $\overline{f}(\overline{x}) = \overline{f(x)}$ pour tout $\overline{x} \in A/I$. On a

$$\overline{f}(\overline{xy}) = \overline{f}(\overline{xy}) = f(xy) = f(x)f(y) = \overline{f}(\overline{x})\overline{f}(\overline{y})\,,$$

donc $\overline{f}$ est un homomorphisme d'anneaux, d'où la propriété universelle (P). ∎

Corollaire 1.

Un homomorphisme d'anneaux $f : A \to B$ a une décomposition canonique : f est composé de l'homomorphisme surjectif $\varphi : x \mapsto \overline{x}$, de l'isomorphisme $\overline{f}$ de $A/\mathrm{Ker}\,(f)$ sur $\mathrm{Im}\,(f)$ et de l'homomorphisme injectif $j : x \mapsto x$ de $\mathrm{Im}\,(f)$ dans B.

Corollaire 2.

Si $I \subset J$ sont des idéaux bilatères de l'anneau A, alors les anneaux A/J et $(A/I)/(J/I)$ sont isomorphes.

Démonstration.. Notons $f : A \to A/J$ et $\varphi : A \to A/I$ les homomorphismes canoniques. On a $I \subset J = \mathrm{Ker}\,(f)$. Il existe donc un homomorphisme $\overline{f} : A/I \to A/J$ tel que $\overline{f} \circ \varphi = f$. On a $\mathrm{Im}\left(\overline{f}\right) = \mathrm{Im}\,(f) = A/J$ donc $\overline{f}$ est surjectif. De plus,

$$\overline{x} \in \mathrm{Ker}\left(\overline{f}\right) \quad \Leftrightarrow \quad \overline{f}(\overline{x}) = 0 \quad \Leftrightarrow \quad f(x) = 0 \quad \Leftrightarrow \quad x \in \mathrm{Ker}\,(f) = J\,.$$

Ainsi $\mathrm{Ker}\left(\overline{f}\right) = \varphi(J) = J/I$. Par factorisation de $\overline{f} : A/I \mapsto A/J$ à travers son noyau J/I on obtient un isomorphisme de $(A/I)/(J/I)$ sur A/J. ∎

9.8 Idéaux maximaux

Définition.

On appelle idéal a gauche maximal de l 'anneau A, un idéal a gauche I de A, distinct de A, tel que les seuls idéaux à gauche de A contenant I soient I et A. On définit de même les notions d 'idéal à droite maximal et d 'idéal bilatère maximal.

Proposition.

Soit A un anneau avec unité.
Tout idéal à gauche de A, distinct de A, est inclus dans un idéal à gauche maximal.
Tout idéal à droite de A, distinct de A, est inclus dans un idéal à droite maximal.
Tout idéal bilatère de A, distinct de A, est inclus dans un idéal bilatère maximal.

Démonstration.. Considérons, par exemple, le cas où I est un idéal à gauche. Ordonnons l'ensemble E des idéaux à gauche de A, distincts de A, contenant I, par la relation d'inclusion. Cet ensemble E est non vide car $I \in E$. Vérifions que E est inductif.

Soit $(J_i) - i \in I$ une famille totalement ordonnée d'éléments de E. Vérifions que $J = \bigcup_{i\in I} J_i$ est un idéal à gauche de A. La réunion J d'une chaîne de sous-groupes est un sous-groupe de $(A, +)$ (Voir 1-5, ex. 1). Soient $x \in J$ et $a \in A$. Il existe $i \in I$ tel que $a :\in J_i$. On a $ax \in J_i$ et donc $ax \in J$. Ainsi, J est un idéal à gauche. Il est distinct de A car $1 \notin J$ pour tout i'. Ainsi, $J \in E$ et J majore tout élément J_i de la chaîne. Cela prouve que E est inductif, d'où le résultat d'après le th. de Zorn ([1]). ∎

Exercice. Montrer que les idéaux maximaux de $\mathbb{Z}$ sont les idéaux $p\mathbb{Z}$, où p est premier. Etudier les idéaux de l'anneau $\mathbb{Z}/nZ$, ses idéaux maximaux, le quotient de $\mathbb{Z}/nZ$ par un tel idéal maximal.

Solution. Tout idéal de $\mathbb{Z}$ est un sous-groupe additif et donc de la forme $n\mathbb{Z}$, où $n \in \mathbb{N}$ est unique. Cet idéal est maximal, si pour tout autre idéal $k\mathbb{Z}$ de $\mathbb{Z}$ tel que $n\mathbb{Z} \subset k\mathbb{Z}$, on a $k\mathbb{Z} = n\mathbb{Z}$ ou$k\mathbb{Z} = \mathbb{Z}$. Cela signifie que si $k|n$, alors $k = n$ ou $k = 1$. Les idéaux maximaux de $\mathbb{Z}$ sont donc les idéaux $p\mathbb{Z}$ où p est premier.
D'après 9-7, $\mathbb{Z}/n\mathbb{Z}$ est un anneau et $\varphi : k \mapsto \overline{k}$ est un homomorphisme de $\mathbb{Z}$ sur $\mathbb{Z}/$n$\mathbb{Z}$. D'après 9-5, si I est un idéal de $\mathbb{Z}/n\mathbb{Z}$ alors $\varphi^{-1}(I)$ est un idéal de $\mathbb{Z}$ et est donc de la forme $k\mathbb{Z}$. On a
$I = \varphi(\varphi^{-1}(I))$ car φ est surjectif d'où $I = \{\overline{km};\ m \in \mathbb{Z}\} = \overline{k}(\mathbb{Z}/n\mathbb{Z})$. Les idéaux de $\mathbb{Z}/n\mathbb{Z}$ sont donc les parties de la forme $\overline{k}(\mathbb{Z}/n\mathbb{Z})$. D'après 9-5, φ étant surjectif, $\Phi : I \mapsto \varphi^{-1}(I)$ est une bijection préservant l'inclusion entre idéaux de $\mathbb{Z}/n\mathbb{Z}$ et idéaux de $\mathbb{Z}$ contenant Ker $(\varphi) = n\mathbb{Z}$. Les idéaux de $\mathbb{Z}/n\mathbb{Z}$ correspondent donc bijectivement aux diviseurs $k \in N$ de n. L'idéal $I = \overline{k}(\mathbb{Z}/n\mathbb{Z})$ de $\mathbb{Z}/n\mathbb{Z}$ est maximal, si et seulement si $k\mathbb{Z}$ est maximal dans $\mathbb{Z}$ et contient Ker $(\varphi) = n\mathbb{Z}$, c'est-à-dire si k divise n et si k est premier.
Si l'idéal $\overline{p}(\mathbb{Z}/n\mathbb{Z})$ de $(\mathbb{Z}/n\mathbb{Z})$ est maximal, alors p est premier et $n\mathbb{Z} \subset p\mathbb{Z}$. D'après 9-7, cor. 2, on a $\mathbb{Z}/p\mathbb{Z} \simeq (\mathbb{Z}/n\mathbb{Z})/(p\mathbb{Z}/n\mathbb{Z})$avec $p\mathbb{Z}/n\mathbb{Z} = \overline{p}(\mathbb{Z}/n\mathbb{Z})$. Le quotient de $\mathbb{Z}/n\mathbb{Z}$ par l'idéal maximal $\overline{p}\mathbb{Z}/n\mathbb{Z})$ est isomorphe à $\mathbb{Z}/p\mathbb{Z}$.

1. Rappelons que dans les systèmes d'axiomes usuellement considérés pour fonder la théorie des ensembles, l'axiome du choix est indépendant des autres et permet de démontrer (th. de Zorn) qu'un ensemble inductif E possède un élément maximal. Un ensemble ordonné E est dit inductif, si toute famille totalement ordonnée d'éléments possède un majorant.

9.9 Corps

Définitions.

Un corps est un anneau K, possédant une unité 1 (distincte du zéro) tel que tout élément non nul x possède un inverse x^{-1}.
Si le produit est commutatif, on dit que K est un corps commutatif.
On appelle sous-corps de K un sous-anneau K_0 de K contenant l'unité de K et tel que pour tout $x \in K_0$ non nul on ait $x^{-1} \in K_0$.

Un corps K est donc un anneau unifère dont le groupe des unités est $K_* = \mathrm{K}\backslash\{0\}$.

Un corps est intègre : si $xy = 0$ et si $x \neq 0$ alors x est inversible et $y = x^{-1}(xy) = 0$.

L'intersection d'une famille $(K_i)_{i\in I}$ de sous-corps d'un corps K est non seulement un sous-anneau de K contenant l'unité mais c'est un sous-corps de K. En effet, pour tout $x \in \bigcap_{i\in I} K_i$, avec $x \neq 0$, on a $x^{-1} \in K_i$ pour tout $i \in I$ et donc$x^{-1} \in \bigcap_{i\in I} K_i$.

Soit X une partie non vide de K. L'intersection des sous-corps de K contenant X, est le plus petit sous-corps de K contenant X, appelé le *sous-corps engendré* par X.

Les corps $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ jouent un rôle essentiel en mathématique.

Proposition.

Soit K un anneau avec unité. Pour que K soit un corps, il faut et il suffit que $\{0\}$ et K soient les seuls idéaux à gauche de K. Il en est de même pour les idéaux à droite.

Démonstration. Soit I un idéal à gauche du corps K. Si $I \neq \{0\}$, il existe $x \in I$ non nul. On a $1 = x^{-1}x \in I$ et donc $I = K$.

Réciproquement, soit K un anneau unifère ayant pour seuls idéaux à gauche $\{0\}$ et K. Pour tout $x \neq 0$ l'idéal à gauche Kx de K contient x. Il est donc égal à K. En particulier, il existe $y \in K$ tel que $yx = 1$. Comme $y \neq 0$, il existe de même $z \in K$ tel que $zy = 1$. Alors y qui a un inverse à droite x et un inverse à gauche z, est inversible d'inverse $y^{-1} = x$. Tout élément non nul x de K est donc inversible et K est un corps. On montre de même l'assertion concernant les idéaux à droite. ∎

Exercice 1. Montrer qu'un anneau fini intègre avec unité A est un corps.

Solution. Soit I un idéal à gauche de A. Supposons $I \neq \{0\}$. Il existe $x \in I$ non nul. Comme A est intègre, $y \mapsto yx$ est un homomorphisme injectif du groupe $(A, +)$ dans lui-même. Comme A est fini, son image est $Ax = A$ et on a $Ax \subset I$ car I est un idéal à gauche. Ainsi $\{0\}$ et A sont les seuls idéaux à gauche de A et A est un corps.

Exercice 2. Nous allons voir que non seulement $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ ne sont pas les seuls corps mais qu'il existe une infinité de sous-corps de $\mathbb{C}$ non isomorphes (extensions quadratiques de $\mathbb{Q}$). Notons $\mathcal{P}$ l'ensembles des nombres entiers premiers.

a) Soit K un sous-corps de $\mathbb{C}$ et $P(X) = x^2 - uX - v$ un polynôme de $K[X]$ sans racine dans K. Soit α une racine de $P(X)$ dans $\mathbb{C}$. Montrer que $K(\alpha) = \{a + b\alpha \ , \ a, b \in K\}$ est un sous corps de $\mathbb{C}$, de dimension 2 sur K.

b) Montrer que $K_1 = \{a + b\sqrt{2}\,; \ \ a, b \in \mathbb{Q}\}$, $K_2 = \{a + ib\,; \ \ a, b \in \mathbb{Q}\}$, $K_3 = \{a + b\sqrt{2} + ic + id\sqrt{2}\,; \ \ a, b, c, d \in \mathbb{Q}\}$ sont des sous-corps de $\mathbb{C}$.

c) Soient $d \in \mathbb{Z}$, $d' \in \mathbb{Z}$ autres que 0, 1, dont tous les facteurs premiers sont sans multiplicité. Soit δ (resp. δ') une racine carrée dans $\mathbb{C}$ de d (resp. de d').
Montrer que $\mathbb{Q}(\delta)$ et $\mathbb{Q}(\delta)$ sont des sous-corps de $\mathbb{C}$ non isomorphes si $d \neq d'$.
Montrer que Id et $\sigma : x + y\delta \mapsto x - y\delta$ sont les seuls automorphismes de $\mathbb{Q}(\delta)$.

d) Montrer que tout sous-corps K de $\mathbb{C}$ qui est une extension quadratique de $\mathbb{Q}$ (sous-espace vectoriel de $\mathbb{C}$ de dimension 2 sur $\mathbb{Q}$) est de la forme $\mathbb{Q}(\delta)$ précédente.

Solution. **a)** On a $1 \in K$. Soient $x = a + b\alpha \in K(\alpha)$ et $x' = a' + b'\alpha \in K(\alpha)$.
$x + x' = (a + a') + (b + b')\alpha \in K(\alpha)$,
$xx' = (aa' + vbb') + (ba' + ab' + ubb')\alpha \in K(a)$,
car $\alpha^2 = ua + v$. Donc $K(\alpha)$ est un sous-anneau de $\mathbb{C}$. Si $x = a + b\alpha \neq 0$, montrons que son inverse dans $\mathbb{C}$ est élément de $K(\alpha)$. Si $b = 0$ alors l'inverse dans $\mathbb{C}$ de $x = a \neq 0$ est un élément du corps K. Supposons $b \neq 0$. Pour que $x' = a' + b'\alpha \in \mathbb{C}$ soit l'inverse de x, il faut et il suffit que $aa' + vbb' = 1 \quad , \quad ba' + (a + ub)b' = 0$. Le déterminant de ce système $a^2 + uab - vb^2$ est non nul, sinon $-a/b \in K$ serait racine de $P(X)$. Ce système de Cramer a donc une solution $(a', b') \in K^2$ et $K(\alpha)$ est un sous-corps de $\mathbb{C}$, qui contient K. C'est un espace vectoriel de dimension 2 sur K car $\alpha \notin K$ et donc 1 et α sont libres sur K et générateurs par définition de $K(\alpha)$. On dit que $K(\alpha)$ est une extension quadratique de K.

b) Prenons $K = \mathbb{Q}$ et $P(X) = X^2 - p$, où $p \in \mathcal{P}$. Un rationnel, $\frac{m}{n}$ où $m \in \mathbb{Z}$, $n \in N_*$ avec $m \wedge n = 1$, ne peut être racine de $P(X)$ sinon $m^2 = pn^2$ et p diviserait m. On aurait $m = pm'$ et $pm'^2 = n^2$ et p diviserait n. C'est absurde car $m \wedge n = 1$. En prenant $p = 2$, on voit que K_1 est un sous-corps de $\mathbb{C}$.

Avec $K = \mathbb{Q}$, $P(X) = X^2 + 1$ et $\alpha = i$, on voit que K_2 est un sous-corps de $\mathbb{C}$.

Puisque $P(X) = X^2 + 1$ est sans racine sur $K_1 \subset \mathbb{R}$, la question a) montre que $K_1(i) = K_3$ est un sous-corps de $\mathbb{C}$. Ici K_3 est un espace vectoriel de dimension 4 sur $\mathbb{Q}$ car $(1, \sqrt{2}, i, i\sqrt{2})$ est une base de K_3 sur $\mathbb{Q}$. (tout $x \in K_3$ admet une unique expression comme combinaison linéaire sur $\mathbb{Q}$ de ces éléments).

c) Soit f un isomorphisme de $\mathbb{Q}(\delta) = K$ sur $\mathbb{Q}(\delta') = K'$. Il existe $a = \frac{m}{n} \in \mathbb{Q}$ avec $m \wedge n = 1$ et $b = \frac{r}{s}$ avec $r \wedge s = 1$, tels que $f(\delta) = a + b\delta'$. On a

$$d = df(1) = f(d1) = f(\delta^2) = [f(\delta)]^2 = (a + b\delta')^2 = a^2 + b^2d' + 2ab\delta' .$$

Comme $\delta' \notin \mathbb{Q}$, on a $a = 0$ ou $b = 0$. Si $b = 0$ on obtient $d = a^2 = (\frac{m}{n})^2$ d'où $n = 1$ et $d = m^2$, impossible car d est sans facteur carré. Donc $b \neq 0$ et $a = 0$, d'où $d = d'b^2$ soit $s^2d = r^2d'$. Comme $r \wedge s = 1$, s^2 divise d' donc $s^2 = 1$ car d' est sans facteur carré. Pareillement, $r^2 = 1$ et $d = d'$. Pour $d \neq d'$, les corps $\mathbb{Q}(\delta)$ et $\mathbb{Q}(\delta')$ ne sont pas isomorphes.
Si $d = d'$, le calcul précédent montre que tout automorphisme$f$ de $\mathbb{Q}(\delta)$ est tel que $f(\delta) = \neq \delta'$ donc $f =$ Id ou f est l'automorphisme $\sigma a : a + b\delta \mapsto a - b\delta$.
L'ensemble $\mathcal{P}$ des nombres premiers est infini (Euclide). Il existe donc une infinité de corps $\mathbb{Q}(\sqrt{p})$, où $p \in \mathcal{P}$, deux à deux non isomorphes.

d) Soit $\alpha \in K \setminus \mathbb{Q}$. Alors 1 et α sont libres sur $\mathbb{Q}$ et forment donc une base de K sur $\mathbb{Q}$. On a $\alpha^2 \in K$. Il existe $u \in \mathbb{Q}$, $v \in \mathbb{Q}$ tels que $\alpha^2 = u\alpha + v$. Réduisons au même dénominateur $u = \frac{m}{n}$, $v = \frac{s}{t}$ d'où $u = \frac{b}{a}$, $v = \frac{c}{a}$ Alors α est racine de $aX^2 - bX - c \in \mathbb{Z}[X]$. Or $\Delta = b^2 + 4ac$ n'est pas un carré parfait, sinon $\alpha \in \mathbb{Q}$. Soit Δ_1 le plus grand carré diviseur de Δ. On a $\Delta = \Delta_1^2 d$ et $\alpha = \frac{1}{2a}(b + \Delta_1\delta)$, où δ est l'une des racines carrées de d dans $\mathbb{C}$. Alors δ est élément de K, puisque α, a, b, Δ_1 sont éléments de K et $d \notin \mathbb{Q}$ (sinon $\alpha \in \mathbb{Q}$. Ainsi $\mathbb{Q}(\delta)$ est de dimension 2 sur $\mathbb{Q}$, avec $\mathbb{Q}(\delta) \subset K$ et donc $K = \mathbb{Q}(\delta)$. Si d' est un autre élément de $\mathbb{Z}$, sans diviseur carré autre que 1, tel que $\mathbb{Q}(\delta') = K$, d'après c), on a $d' = d$.

9.10 Corps des fractions d'un anneau intègre

Proposition.

Considérons un anneau commutatif unifère intègre A et une partie multiplicativement stable S de $A \setminus \{0\}$ qui contient l'unité 1 de A.

(i) *La relation binaire $\mathcal{R}$ définie par $(a,s)\mathcal{R}(a',s') \Leftrightarrow as' = a's$ est une relation d'équivalence sur l'ensemble $A \times S$ des fractions à dénominateur dans S.*

(ii) *Les opérations d'addition et de multiplication des fractions définies par*
$(a_1,s_1) + (a_2,s_2) = (a_1s_2 + a_2s_1, s_1s_2)$ $\quad (a_1,s_1)(a_2,s_2) = (a_1a_2, s_1s_2)$
sont compatibles avec $\mathcal{R}$ et définissent des opérations sur $K = (AXS)/\mathcal{R}$.

(iii) *Muni de ces opérations, K est un anneau commutatif intègre, avec unité. Si $S = A \setminus \{0\}$, alors K est un corps.*

(iv) *L'application φ associant à $a \in A$ la classe de $(a,1)$ dans K est un homomorphisme injectif, respectant l'unité, plongeant A dans K et tel que $\varphi(S) \subset K_*$.*

Le couple (K,φ) possède la propriété universelle suivante :

(P) Si f est un homomorphisme de A dans un anneau unifère B, tel que $f(1) = 1$ et $f(S) \subset B_*$, il existe un homomorphisme unique $\overline{f}$ de K dans B tel que $\overline{f} \circ \varphi = f$. De plus, si f est injectif alors $\overline{f}$ est injectif.

Démonstration. $\mathcal{R}$ est réflexive et symétrique. Vérifions la transitivité.

Si $(a,s)\mathcal{R}(a',s')$ et $(a',s')\mathcal{R}(a'',s'')$ alors $as' = a's$ et $a's'' = a''s'$; d'où $as's'' = a'ss''$ et $a's''s = a''s's$. La commutativité de A implique $s'(as'') = s'(a''s)$. Comme A est intègre et $s' \neq 0$, on obtient $as'' = a''s$. Ainsi $\mathcal{R}$ est transitive.

(ii) Comme S est multiplicativement stable, les opérations sont bien définies sur $A \times S$. Supposons que l'on ait $(a_1,s_1)\mathcal{R}(a_1',s_1')$ et $(a_2,s_2)\mathcal{R}(a_2',s_2')$, soit encore :

$$(1) \qquad a_1s_1' = a_1's_1 \qquad \text{et} \qquad (2) \qquad a_2s_2 = a_2's_2 \,.$$

Multiplions (1) par s_2s_2', et (2) par s_1s_1' et ajoutons les relations. On obtient

$$(a_1s_2 + a_2s_1)s_1's_2 = (a_1's_2 + s_1'a_2')s_1s_2$$

d'où $(a_1s_2 + a_2s_1, s_1s_2)\mathcal{R}(a_1's_2' + s_1'a_2', s_1's_2')$. Ainsi l'addition et $\mathcal{R}$ sont compatibles.

En multipliant membre à membre (1) et (2), on obtient $a_1a_2s_1's_2' = a_1'a_2's_1s_2$ donc le produit et $\mathcal{R}$ sont compatibles. D'après 1-2, on peut alors définir sur le quotient $K = (A \times S)/\mathcal{R}$ des opérations d'addition et de multiplication quotient.

(iii) On vérifie immédiatement, que sur l'ensemble $A \times S$ des fractions l'addition est commutative, associative, d'élément neutre $(0,1)$ et que le produit est commutatif, asso- ciatif, d'élément neutre $(1,1)$. Ces propriétés se transmettent au quotient. L'addition de K est donc commutative, associative, d'élément neutre la classe $\overline{0}$ de $(0,1)$. Pour tout $(a,s) \in A \times S$ on a $(a,s) + (-a,s) = (0,s^2)$ équivalente à $(0,1)$. On voit donc que tout élément x de K, classe d'une fraction (a,s), a un opposé $-x$ qui est la classe de $(-a,s)$. Ainsi l'addition fait de K un groupe commutatif.

Dans K, le produit distribue l'addition car les fractions $[(a,s) + (a',s')](a'',s'')$ et $(a,s)(a'',s'') + (a',s')(a'',s'')$ sont équivalentes. Donc K est un anneau commutatif, unifère. Cet anneau est intègre. En effet, si les fractions $(a,s)(a',s') = (aa',ss')$ et

$(0,1)$ sont équivalentes, alors $aa' = 0$. On a donc $a = 0$ ou $a' = 0$ puisque A est intègre. Donc dans K, la classe de (a,s) ou la classe de (a',s'), est nulle.

Comme A est intègre, $A \setminus \{0\}$ est multiplicativement stable. Si $S = A \setminus \{0\}$, tout élément non nul de K, classe d'une fraction (a,b) où $a \neq 0$, a pour inverse la classe de (b,a) car $(a,b)(b,a) = (ab,ba)$ est équivalente à $(1,1)$. L'anneau K est alors un corps.

(iv) Comme $(a,1) + (b,1) = (a+b,1)$ et $(a,1)(b,1) = (ab,1)$, on a
$\varphi(a) + \varphi(b) = \varphi(a+b)$ et $\varphi(a)\varphi(b) = \varphi(ab)$. Donc « p est un homomorphisme. De plus, $\varphi(1)$ est la classe de $(1,1)$, c'est-à-dire l'unité de K. L'homomorphisme φ est injectif car

$$\varphi(a) = 0 \quad \Leftrightarrow \quad (a,1)\mathcal{R}(0,1) \quad \Leftrightarrow \quad a = 0\,.$$

Soit $f : A \to B$ un homomorphisme d'anneaux tel que tout élément de S ait une image inversible. Comme A est commutatif, le sous-anneau $f(A)$ est également commutatif. Pour $(a,s) \in A \times S$ posons $f_0(a,s) = f(a)f(s)^{-1}$. Des fractions équivalentes (a,s) et (a',s') sont telles que $as' = a's$ d'où $f(a)f(s') = f(a')f(s)$ ou encore $f(a)f(s)^{-1} = f(a')f(s')^{-1}$. Ainsi l'application f_0 est constante sur les classes de fractions équivalentes et se factorise : on définit une application $\overline{f}$ en associant à la classe de (a,s) l'élément $f_0(a,s) = f(a)f(s)^{-1}$ de B. On a $\overline{f} \circ \varphi = f$ et $\overline{f}$ est un homomorphisme. Il est unique car ses valeurs sur A le déterminent. ∎

Définition.

L'anneau K est appelé l'anneau des fractions de l'anneau A à dénominateur dans S. Si $S = A \setminus \{0\}$, on appelle K le corps des fractions de A.

Corollaire.

Soient K_0 un corps et A un sous-annneau de K_0. Si A engendre K, alors K_0 est isomorphe au corps des fractions de A.

Démonstration. Le corps K_0 étant intègre, A est intègre. Soit K son corps des fractions. D'après la propriété universelle (P), l'homomorphisme $f : x \mapsto x$ de A dans K_0 se prolonge en un homomorphisme injectif $\overline{f}$ de K dans K_0. Alors $\overline{f}(K)$ est un corps qui contient $f(A) = A$ et on a $\overline{f}(K) \subset K_0$. Comme A engendre K_0, on en déduit que $\overline{f}(K) = K_0$. ∎

Remarques.

a) La terminologie "corps dés fractions" est un abus de langage : les éléments de K ne sont pas des fractions mais des classes de fractions équivalentes pour la relation $\mathcal{R}$.

On notera aussi que l'ensemble des fractions n'est pas un anneau, pas même un groupe additif, quand on le munit des opérations introduites. Ce n'est qu'en passant aux classes de fractions que la structure d'anneau se met en place.

b) Le corps des fractions de l'anneau intègre $\mathbb{Z}$ est $\mathbb{Q}$. Le rationnel classe d'une fraction $f = \frac{a}{b}$, où $a \in \mathbb{Z}$ et $b \in N_*$, est aussi la classe des fractions $\frac{2a}{2b}$, $\frac{3a}{3b}$, ... équivalentes à $\frac{a}{b}$. Parmi ces fractions équivalentes, il en existe une et une seule, telle que a et b soient premiers entre eux. On l'appelle la fraction réduite. On l'obtient en simplifiant par le pgcd de a et de b. Par exemple, $\frac{12}{270}$ a pour fraction réduite $\frac{2}{45}$.

Le rationnel, classe de $\frac{a}{b}$, admet un développement décimal fourni par la division euclidienne poursuivie indéfiniment. Rappelons qu'un réel est rationnel si et seulement si son développement décimal est périodique à partir d'un certain terme. Par exemple, le réel de développement décimal $0,333...$ est $\displaystyle\sum_{k=1}^{\infty} \frac{3}{10^k} = \frac{3}{10}\,\frac{1}{1-\frac{1}{10}} = \frac{1}{3}$.

c) On note $K(X)$ le corps des fractions de l'anneau $K[X]$ des polynômes à coefficients dans un corps K. C'est le corps des fractions rationnelles sur K. Ici aussi, les éléments de $K(X)$ ne sont pas des fractions mais les classes de fractions équivalentes.

d) Comme toujours pour une propriété universelle, le couple (K, φ) est le seul, à isomorphisme près, qui vérifie (P)

En effet, soit (K_1, φ_1) un autre couple vérifiant Appliquons la propriété (P) du couple (K, φ) à l'homomorphisme $\varphi_1 : A \to K_1$. On obtient un homomorphisme $\overline{\varphi_1} : K \to K_1$ tel que $\overline{\varphi_1} \circ \varphi = \varphi_1$. De même, la propriété (P) du couple (K_1, φ_1) appliquée à l'homomorphisme $\varphi : A \to K$ donne un homomorphisme $\overline{\varphi} : K_1 \to K$ tel que $\overline{\varphi} \circ \varphi_1 = \varphi$. En combinant ces relations, on obtient $\overline{\varphi} \circ \overline{\varphi_1} \circ \varphi = \varphi$. On a aussi $\mathrm{Id}_K \circ \varphi = \varphi$. L'unicité dans la propriété (P) donne $\overline{\varphi} \circ \overline{\varphi_1} = \mathrm{Id}_K$. De même, on a $\overline{\varphi_1} \circ \overline{\varphi} = \mathrm{Id}_{K_1}$. Ainsi, $\overline{\varphi}$ et $\overline{\varphi_1}$ sont deux isomorphismes réciproques entre K_1 et K.

Exercice 1. Soient $A = \mathbb{Z}$ et $S = \{10^k ; \ k \in \mathbb{N}\}$. Montrer que l'anneau $K = (A \times S)/\mathcal{R}$ des fractions est isomorphe à l'anneau $\mathbb{D}$ des nombres décimaux.

Solution. Evidemment S est multiplicativement stable et K existe. Appliquons la propriété universelle de K à l'homomorphisme injectif $f : n \mapsto \overline{n}$ de $\mathbb{Z}$ dans $\mathbb{Q}$, où $\overline{n}$ désigne la classe de la fraction $(n, 1)$ dans $\mathbb{Q}$. On obtient un homomorphisme injectif $\overline{f}$ de K dans $\mathbb{Q}$, dont l'image est l'ensemble $\mathbb{D}$ des rationnels classes des fractions $\frac{a}{10^k}$, où $a \in \mathbb{Z}$, $k \in \mathbb{N}$, c'est-à-dire l'ensemble des nombres décimaux.

Exercice 2. Soit $d \in \mathbb{Z} \setminus \{0, 1\}$ dont tous les facteurs premiers soient sans multiplicité. Soit $\delta \in \mathbb{C}$ une de ses racines carrées. Montrer que $A_d = \mathbb{Z} + \mathbb{Z}\delta$ est un sous-anneau de $\mathbb{C}$ et déterminer son corps des fractions.

Solution. Comme dans 9-9, ex. 2 pour le corps $\mathbb{Q}(\delta)$, on vérifie que $A_d = \mathbb{Z} + \mathbb{Z}\delta$ est un sous-anneau de $\mathbb{C}$. Considérons un élément $x = \frac{m}{n} + \frac{s}{t}\delta$ du corps $\mathbb{Q}(\delta)$, avec $m, s \in \mathbb{Z}$, $n, t \in N^*$. On a $ax = \frac{mt+ns\delta}{nt}$, avec $mt + ns\delta \in A_d$ et $nt \in A_d^*$. Ainsi, tout $x \in \mathbb{Q}(\delta)$ est élément du sous-corps K_0 de $\mathbb{C}$ engendré par A_d. Comme K_0 est le plus petit sous-corps de $\mathbb{C}$ contenant A_d, on a $K_0 = \mathbb{Q}(\delta)$. D'après le corollaire, $K_0 = \mathbb{Q}(\delta)$ est isomorphe au corps des fractions de A_d.

9.11 Quotient par un idéal maximal

Proposition.

Soit A un anneau commutatif unifère. Pour qu'un idéal I de A soit maximal, i1 faut et il sufiît que A/I soit un corps.

Démonstration.. D'après 9-9, l'anneau commutatif unifère A/I est un corps si et seulement si $\{0\}$ et A/I sont ses seuls idéaux. D'après 9-5, prop. (iii), cela signifie que I et A sont les seuls idéaux de A contenant 1, c'est-à-dire que I est maximal. ∎

Corollaire 1.

L'anneau $\mathbb{Z}/p\mathbb{Z}$est un corps si et seulement si $p \in N$ est premier.

Démonstration. Nous avons vu en 9-8, ex. et reverrons en 11-8, que l'idéal $p\mathbb{Z}$ de $\mathbb{Z}$ est maximal si et seulement si l'entier $p \in N$ est premier. ∎

Définition.

Soit A un anneau commutatif unifère. Un idéal I de A est dit premier, si $I \neq A$ et si la condition $xy \in I$ implique $x \in I$ ou $y \in$, c'est-à-dire si dans A/I la condition $\overline{x}\,\overline{y} = 0$ implique $olx = 0$ ou $\overline{y} = 0$, ce qui signifie que A/I est un anneau intègre.

Corollaire 2.

Tout idéal maximal de A est un idéal premier.

Démonstration. Si l'idéal I est maximal, A/I est un corps et donc intègre. Il n'y a pas de réciproque à cet énoncé : l'idéal $\{0\}$ de $\mathbb{Z}$ est premier et n'est pas maximal. ∎

9.12 Sous-corps premier d'un corps

Proposition.

Soient K un corps et p sa caractéristique. Il existe dans K un plus petit sous-corps K_0. Si $p = 0$, alors K_0 est isomorphe à $\mathbb{Q}$. Si $p \neq 0$, alors K_0 est isomorphe au corps $\mathbb{Z}/p\mathbb{Z}$.

Démonstration.. Soit $f : n \mapsto n1$ l'homomorphisme d'anneaux de $\mathbb{Z}$ dans K.

Supposons $p = 0$. L'homomorphisme f est injectif (Voir 9-1). D'après la propriété universelle du corps des fractions $\mathbb{Q}$ de $\mathbb{Z}$, f se prolonge en un homomorphisme injectif $\overline{f}$ de $\mathbb{Q}$ dans K. C'est donc un isomorphisme de $\mathbb{Q}$ sur un sous-corps K_0 de K. Les éléments de K_0 sont les images par $\overline{f}$ des rationnels $\frac{k}{m} \in \mathbb{Q}$. Tout sous-corps de K doit contenir 1, les multiples $k1$ de 1, où $k \in \mathbb{Z}$ et donc tous les éléments $(k1)(m1)^{-1}$, où $m \neq 0$, de $\overline{f}(\mathbb{Q})$. Ainsi, $\overline{f}(\mathbb{Q})$ est un plus petit sous-corps de K.

Supposons $p \neq 0$. Alors $p \in N^*$ est premier (Voir 9-1), $p\mathbb{Z}$ est un idéal maximal de $\mathbb{Z}$ (9-8, ex.) et $\mathbb{Z}/p\mathbb{Z}$ est un corps (9-11, cor. 1). Par factorisation de f, à travers son noyau $\mathrm{Ker}\,(f) = p\mathbb{Z}$, on obtient un homomorphisme injectif $\overline{f}$ de $\mathbb{Z}/p\mathbb{Z}$ sur $\mathrm{Im}\,(f) = \{n1 \mid n \in \mathbb{Z}\}$. Cette image K_0, isomorphe par $\overline{f}$ à $\mathbb{Z}/\mathrm{p}\mathbb{Z}$, est un sous-corps de K. Tout sous-corps de K contient $K_0 = \{k1\,;\ 0 \leqslant k \leqslant p-1\}$. ∎

Définition.

Ce plus petit sous-corps du corps K, isomorphe à $\mathbb{Q}$ ou à $\mathbb{Z}/p\mathbb{Z}$ avec p premier, est appelé le sous-corps premier de K.

Corollaire.

Le cardinal d'un corps fini K est une puissance p^m de sa caractéristique p.

Démonstration. Puisque K est fini, son sous-corps premier K_0 est fini, isomorphe à $\mathbb{Z}/p\mathbb{Z}$, avec p premier. Ses éléments $k1$, où $0 \leqslant k \leqslant p-1$, commutent avec tout élément de K. Si on fait opérer les éléments de K_0 par multiplication sur K, ce dernier est un espace vectoriel sur K_0. Etant fini, il est de dimension finie m. Soit $(e_1, \ldots, e_m)$ une base de K sur K_0. L'application linéaire $(x_1, \ldots, x_m) \mapsto x_1e_1 + \cdots + x_me_m$ est un isomorphisme d'espaces vectoriels de $(K_0)^m$ sur K. On voit que $\mathrm{card}\,(K) = p^m$. ∎

Exercices du chapitre 9

Ex 9 - 1

a) Soit A un anneau commutatif, unifère, ayant la propriété (P) suivante :

tout $x \in A \setminus \{1\}$ *est diviseur de zéro.*

Montrer que $\text{caract}(A) = 2$, et si A est un corps, que A est isomorphe à $\mathbb{Z}/2\mathbb{Z}$.

b) Soient A, B deux anneaux commutatifs, avec unité. Montrer que $A \times B$ a la propriété (P), si et seulement si A et B ont la propriété (P). Généraliser.

c) Soit A un anneau commutatif avec unité, booléen (tel que tout élément de A soit idempotent). Montrer que A a la propriété (P). Donner des exemples d'anneaux ayant la propriété (P).

Ex 9 - 2

Résoudre dans $\mathbb{Z}$ les systèmes :

$$(1)\ \begin{cases} 4x+9y \equiv 4 \pmod{48} \\ 3x+8y \equiv 7 \pmod{48} \end{cases},$$

$$(2)\ \begin{cases} 4x-11y \equiv 3 \pmod{48} \\ 3x+8y \equiv 4 \pmod{48} \end{cases}.$$

Ex 9 - 3

Soient $a, b, c, d \in \mathbb{Z}$. On considère les suites (x_n) et (y_n) de $\mathbb{Z}$ définies par la donnée de $x_0 \in \mathbb{Z}$ et $y_0 \in \mathbb{Z}$ et les relations de récurrence

$$x_{n+1} = ax_n + by_n \quad , \quad y_{n+1} = cx_n + dy_n .$$

Soit $N \in \mathbb{N}$, avec $N \geqslant 2$, premier avec $D = \begin{vmatrix} a & b \\ c & d \end{vmatrix}$. Montrer que les restes r_n et r'_n de la division de x_n et y_n par N constituent deux suites périodiques.

Ex 9 - 4

Notons C le groupe additif $(\mathbb{Z}, +)^n$.

a) Montrer que l'anneau $\text{End}(C)$ est isomorphe à $A = \mathcal{M}_n(\mathbb{Z})$.

b) Dans $A_* = \text{GL}(n, \mathbb{Z})$, montrer que

$$\text{SL}(n, \mathbb{Z}) = \{a \in A \mid \det(a) = 1\}$$

est un sous-groupe distingué d'indice 2.

c) Montrer que

$$f : (x, y) \mapsto (2x + y\,,\, 3x + 2y)$$

est un automorphisme du groupe $\mathbb{Z}^2$. Exprimer l'automorphisme réciproque f^{-1}. Pour $n = 3$, étudier de même

$g : (x, y, z) \mapsto (x', y', z')$ où

$$\begin{cases} x' = x + 2y + 3z \\ y' = 2x + 4y + 5z \\ z' = 2x + 5y + 6z \end{cases}.$$

Ex 9 - 5

On considère le groupe additif $(\mathbb{Z}/n\mathbb{Z}, +)$ et le groupe produit direct $C = (\mathbb{Z}/n\mathbb{Z})^k$.

a) Montrer que l'anneau $\text{End}(C)$ est isomorphe à l'anneau $A = \mathcal{M}_k(\mathbb{Z}/n\mathbb{Z})$.

En déduire la structure du groupe des automorphismes du petit groupe de Klein $(\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/2\mathbb{Z})$.

b) Montrer que le groupe $\text{Aut}(\mathbb{Z}/11\mathbb{Z}, +)$ des automorphismes du groupe additif $(\mathbb{Z}/11\mathbb{Z}, +)$ est cyclique. Donner les gérérateurs de ce groupe.

c) Etudier les endomorphismes et les automorphisme de l'anneau $\mathbb{Z}/n\mathbb{Z}$.

Ex 9 - 6

Soit A un anneau avec unité. On dit qu'un sous-anneau B de A est plein si $x^{-1} \in B$ pour tout $x \in B$ inversible dans A.

a) Si K est un corps, que sont les sous-anneaux pleins de K ?

b) Soit K un corps commutatif. Montrer que toute sous-algèbre unifère $\mathcal{A}$ de $\mathcal{M}_n(K)$ est pleine.

c) Soit $N \in \mathcal{M}_n(K)$. Dans $\mathcal{M}_{2n}(K)$, montrer que $M = \begin{pmatrix} N & I_n \\ I_n & N \end{pmatrix}$ est inversible si et seulement si 1 n'est pas valeur propre de N^2. Exprimer le polynôme caractéristique $P(\lambda)$ de M.

Ex 9 - 7

Montrer que $X = (x_1, x_2) \in \mathbb{Z}^2$ peut être inclus dans une base (X, Y) du réseau $\mathbb{Z}^2$ de $\mathbb{R}^2$ si et seulement si $x_1 \wedge x_2 = 1$.

Ex 9 - 8

Soit A un anneau commutatif unifère. Montrer que $a \in A$ est inversible si et seulement s'il n'appartient à aucun idéal maximal de A.

Ex 9 - 9

Soient A un anneau commutatif unifère et I un idéal de A. Montrer que le radical $r(I) = \{x \in A \ \exists k \in \mathbb{N} \ x^k \in I\}$ de I est un idéal de A. Que dire si I est premier ?

Indications

Ex 9 - 1

a) Utiliser la définition de caract(A).

b) et **c)** sont sans difficultés.

Ex 9 - 2

On résout des systèmes de Cramer sur l'anneau $\mathbb{Z}/48\mathbb{Z}$.

Ex 9 - 3

Dans le groupe fini $\mathrm{GL}(2, \mathbb{Z}/N\mathbb{Z})$, appliquer le th. de Lagrange à l'image de la matrice du système des relations de récurrence.

Ex 9 - 4

a) Démontrer la bijectivité de la correspondance entre matrices et endomorphismes du groupe $\mathbb{Z}^n$, comme en algèbre linéaire sur un corps.

b) On peut factoriser l'homomorphisme $a \mapsto \det(a)$.

c) Les matrices de ces endomorphismes de $\mathbb{Z}^2$ ou $\mathbb{Z}^3$ sont inversibles.

Ex 9 - 5

a) On a $\mathrm{End}(C) \simeq \mathcal{M}_k(\mathbb{Z}/n\mathbb{Z})$, comme dans Ex 9-4 a). Il existe 6 matrices inversibles dans $\mathcal{M}_2(\mathbb{Z}/2\mathbb{Z})$.

b) $\overline{2}$ est un générateur de $(\mathbb{Z}/11\mathbb{Z})_*$.

c) Choisir parmi les automorphismes du groupe additif $(\mathbb{Z}/n\mathbb{Z}, +)$.

Ex 9 - 6

a) On obtient les sous-corps.

b) On peut utiliser le th. de Cayley-Hamilton.

c) Considérer le déterminant $\det(M)$ à valeurs dans l'algèbre $\mathcal{A}$.

Ex 9 - 7

Utiliser le th. de Bezout.

Ex 9 - 8

Soit $a \in A$. On a $a \notin A_* \Leftrightarrow 1 \notin aA$. Alors aA est inclus dans un idéal maximal de A.

Ex 9 - 9

Pour I premier, on a $r(I) = I$.

Solutions des exercices du chapitre 9

Ex 9 - 1

a) Si -1 était diviseur de zéro, il existerait $b \neq 0$ tel que $0 = (-1)b = -b$. C'est absurde. Ainsi, -1 n'est pas diviseur de zéro. On a donc $-1 = 1$, soit $2 \times 1 = 0$. Ainsi, $\text{caract}(A) = 2$.

Si A est un corps, il est intègre. S'il vérifie (P), tout élément de A, distinct de 1, est nul. Donc $A = \{0,1\}$ est isomorphe à $\mathbb{Z}/2\mathbb{Z}$. Réciproquement $\mathbb{Z}/2\mathbb{Z}$ vérifie (P).

b) L'unité de $A \times B$ est $(1,1)$. Supposons que A et B vérifient (P). Soit $(x,y) \in A \times B$ distinct de $(1,1)$. On a $x \neq 1$ ou $y \neq 1$. Si par exemple $x \neq 1$, il existe $x' \neq 0$ dans A tel que $xx' = 0$. Alors $(x,y)(x',0) = (0,0)$ avec $(x',0) \neq (0,0)$. On raisonne de même si $y \neq 1$. Donc $A \times B$ vérifie (P).

Réciproquement, supposons que $A \times B$ vérifie (P). Soit $x \in A$ tel que $x \neq 1$. On a $(x,1) \neq (1,1)$. Il existe donc $(x',y') \in A \times B$ non nul tel que $(0,0) = (x,1)(x',y') = (xx',y')$, soit tel que $xx' = 0$ et $y' = 0$. On a $(x',y') = (x',0)$ non nul et donc $x' \neq 0$. Ainsi x est diviseur de zéro et A a la propriété (P). De même pour B.

Cette démonstration est encore valable pour un produit quelconque $\prod_{i \in I} A_i$ d'anneaux.

c) Si A est booléen, pour tout $x \in A$ on a $x^2 = x$, soit $x(1-x) = 0$. Si $x \neq 1$, alors $x' = 1 - x \neq 0$ et x est diviseur de zéro. Donc A vérifie (P).

D'après a), $\mathbb{Z}/2\mathbb{Z}$ a la propriété (P). D'après b), $(\mathbb{Z}/2\mathbb{Z})^k$ a la propriété (P) pour tout $k \in \mathbb{N}_*$. Plus généralement, c'est vrai pour $(\mathbb{Z}/2\mathbb{Z})^E = \mathcal{F}(E, \mathbb{Z}/2\mathbb{Z})$ ensemble des applications d'un ensemble E dans l'anneau $\mathbb{Z}/2\mathbb{Z}$, muni des opérations naturelles définies par

$$(f+g)(x) = f(x) + g(x) \quad , \quad (fg)(x) = f(x)g(x)\,.$$

Par ailleurs, ces anneaux sont booléens et c) donne la même conclusion.

Si une fonction f de E dans $\mathbb{Z}/2\mathbb{Z} = \{\overline{0}, \overline{1}\}$ est vue comme fonction indicatrice 1_A de la partie $A = \{x \in E\,;\, f(x) = \overline{1}\}$, nous avons vu en 1-10, ex., que $1_A + 1_B = 1_{A\Delta B}$ et $1_A 1_B = 1_{A \cap B}$, où $A\Delta B = (A \setminus B) \cup (B \setminus A)$. Cet anneau $\mathcal{F}(E, \mathbb{Z}/2\mathbb{Z})$ est donc isomorphe à l'anneau $\mathcal{P}(E)$ où l'addition est $A\Delta B$ et où le produit est $A \cap B$ (transport de la structure de $\mathcal{F}(E, \mathbb{Z}/2\mathbb{Z})$ sur $\mathcal{P}(E)$). Cet anneau est booléen.

Ex 9 - 2

Dans l'anneau $\mathbb{Z}/48\,\mathbb{Z}$, on cherche $\overline{x}, \overline{y}$ solutions de $\left\{ \begin{array}{rcrcl} \overline{4}\,\overline{x} & + & \overline{9}\,\overline{y} & = & \overline{4} \\ \overline{3}\,\overline{x} & + & \overline{8}\,\overline{y} & = & \overline{7} \end{array} \right.$.

On a $d = \begin{vmatrix} \overline{4} & \overline{9} \\ \overline{3} & \overline{8} \end{vmatrix} = \overline{5}$, inversible dans $\mathbb{Z}/48\mathbb{Z}$ car $5 \wedge 48 = 1$. Ce système de Cramer sur $\mathbb{Z}/48\mathbb{Z}$ a une seule solution. Or nous avons vu en 9-1, ex. 2 que $x = 1$, $y = 8$ vérifient $4x + 9y \equiv 7 \pmod{12}$ et $3x + 8y \equiv 7 \pmod{12}$. Ils vérifient donc ces relations modulo 48. Ainsi $(\overline{1}, \overline{8})$ est dans $\mathbb{Z}/48\mathbb{Z}$ l'unique solution. Les solutions du problème sont $x = 1 + 48p$, $y = 8 + 48q$ où $p, q \in \mathbb{Z}$.

Résolvons (2) par la méthode utilisée en 9-1, ex. 2. Le système obtenu dans $\mathbb{Z}/48\mathbb{Z}$ a pour déterminant $d = \overline{17}$. Par divisions,

$48 = 17 \times 2 + 14$, $17 = 14 + 3$, $14 = 3 \times 4 + 2$, $3 = 2 + 1$ d'où la relation de Bezout : $1 = 3 - 2 = 3 - (14 - 3 \times 4) = -14 + 3 \times 5 = \cdots = -48 \times 6 + 17 \times 17$.

Ainsi d est inversible dans $\mathbb{Z}/48\mathbb{Z}$, d'inverse $d^{-1} = \overline{17}$. En appliquant les formules de Cramer, on les solutions : $x = 4 + 48p$, $y = 23 + 48q$ où $p, q \in \mathbb{Z}$.

Ex 9 - 3

On a $D \wedge N = 1$, donc $\overline{D}$ est inversible dans l'anneau $A = \mathbb{Z}/N\mathbb{Z}$ et $\overline{M} = \begin{pmatrix} \overline{a} & \overline{b} \\ \overline{c} & \overline{d} \end{pmatrix}$ est un élément de $G = \mathrm{GL}(2, \mathbb{Z}/N\mathbb{Z})$. Ce groupe G est fini. Soit T l'ordre de $\overline{M}$ dans G. D'après le th. de Lagrange, on a $\overline{M}^T = I_2$. Donc $\overline{X}_n = (\overline{x}_n, \overline{y}_n)$, qui est donné par ${}^t\overline{X}_n = (\overline{M})^n \, ({}^t\overline{X}_0)$, admet pour période T, d'où le résultat.

Cela se généralise aux suites de $\mathbb{Z}^k$, où $k \in \mathbb{N}$, qui sont définies par des relations de récurrence linéaires à coefficients entiers.

Ex 9 - 4

a) Soit $a = (a_{ij}) \in A$. Pour $x = (x_1, \ldots, x_n) \in C = \mathbb{Z}^n$, notons encore x la matrice colonne de coefficients $x_1, \ldots, x_n$. Considérons $f_a : \mathbb{Z}^n \mapsto \mathbb{Z}^n$, définie par

$$f_a(x) = ax = \left(\sum_{j=1}^{n} a_{1j}x_j \, , \ldots , \sum_{j=1}^{n} a_{nj}x_j \right).$$

Le calcul matriciel est valable sur un anneau commutatif unifère. On a donc

$$f_a(x + x') = a(x + x') = ax + ax' = f_a(x) + f_a(x').$$

pour tous $x, x' \in \mathbb{Z}^n$. Ainsi, f_a est un endomorphisme du groupe additif C.

Pour tous $a, a' \in A$ et pour tout $x \in C$, on a

$f_{a+b}(x) = (a + b)x = ax + bx = f_a(x) + f_b(x)$,

$f_{ab}(x) = (ab)x = a(bx) = f_a(f_b(x))$.

On a donc $f_{a+b} = f_a + f_b$ et $f_{ab} = f_a \circ f_b$. Ainsi, $\varphi : a \mapsto f_a$ est un homomorphisme d'anneaux de $A = \mathcal{M}_n(\mathbb{Z})$ dans $\mathrm{End}\,(C)$ et $\varphi(1) = f_1 = \mathrm{Id}_C$.

$$a \in \mathrm{Ker}\,(\varphi) \quad \Leftrightarrow \quad f_a = 0 \quad \Leftrightarrow \quad \forall\, x \in C \quad ax = 0.$$

En prenant successivement les éléments $e_1 = (\overline{1}, \overline{0}, \ldots, \overline{0}), \ldots, e_n = (\overline{0}, \cdots, \overline{0}, \overline{1})$, on voit que si $a \in \mathrm{Ker}\,(\varphi)$, les colonnes de la matrice a sont toutes nulles et donc que $a = 0$. Ainsi, φ est injectif.

Soit $f \in \mathrm{End}\,(C)$. Considérons la matrice $a = (a_{ij})$ ayant pour colonnes, les coordonnées de $f(e_1), \ldots, f(e_n)$ dans $\mathbb{Z}^n$. On a $f_a(x) = f(x)$ pour tout $x \in \mathbb{Z}^n$ et donc $f_a = f$. Ainsi φ est est surjectif. C'est un isomorphisme d'anneaux.

b) Le groupe $\mathbb{Z}_*$ des éléments inversibles de l'anneau $\mathbb{Z}$ est $\mathbb{Z}_* = \{-1, 1\}$. Donc $A_* = \{a \in A \mid \det(a) \in \mathbb{Z}_*\}$ est le groupe $\mathrm{GL}(n, \mathbb{Z})$ des matrices de déterminant 1 ou -1. Or $\delta : a \mapsto \det(a)$ est un homomorphisme de groupes de A_* dans $\mathbb{Z}_*$ car $\det(ab) = \det(a)\det(b)$. Donc $\mathrm{Ker}\,(f) = \mathrm{SL}(n, \mathbb{Z})$ est un sous-groupe distingué de A_*. Il existe dans A des matrices diagonales de déterminant $+1$ et d'autres de déterminant -1. Donc f est surjectif. Par factorisation on obtient un isomorphisme $\overline{f} : A_*/\mathrm{SL}(n, \mathbb{Z}) \to \{-1, 1\}$. Ainsi $\mathrm{SL}(n, \mathbb{Z})$ est d'indice 2 et donc distingué. En fait, $A_* = \mathrm{GL}(n, \mathbb{Z})$ est isomorphe à un produit semi-direct de $\mathrm{SL}(n, \mathbb{Z})$ par $\mathbb{Z}/2\mathbb{Z}$ car il existe un homomorphisme $\tau : \{-1, 1\} \to A_*$ tel que $\det \circ \tau = \mathrm{Id}$. Par exemple, si $n = 2$,

$$\tau(1) = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \qquad \text{et} \qquad \tau(-1) = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}.$$

c) L'endomorphisme f_a, où $a \in \mathcal{M}_n(\mathbb{Z})$ est un isomorphisme si et seulement a est inversible. La matrice a^{-1} donnera alors l'isomorphisme réciproque $(f_a)^{-1} = f_{a^{-1}}$. On a $\det(a) = 1 \in \mathbb{Z}_*$ donc a est inversible. Si $a = \begin{pmatrix} 2 & 1 \\ 3 & 2 \end{pmatrix}$ alors $a^{-1} = \begin{pmatrix} 2 & -1 \\ -3 & 2 \end{pmatrix}$, d'où $f^{-1} : (x, y) \mapsto (\,2x - y\,,\ -3x + 2y\,)$.

De même, la matrice b de g, a pour déterminant 1, inversible dans l'anneau $\mathbb{Z}$.

Donc $b = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 4 & 5 \\ 2 & 5 & 6 \end{pmatrix}$ est inversible dans $\mathcal{M}_n(\mathbb{Z})$ et $b^{-1} = \begin{pmatrix} -1 & 3 & -2 \\ -2 & 0 & 1 \\ 2 & -1 & 0 \end{pmatrix}$

(utiliser par exemple la formule des cofacteurs), d'où l'expression de l'isomorphisme réciproque :

$$g^{-1} : (x, y, z) \mapsto (\,-x + 3y + 2z\,,\ -2x + z\,,\ 2x - y\,).$$

Ex 9 - 5

a) Comme dans l'exercice précédent pour $\mathbb{Z}^n$, on voit que l'application associant à tout élément de $\mathrm{End}\,(C)$, où $C = (\mathbb{Z}/n\mathbb{Z})^k$, sa "matrice" dans la "base" canonique de $(\mathbb{Z}/n\mathbb{Z})^k$, est un isomorphisme de $\mathrm{End}\,(C)$ sur l'anneau $A = \mathcal{M}_k(\mathbb{Z}/n\mathbb{Z})$.

Si $C = (\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/2\mathbb{Z})$ le groupe $\mathrm{Aut}\,(C)$ des unités de l'anneau $\mathrm{End}\,(C)$ est isomorphe au groupe A_* des matrices $a \in \mathcal{M}_2(\mathbb{Z}/2\mathbb{Z})$ inversibles. Pour que $a = (\overline{a}_{ij}) \in \mathcal{M}_2(\mathbb{Z}/2\mathbb{Z})$ soit inversible, il faut et il suffit que $\det(a) = \overline{a}_{11}\,\overline{a}_{22} - \overline{a}_{12}\,\overline{a}_{21}$ soit égal à $\overline{1}$ (non nul dans $\mathbb{Z}/2\mathbb{Z}$). C'est possible si $\overline{a}_{11}\,\overline{a}_{22} = \overline{1}$ et $\overline{a}_{12} = \overline{0}$ ou $\overline{a}_{21} = \overline{0}$, ce qui détermine 3 matrices

$$\begin{pmatrix} \overline{1} & \overline{0} \\ \overline{0} & \overline{1} \end{pmatrix} \quad , \quad \begin{pmatrix} \overline{1} & \overline{1} \\ \overline{0} & \overline{1} \end{pmatrix} \quad , \quad \begin{pmatrix} \overline{1} & \overline{0} \\ \overline{1} & \overline{1} \end{pmatrix},$$

ou bien si $\overline{a}_{12}\,\overline{a}_{21} = \overline{1}$ et $\overline{a}_{11} = \overline{0}$ ou $\overline{a}_{22} = \overline{0}$, ce qui fournit 3 matrices

$$\begin{pmatrix} \overline{0} & \overline{1} \\ \overline{1} & \overline{0} \end{pmatrix} \quad , \quad \begin{pmatrix} \overline{1} & \overline{1} \\ \overline{1} & \overline{0} \end{pmatrix} \quad , \quad \begin{pmatrix} \overline{0} & \overline{1} \\ \overline{1} & \overline{1} \end{pmatrix}.$$

Il existe donc 6 matrices inversibles dans A. L'ordre du groupe $\mathrm{Aut}\,((\mathbb{Z}/2\mathbb{Z}) \times \mathbb{Z}/2\mathbb{Z}))$ est 6. Un groupe d'ordre 6 est isomorphe à $\mathbb{Z}/6\mathbb{Z}$ s'il est abélien ou à $\mathcal{S}_3$ s'il n'est pas abélien. Certaines des matrices précédentes ne commutent pas. Donc $\mathrm{Aut}\,\big((\mathbb{Z}/2\mathbb{Z})^2\big)$ est isomorphe à $\mathcal{S}_3$ (résultat déjà vu dans Ex. 1-4).

b) Par l'isomorphisme $\varphi : a \mapsto f_a$, les unités de l'anneau $\mathbb{Z}/n\mathbb{Z}$ sont associées aux unités de l'anneau $\mathrm{End}(\mathbb{Z}/n\mathbb{Z},+)$, c'est-à-dire aux éléments de $\mathrm{Aut}(\mathbb{Z}/n\mathbb{Z},+)$. Les automorphismes du groupe cyclique $(\mathbb{Z}/n\mathbb{Z},+)$ sont donc de la forme $\overline{x} \mapsto \overline{k}\overline{x}$ où $\overline{k} \in \mathbb{Z}/n\mathbb{Z}$, avec $k \wedge n = 1$. Donc $[\mathrm{Aut}(\mathbb{Z}/n\mathbb{Z},+) : 1] = [(\mathbb{Z}/n\mathbb{Z})_* : 1] = \varphi(n)$ où φ désigne la fonction d'Euler. Ce résultat avait été vu dans l'étude des groupes cycliques : l'image $\overline{k} = \alpha(\overline{1})$ du générateur $\overline{1}$ de $(\mathbb{Z}/n\mathbb{Z},+)$ par un automorphisme α de $(\mathbb{Z}/n\mathbb{Z},+)$ est un autre générateur et la donnée de $\alpha(\overline{1}) = \overline{k}$ détermine α.

Si $p = 11$ alors $(\mathbb{Z}/p\mathbb{Z})_*$ est un groupe d'ordre $\varphi(11) = 11 - 1 = 10 = 2 \times 5$. L'ordre $o(\overline{2})$ de $\overline{2}$ divise $[(\mathbb{Z}/11\mathbb{Z})_* : 1] = 10$ donc $o(\overline{2}) \in \{2,5,10\}$. Comme $\overline{2}^2 = \overline{4}$, $\overline{2}^5 = \overline{10} = -\overline{1}$ on a $o(\overline{2}) = 10$. Ainsi $\overline{2}$ engendre $(\mathbb{Z}/11\mathbb{Z})_*$. L'automorphisme de $(\mathbb{Z}/11\mathbb{Z},+)$ correspondant est $f : \overline{x} \mapsto \overline{2}\,\overline{x} = \overline{2x}$. Il engendre $\mathrm{Aut}(\mathbb{Z}/11\mathbb{Z},+)$. Les automorphismes de $(\mathbb{Z}/11\mathbb{Z},+)$ sont les puissances $f^k : \overline{x} \mapsto \overline{2}^k\,\overline{x}$ de f, où $0 \leqslant k \leqslant 9$. Pour que f^k engendre $\mathrm{Aut}(\mathbb{Z}/11\mathbb{Z},+)$ il faut et il suffit que $k \wedge 10 = 1$.

Si p est premier, $\mathbb{Z}/p\mathbb{Z}$ est un corps. On verra en 10-7, que le groupe multiplicatif $(\mathbb{Z}/p\mathbb{Z})_*$ est cyclique. Le groupe $\mathrm{Aut}(\mathbb{Z}/p\mathbb{Z},+)$ qui lui est isomorphe est cyclique.

c) Si f est un endomorphisme de l'anneau $\mathbb{Z}/n\mathbb{Z}$, c'est en particulier un endomorphisme du groupe additif $(\mathbb{Z}/n\mathbb{Z},+)$. Il est donc de la forme $f : \overline{x} \mapsto \overline{k}\overline{x}$. De plus, pour tous $\overline{x},\overline{y} \in \mathbb{Z}/n\mathbb{Z}$ on doit avoir $f(\overline{xy}) = f(\overline{x})f(\overline{y})$, soit $\overline{k}\overline{xy} = \overline{k}\overline{x}\overline{k}\overline{y}$. Pour cela il faut et il suffit que $\overline{k} = \overline{k}^2$. Si n est premier, alors $\mathbb{Z}/n\mathbb{Z}$ est un corps. Le polynôme $X^2 - X$ aura pour seules racines $\overline{1}$ et $\overline{0}$. Si n n'est pas premier, ce polynôme peut avoir d'autres racines dans $\mathbb{Z}/n\mathbb{Z}$. Par exemple, on a $\overline{3}^2 = \overline{3}$ dans $\mathbb{Z}/6\mathbb{Z}$.

Si f est un automorphisme de l'anneau $\mathbb{Z}/n\mathbb{Z}$, alors étant surjectif, on a nécessairement $f(\overline{1}) = \overline{1}$, d'où $\overline{k} = \overline{1}$ et $f = \mathrm{Id}$.

Ex 9 - 6

a) Un sous-anneau B d'un corps K est plein si $x^{-1} \in B$ pour tout $x \in B$ non nul, c'est-à-dire si B est un sous-corps de K.

b) Soient $A \in \mathcal{A}$ inversible dans $\mathcal{M}_n(K)$ et $p(X) = X^n + \cdots + \alpha_1 X + \alpha_0 = \det(XI_n - A)$ son polynôme caractéristique. On a $\det(A) \neq 0$ et donc $\alpha_0 = (-1)^n \det(A) \neq 0$. D'après le th. de Cayley-Hamilton $p(A) = 0$ donc $A\left[-\frac{1}{\alpha_0}A^{n-1} - \cdots - \frac{\alpha_1}{\alpha_0}\right] = I_n$. L'inverse de A est une expression polynomiale de A et donc un élément de $\mathcal{A}$.

c) Soit $\mathcal{A}$ la sous-algèbre unifère de $\mathcal{M}_n(K)$ engendrée par N. D'après b), $M = \begin{pmatrix} N & I_n \\ I_n & N \end{pmatrix}$ est inversible dans $\mathcal{M}_{2n}(K)$ si et seulement si elle est inversible dans la sous-algèbre $\mathcal{M}_2(\mathcal{A})$ de $\mathcal{M}_{2n}(K)$. D'après 9-1, prop., pour cela il faut et il suffit que $\det(M) = N^2 - I_n$ soit inversible dans l'algèbre $\mathcal{A}$. D'après b), cela équivaut à l'inversibilité de $N^2 - I_n$ dans $\mathcal{M}_n(K)$, d'où la condition $\det(N^2 - I_n) \neq 0$, qui signifie que 1 n'est pas une valeur propre de N^2. Des manipulations sur les lignes et les colonnes dans l'algèbre $\mathcal{M}_2(\mathcal{A})$ conduit aux mêmes conclusions :

$$\begin{pmatrix} I_n & 0 \\ -N & I_n \end{pmatrix}\begin{pmatrix} 0 & I_n \\ I_n & 0 \end{pmatrix}\begin{pmatrix} N & I_n \\ I_n & N \end{pmatrix}\begin{pmatrix} I_n & -N \\ 0 & I_n \end{pmatrix} = \begin{pmatrix} I_n & 0 \\ 0 & I_n - N^2 \end{pmatrix}.$$

De même, $M - \lambda I_{2n}$ est non inversible, si et seulement si

$$\det\begin{pmatrix} N - \lambda I_n & I_n \\ I_n & N - \lambda I_n \end{pmatrix} = (N - \lambda I_n)^2 - I_n \notin \mathcal{A}_*,$$

soit si $P(\lambda) = \det[\,(N - \lambda I_n)^2 - I_n\,] = 0$.

Ex 9 - 7

Dans $\mathbb{Z}^2$ il existe une "base" canonique $\mathcal{B}$ constituée de $e_1 = (1,0)$ et $e_2 = (0,1)$. La matrice des coordonnées de $X = (x_1, x_2) = x_1e_1 + x_2e_2$ et $Y = (y_1, y_2) = y_1e_1 + y_2e_2$ est $P = \begin{pmatrix} x_1 & y_1 \\ x_2 & y_2 \end{pmatrix}$. Si $\mathcal{B}' = (X, Y)$ est une autre "base", alors il existe $u_1, u_2, v_1, v_2 \in \mathbb{Z}$ uniques tels que $e_1 = u_1X + u_2Y$, $e_2 = v_1X + v_2Y$. Substituons ces expressions dans les précédentes. En utilisant l'unicité de l'expression dans la "base" $\mathcal{B}$, on voit que $\begin{pmatrix} x_1 & y_1 \\ x_2 & y_2 \end{pmatrix} \begin{pmatrix} u_1 & v_1 \\ u_2 & v_2 \end{pmatrix} = I_2$. De même, $\begin{pmatrix} u_1 & v_1 \\ u_2 & v_2 \end{pmatrix} \begin{pmatrix} x_1 & y_1 \\ x_2 & y_2 \end{pmatrix} = I_2$. Ainsi $P \in \mathrm{GL}(2,\mathbb{Z})$.

Réciproquement si $P \in \mathrm{GL}(2,\mathbb{Z})$, en utilisant P et P^{-1}, on voit que tout élément de $\mathbb{Z}^2$ a une expression unique dans la "base" canonique $\mathcal{B}$ et une expression unique en fonction de X et Y. Donc (X, Y) est une "base" de $\mathbb{Z}^2$. En conclusion, (X, Y) est une base de $\mathbb{Z}^2$ si et seulement si $P \in \mathrm{GL}(2,\mathbb{Z})$. D'après 9-1, prop., pour cela il faut et il suffit que $\det(P)$ soit inversible dans l'anneau $\mathbb{Z}$. Comme $\mathbb{Z}_* = \{1, -1\}$, on pourra inclure X dans un base (X, Y) de $\mathbb{Z}^2$ si et seulement si il existe $y_1 \in \mathbb{Z}$ et $y_2 \in \mathbb{Z}$ tels que $x_1y_2 - x_2y_1 = \pm 1$. D'après le th. de Bezout (voir 11-4), cela est possible si et seulement si x_1 et x_2 sont premiers entre eux.

Ex 9 - 8

Si $a \in A$ est inversible, on a $aA = A$. Si un idéal I contient a, on a $I = A$. Donc a n'appartient à aucun idéal distinct de A et n'appartient donc à aucun idéal maximal.

Réciproquement, supposons que $a \in A$ n'appartienne à aucun idéal maximal. Si on avait $aA \neq A$, il existerait un idéal maximal contenant aA et contenant donc a. C'est exclu. Donc $aA = A$ et $a \in A_*$.

Ex 9 - 9

Soient $x, y \in r(I)$. Il existe $m, n \in \mathbb{N}$ tels que $x^m \in I$ et $y^n \in I$. Alors :

$$(x-y)^{m+n} = \sum_{p+q=m+n} (-1)^q \, C^p_{m+n} \, x^p y^q .$$

Dans chaque terme de cette somme, on a $m \leqslant p$ ou $n \leqslant q$ (sinon $p + q < m + n$). De ce fait on a $x^p y^q = x^m (x^{p-m} y^n) \in I$ ou $x^p y^q = x^p y^{q-n} y^n \in I$. Cela montre que $(x-y)^{m+n} \in I$ et que $x - y \in r(I)$. Comme $0 \in r(I)$, on a vérifié que $r(I)$ est un sous-groupe de $(A, +)$.

Pour tout $a \in A$, on a $(xa)^m = x^m a^m \in I$ donc $xa \in r(I)$. Le radical $r(I)$ de I est un idéal de A. Si $I = \{0\}$, nous venons de vérifier, en particulier, que dans l'anneau A, l'ensemble $\mathrm{rad}(A) = r(\{0\}) = \{\, x \in A \mid \exists\, n \in \mathbb{N} \quad x^n = 0 \,\}$ des éléments nilpotents constituent un idéal de A.

Notons que l'on a $I \subset r(I)$. En notant φ l'homomorphisme canonique de A sur A/I, on voit donc que $r(I) = \varphi^{-1}(rad(A/I))$.

Supposons que I soit un idéal premier. On voit par récurrence sur k, que si $x_1 \cdots x_k \in I$, alors l'un des éléments $x_1, \ldots, x_k$ appartient à I. Pour tout $x \in r(I)$ il existe $n \in \mathbb{N}^*$ tel que $x^n \in I$ donc $x \in I$. Ainsi, on a $r(I) \subset I$ et donc $r(I) = I$. D'ailleurs, I est premier si et seulement si A/I est intègre. On a alors $\mathrm{rad}(A/I) = \{0\}$ et donc $r(I) = \varphi^{-1}(\mathrm{rad}(A/I)) = I$.

Chapitre 10

Anneaux de polynômes

10.1 Polynômes à coefficients dans un anneau

Définition.

Soit A est un anneau commutatif, unifère. On appelle polynôme à coefficients dans A, une suite infinie $a = (a_0, a_1, \ldots)$ d'éléments de A, dont tous les termes sont nuls, sauf un nombre fini d'entre eux.

Le plus grand indice n tel que $a_n \neq 0$ est appelé le *degré* du polynôme a. Nous le noterons $\mathrm{d}^\circ(a)$. Si $a = 0$, soit $a_k = 0$ pour tout $k \in \mathbb{N}$, on convient que $\mathrm{d}^\circ(a) = -\infty$.

Si $a_n = 1$, où $n = \mathrm{d}^\circ(a)$, on dit que le polynôme a est unitaire.
On note $A[X]$ l'ensemble des polynômes à coefficients dans l'anneau commutatif A.
On définit la somme de deux polynômes $a = (a_0, a_1, ...)$ et $b = (b_0, b_1, ...)$ de $A[X]$ comme étant la somme des deux suites au sens habituel, soit :

$$a + b = (a_0 + b_0, a_1 + b_1, \ldots)$$

Le produit ab est le polynôme $c = (c_0, c_1, \ldots)$ où pour tout $k \in \mathbb{N}$ on pose

$$c_k = a_0 b_k + a_1 b_{k-1} + \cdots + a_k b_0 \,.$$

On a évidemment

$$\mathrm{d}^\circ(a+b) \leqslant \max(\mathrm{d}^\circ(a), \mathrm{d}^\circ(b)) \quad , \qquad \mathrm{d}^\circ(ab) \leqslant \mathrm{d}^\circ(a) + \mathrm{d}^\circ(b) \,.$$

Proposition.

Soit A un anneau commutatif avec unité.

(i) *$A[X]$ est une A-algèbre commutative, ayant pour unité $\mathbb{1} = (1, 0, 0, \ldots)$. L'homomorphisme injectif $j : a \mapsto (a, 0, 0, \ldots) = a\mathbb{1}$ de A dans $A[X]$ permet d'identifier A avec le sous-anneau de $A[X]$ constitué des polynômes constants.*

(ii) *Les polynômes 1 et $X = (0, 1, 0, \ldots)$ engendrent $A[X]$: tout $a = (a_0, a_1, \ldots)$ de degré n dans $A[X]$, a pour expression $a = a_0 + a_1 X + \cdots + a_n X^n$.*

(iii) *$A[X]$ est intègre si et seulement si A est intègre. Alors, $\mathrm{d}^\circ(ab) = \mathrm{d}^\circ(a) + \mathrm{d}^\circ(b)$ pour tout $a \in A$, tout $b \in A$ et les unités de $A[X]$ sont les polynômes constants dont la valeur a_0 est élément de A_*.*

Démonstration. (i) La définition de l'addition dans $A[X]$ montre que $A[X]$ est un sous-groupe du groupe additif $A^{\mathbb{N}}$ des suites à valeurs dans A.

Soient $a, b, c \in A[X]$. Pour tout $n \in \mathbb{N}$, le coefficient au degré n de $a(bc)$ est $\sum_{p+k=n} a_p(bc)_k = \sum_{p+k=n} a_p \left(\sum_{q+r=k} b_q c_r\right) = \sum_{p+q+r=n} a_p b_q c_r$. Il est égal à celui de $(ab)c$. On a donc $a(bc) = (ab)c$ et le produit est associatif.

Si a, a', b sont des éléments de $A[X]$, alors le coefficient au degré n de $ab + a'b$ est $(a_0b_n + a_1b_{n_1} + \cdots + a_nb_0) + (a'_0b_n + a'_1b_{n-1} + \cdots + a'_nb_0)$
$= (a_0 + a'_0)b_n + \cdots + (a_n + a'_n)b_0$,
donc $ab + a'b = (a + a')b$. Le produit distribue donc l'addition.

L'expression du coefficient c_k de $c = ab$ montre que le produit est commutatif. Si $b_0 = 1$ et $b_i = 0$ pour $i \geqslant 1$, alors $c_k = a_k$ pour tout $k \in \mathbb{N}$ donc $a\mathbb{1} = a$. Ainsi $\mathbb{1}$ est élément neutre pour le produit et $A[X]$ est un anneau commutatif unifère et une A-algèbre. Il est clair que j est un homomorphisme d'anneaux injectif de A dans $A[X]$.

(ii) Le coefficient au degré n de X^2 est $\sum_{p=0}^{n} \delta_{1,p}\delta_{1,n-p} = \delta_{1,n-1}$. Sa valeur est un si $n = 2$, zéro sinon. Donc $X^2 = (0, 0, 1, 0, \ldots)$. Par récurrence on montre de même que X^k est la suite $(0, \ldots, 0, 1, 0, \ldots)$, où 1 est le coefficient au degré k. En identifiant à l'aide de j tout élément a de A avec le polynôme constant $a\mathbb{1} = (a, 0, 0, ...)$, tout polynôme $a = (a_0, a_1, a_2, \ldots, a_n, 0, \ldots)$ de degré n, est égal à $ao + a_1X + a_2X^2 + \cdots + a_nX^n$.

(iii) Si $\mathrm{d}^\circ(a) = p \in \mathbb{N}$ et si $\mathrm{d}^\circ(b) = q \in \mathbb{N}$, le coefficient c_k de ab est nul pour tout $k > p + q$ et $c_{p+q} = a_pb_q$. Si A est intègre, $c_{p+q} = a_pb_q \neq 0$ et donc $\mathrm{d}^\circ(ab) = \mathrm{d}^\circ(a) + \mathrm{d}^\circ(b)$. Cette formule est encore valable si a ou b est nul. Cette propriété montre en particulier que l'anneau $A[X]$ est intègre. Réciproquement, si $A[X]$ est intègre alors A est intègre car d'après (i) il s'identifie à un sous-anneau de $A[X]$.

Pour avoir $ab = \mathbb{1}$, il faut que $p + q = 0$ (soit $p = 0$ et $q = 0$) et que $a_0b_0 = 1$ (soit $a_0 \in A_*$ et $b_0 = a_0^{-1}$). Ainsi a est une unité de $A[X]$ si et seulement si a est un polynôme constant égal à une unité a_0 de A. ∎

Exercice 1. Soient A, B deux anneaux avec unités, commutatifs. Soit $\varphi : A \to B$ un homomorphisme tel que $\varphi(1) = 1$. A tout $p = a_0 + \cdots + a_nX^n \in A[X]$ on associe le polynôme $\Phi(p) = \varphi(ao) + \cdots + \varphi(a_n)X^n$. Montrer que Φ est un homomorphisme d'anneaux de $A[X]$ dans $B[X]$. Quel est son noyau ?

Solution. Soient $a = \sum a_kX^k$, $b = \sum b_kX^k$ des éléments de $A[X]$. On a alors $\Phi(a + b) = \Phi(a) + \Phi(b)$ car pour tout degré k les coefficients $\varphi(a_k + b_k)$ et $\varphi(a_k) + \varphi(b_k)$ de ces polynômes sont égaux. De même,

$$\Phi(ab) = \Phi(a)\Phi(b) \quad \text{car} \quad \varphi(\sum_{i=0}^{k} a_ib_{k-i}) = \sum_{i=0}^{k} \varphi(a)\varphi(b_{k-i}) .$$

De plus $\Phi(\mathbb{1}) = \mathbb{1}$. Le noyau de Φ est $I[X]$ où $I = \mathrm{Ker}\,(\varphi)$ car

$$a \in \mathrm{Ker}\,(\Phi) \quad \Leftrightarrow \quad \forall i \quad \varphi(a_i) = 0 \quad \Leftrightarrow \quad a_0, \ldots, a_n \in \mathrm{Ker}\,(\varphi) .$$

Exercice 2. Soit $n \in \mathbb{N}^*$, distinct de 1, non premier. Montrer que l'anneau $A = \mathbb{Z}/n\mathbb{Z}$ n'est pas intègre. Pour $n = 4$, montrer que les propriétés (iii) de la proposition sont en défaut dans $\mathbb{Z}/4\mathbb{Z})[X]$.

Solution. Puisque n n'est pas premier, il existe $a \in \mathbb{N}$, $b \in \mathbb{N}$, tels que $n = ab$, avec $1 < a \leqslant b < n$. On a $\overline{a} \neq \overline{0}$, $\overline{b} \neq \overline{0}$, $\overline{a}\overline{b} = \overline{0}$ donc $\mathbb{Z}/n\mathbb{Z}$ n'est pas intègre.
On a $(\overline{2}X)(\overline{2}X) = \overline{0}$. Donc $(\mathbb{Z}/4\mathbb{Z})[X]$ n'est pas intègre et la règle (iii) concernant le degré d'un produit est fausse. On a $(\overline{1} + \overline{2}X)(\overline{1} + \overline{2}X) = \overline{1}$ donc $\overline{1} + \overline{2}X$, non constant, est une unité de $A[X]$.

10.2 Division euclidienne

Proposition.

Soient A un anneau commutatif unifère et $b = b_0 + \cdots + b - mX^m \in A[X]$ avec b_m, inversible. Pour tout $a \in A[X]$, il existe $q \in A[X]$ et $r \in A[X]$ uniques tels que

$$a = bq + r \quad \textit{et} \quad \mathrm{d}^\circ(r) < \mathrm{d}^\circ(b)\ .$$

De plus on a $\mathrm{d}^\circ(q) = \mathrm{d}^\circ(a) - \mathrm{d}^\circ(b)$.

Démonstration. Cette division euclidienne s'effectue selon l'algorithme bien connu. Soit $a \in A[X]$. Montrons l'existence de q et r par récurrence sur le degré n de a.

Si $\mathrm{d}^\circ(a) = 0$, c'est à dire si a est constant, on prendra :
$q = 0$ et $r = a$ si $\mathrm{d}^\circ(b) > 0$,
$q = b^{-1}a$ et $r = 0$ si $\mathrm{d}^\circ(b) = 0$ (q existe car on a $b \in A_*$, par hypothèse).

Soit $n \in \mathbb{N}^*$. Supposons établie l'existence de q, r pour tout polynôme a de degré $\mathrm{d}^\circ(a) \leqslant n-1$. Considérons $a(X) = a_n X^n + \cdots + a\circ$ de degré n. Si on a $\mathrm{d}^\circ(a) < \mathrm{d}^\circ(b)$, le choix $q = 0$ et $r = a$ convient. Si $\mathrm{d}^\circ(a) \geqslant \mathrm{d}^\circ(b)$, considérons $a_1 = a - [a_n b_m^{-1} X^{n-m}]b$. Le degré de a_1 est majoré par le plus grand des degrés des deux termes de cette différence. Il est donc inférieur ou égal à n. Par ailleurs, il n'y a plus de monôme de degré n dans a_1. On a donc $\mathrm{d}^\circ(a_1) \leqslant n-1$. D'après l'hypothèse de récurrence, il existe $q_1, r_1 \in A[X]$ tels que $a_1 = bq_1 + r_1$ avec $\mathrm{d}^\circ(r_1) < \mathrm{d}^\circ(b)$ et $\mathrm{d}^\circ(q1) = \mathrm{d}^\circ(a_1) - \mathrm{d}^\circ(b) \leqslant n - 1 - m$. Alors $q = a_n b_m^{-1} X^{n-m} + q_1$ et $r = r_1$ conviennent et $\mathrm{d}^\circ(q) = n - m = \mathrm{d}^\circ(a) - \mathrm{d}^\circ(b)$.

Montrons l'unicité de q et r. Considérons q', r' avec des propriétés analogues. Par soustraction, les relations $a = bq + r$ et $a = bq' + r'$ donnent $b(q - q') = r' - r$. Supposons $q - q' \neq 0$ de degré k et soit q_k le coefficient de X^k dans $q - q'$. Comme b_m est inversible, on a $b_m q_k \neq 0$, d'où $\mathrm{d}^\circ(b(q-q')) = \mathrm{d}^\circ(b) + \mathrm{d}^\circ(q-q')$. Comme $\mathrm{d}^\circ(r) < \mathrm{d}^\circ(b)$ et $\mathrm{d}^\circ(r') < \mathrm{d}^\circ(b)$, on obtient $\mathrm{d}^\circ(r'-r) < \mathrm{d}^\circ(b) \leqslant \mathrm{d}^\circ(b(q--q')) = \mathrm{d}^\circ(r'-r)$, ce qui est absurde. On a donc $q - q' = 0$ et $r' - r = 0$. ∎

Exercice 1. Effectuer la division de $a(X) = X^7 + X^6 + X^5 + X^4 + X^2 - 1$ par $b(X) = X^5 - X^2 + 1$ dans l'anneau $\mathbb{Z}[X]$. En déduire le reste et le quotient de la division dans $(\mathbb{Z}/2\mathbb{Z})[X]$ pour les polynômes ayant la même expression que a et b.

Solution. $a = bq + r$ où $q(X) = X^2 + X + 1$, $r(X) = 2X^4 + X^3 + X^2 - X - 2$. Soit φ l'homomorphisme canonique $\varphi : n \mapsto \overline{n}$ de $\mathbb{Z}$ dans $\mathbb{Z}/2\mathbb{Z}$. D'après 10-1, ex. 1, on obtient $\Phi(a) = \Phi(b)\Phi(q) + \Phi(r)$ avec $\mathrm{d}^\circ(\Phi(r)) \leqslant \mathrm{d}^\circ(r)) < \mathrm{d}^\circ(b) = \mathrm{d}^\circ(\Phi(b))$. Donc $\Phi(q) = X^2 + X + \overline{1}$ et $\Phi(r) = X^3 + X^2 + X$ sont le quotient et le reste dans $(\mathbb{Z}/2\mathbb{Z})[X]$.

Exercice 2. Pour $n \in \mathbb{N}$, calculer A^n où $A = \begin{pmatrix} 4 & 3 \\ -2 & -1 \end{pmatrix} \in \mathcal{M}_2(\mathbb{R})$.

Solution. D'après le th. de Cayley-Hamilton, le polynôme caractéristique de A :

$$p(X) = X^2 - \mathrm{tr}(A)X + \det(A) = X^2 - 3X + 2 = (X-1)(X-2),$$

est tel que $p(A) = 0$. Par division euclidienne, $X^n = p(X)q(X) + \alpha X + \beta$. Pour $X = 1$ puis $X = 2$, on obtient $1 = \alpha + \beta$, $2^n = 2\alpha + \beta$, d'où $\alpha = 2^n - 1$, $\beta = 2 - 2^n$ et $A^n = p(A)q(A) + \alpha A + \beta I_2 = (2^n - 1)A + (2 - 2^n)I_2$.

10.3 Fonction polynomiale et racines d'un polynôme

Définition.

Soit A un anneau commutatif avec unité. Tout $p \in A[X]$ d'expression $p = a_0 + a_1X + \cdots + anX^n$ définit une application $\tilde{p} : \lambda \mapsto a_0 + a_1\lambda + \cdots + a_n\lambda^n$ de A dans A appelée la fonction polynomiale définie par p.

On dit que $\lambda \in A$ est racine d'un polynôme p (non nul) si $\tilde{p}(\lambda) = 0$.

On dit qu'un corps K est algébriquement clos si tout $p \in K[X]$, non constant, admet une racine dans K. Le corps $\mathbb{C}$ est algébriquement clos (th. de d 'Alembert).

Soient $p = a_0 + \cdots + a - mX^m$ et $q = b_0 + \cdots + b_nX^n$ des éléments de $A[X]$. On a

$$\widetilde{(p+q)}(\lambda) = \tilde{p}(\lambda) + \tilde{q}(\lambda) \quad , \quad (\widetilde{pq})(\lambda) = \tilde{p}(\lambda)\tilde{q}(\lambda) \quad , \quad \tilde{1}(\lambda) = 1\,,$$

pour tout $\lambda \in A$. Donc $\varphi : p \mapsto \tilde{p}$ est un homomorphisme de l'anneau $A[X]$ dans l'anneau $\mathcal{F}(A, A)$ des fonctions de A dans A.

Il convient de bien distinguer le polynôme formel p et la fonction polynomiale $\tilde{p}$ qu'il définit car l'homomorphisme φ n'est pas toujours injectif. Par exemple, si A est le corps $\mathbb{Z}/n\mathbb{Z}$, où n est un nombre premier, le polynôme $p(X) = X^n - X$ est non nul, de degré n et tel que $\overline{k}^n - \overline{k} = \overline{0}$ pour tout $\overline{k} \in A$ (voir 2-3, ex. 1 ou 12-2). On a donc $\tilde{p} = 0$.

Néanmoins, dans la suite, pour simplifier, nous désignerons par la même lettre le polynôme formel et la fonction polynomiale qu'il définit.

Proposition.

Soit A un anneau commutatif avec unité. Supposons que $\lambda \in A$ soit racine de $a \in A[X]$. Alors il existe $q \in A[X]$ avec $\mathrm{d}^\circ(q) = \mathrm{d}^\circ(a) - 1$ tel que $a = (X - \lambda)q$.

Démonstration. Comme b = $X - \lambda$ est unitaire, on peut diviser a par b. On obtient $a = (X - \lambda)q + r$ où $\mathrm{d}^\circ(r) < \mathrm{d}^\circ(b) = 1$. Ainsi r est constant et $r = a(\lambda) = 0$. ∎

Corollaire 1.

Soit A un anneau commutatif, avec unité, intègre. Soit $a \in A[X]$ admettant k racines distinctes $\lambda_1, \ldots, \lambda_k$, où $k \leqslant \mathrm{d}^\circ(a)$. Alors il existe $q \in A[X]$ de degré $\mathrm{d}^\circ(q) = \mathrm{d}^\circ(a) - k$ tel que $a = (X - \lambda_1) \cdots (X - \lambda_k)q$.

Démonstration. D'après la proposition, $a = (X - \lambda_1)q_1$ avec $\mathrm{d}^\circ(q_1) = \mathrm{d}^\circ(a) - 1$. On en déduit $0 = a(\lambda_2) = (\lambda_2 - \lambda_1)q1(\lambda_2)$ avec $\lambda_2 - \lambda_1 \neq 0$, d'où $q_1(\lambda_2) = 0$ car A est intègre. La proposition montre ensuite que $q_1 = (X - \lambda_2)q_2$ avec $\mathrm{d}^\circ(q2) = \mathrm{d}^\circ(q1) - 1 = \mathrm{d}^\circ(a) - 2$. En poursuivant par récurrence ce raisonnement, on obtient le résultat. ∎

Corollaire 2.

Soit K un corps commutatif algébriquement clos. Tout polynôme $p = a_0 + a_1X + \cdots + anX^n$ de degré $n \geqslant 1$, se factorise sous la forme $a_n(X - \alpha_1) \cdots (X - \alpha_n)$.

Démonstration. Par mises en facteurs successives comme dans le cor. 1. ∎

Corollaire 3.

Soient K un corps commutatif et $p \in K[X]$. Si on a $\mathrm{d}^\circ(p) \leqslant n$ et si p admet $n + 1$ racines distinctes, alors p est le polynôme nul.

Démonstration. Si p n'était pas nul, de degré m, l'existence des m premières racines $\alpha_1, \ldots, \alpha_m$, conduirait à l'expression $p = (X-\alpha_1)\cdots(X-\alpha_m)q$ avec q constant non nul. Pour la racine suivante α_{m+1}, on aurait $p(\alpha_{m+1}) = (\alpha_{m+1}-\alpha_1)\cdots(\alpha_{m+1}-\alpha_m)q$ non nul, ce qui est absurde car K est intègre. ∎

Corollaire 4.

Soit K un corps commutatif. Si K est infini alors l'égalité formelle des polynômes de $K[X]$ est équivalente à l'égalité des fonctions polynomiales associées.

Démonstration. L'homomorphisme $\varphi : p \mapsto \tilde{p}$ de $K[X]$ dans $\mathcal{F}(K,K)$est injectif : si $p \in \mathrm{Ker}\,(\varphi)$, on a $p(\lambda) = 0$ pour tout $\lambda \in K$ et donc $\tilde{p} = 0$ d'après le cor. 3. ∎

Exercice. Pour quelles valeurs de $n \in \mathbb{N}^*, B(X) = X^2+X+1$ divise-t- il $A(X) = X^{2n}+X^n-X^2-X$ dans $\mathbb{C}[X]$? Montrer que le quotient $Q(X)$ est alors à coefficients entiers.

Solution. Puisque $(X^2+X+1)(X-1) = X^3-1$, les racines de $B(X)$ dans $\mathbb{C}$ sont $j = \exp(\frac{2i\pi}{3})$ et $\bar{j} = j^2$ et on a $j^2+j+1 = 0$. Regardons si j est racine de
$$A(X) = X^{2n}+X^n-X^2-X = (X^{2n}+X^n+1)-(X^2+X+1).$$
- Si $n \equiv 0\ (\mathrm{mod}\,3)$ on a $A(j) = 3-(j^2+j+1) = 3 \neq 0$
- Si $n \equiv 1\ (\mathrm{mod}\,3)$ on a $A(j) = (j^2+j+1)-(j^2+j+1) = 0$
- Si $n \equiv 2\ (\mathrm{mod}\,3)$ on a $A(j) = (j+j^2+1)-(j^2+j+1) = 0$.

Comme $A(X)$ est à coefficients réels, si $A(j) = 0$ alors $A(\bar{j}) = 0$. Le corollaire 1, appliqué dans $\mathbb{C}$[X], montre qu'il existe $Q \in \mathbb{C}[X]$ tel que $A(X) = B(X)Q(X)$. Ainsi, $B(X)$ divise $A(X)$ si et seulement si $n \equiv 1$ ou $n \equiv 2\ (\mathrm{mod}\,3)$.

Par ailleurs, puisque 1 est inversible dans $\mathbb{Z}$, la division de $A(X)$ par $B(X)$ est possible dans $\mathbb{Z}[X]$: il existe $Q_1(X)$ et $R_1(X)$ à coefficients entiers tels que $A(X) = (X^2+X+1)Q_1(X)+R_1(X)$ et $d^\circ(R_1) < 2$. L'unicité de la division dans $\mathbb{C}[X]$ donne $Q(X) = Q_1(X) \in \mathbb{Z}[X]$ et $0 = R_1(X)$. (Raisonnement général...)

10.4 Dérivée formelle d'un polynôme, formule de Taylor

Définition.

Soit A un anneau commutatif avec unité. Soit $p = a_0+a_1X+\cdots+a_nX^n \in A[X]$, de degré n. On appelle dérivée formelle de p, le polynôme nul si p est un polynôme constant et sinon le polynôme :

$$p' = a_1+2a_2X+\cdots+na_nX^{n-1}.$$

Par récurrence, on définit la dérivée d 'ordre $k \in \mathbb{N}^*$ de p en posant $p^{(k)} = (p^{(k-1)})'$.

Par récurrence, on obtient pour tout $k \in \mathbb{N}^*$ tel que $0 \leqslant k \leqslant n$,
$$p^{(k)} = k!\,a_k+\cdots+n(n-1)\cdots(n-k+1)a_nX^{n-k}$$
d'où
$$p^{(k)}(0) = k!\,a_k. \quad (1)$$

Considérons $p = a_0+a_1X+\cdots+a_mX^m \in A[X]$ et $q = b_0+b_1X+\cdots+b_mX^n \in A[X]$. Il est clair que $(p+q)' = p'+q'$. Grâce à cette propriété, la formule $(pq)' = p'q+pq'$, qui est vraie de manière immédiate pour les monômes, s'étend à tous les polynômes.

Le lecteur vérifiera par récurrence que :

$$(p^n)' = np^{n-1}p' . \tag{2}$$

Il établira de même par récurrence la formule de Leibniz :

$$(pq)^{(n)} = \sum_{k=0}^{n} C_n^k \, p^{(k)} q^{(n-k)} \tag{3}$$

Considérons le polynôme composé, obtenu par substitution de q dans p,

$$p \circ q = \sum_{k=0}^{m} a_k q(X)^k = a_0 + a_1(b_0 + \cdots + b_n X^n) + \cdots + a_m(b_0 + \cdots + b_n X^n)^m .$$

En utilisant (2), on voit que

$$(p \circ q)' = (p' \circ q)q' . \tag{4}$$

Avec $q = a + X$, où $a \in A$, on obtient le polynôme $P = poq = p(a + X)$. En utilisant la relation (4), on vérifiera par récurrence que pour tout $k \in \mathbb{N}^*$ on a

$$P^{(k)} = p^{(k)}(a + X) . \tag{5}$$

Proposition. (Formule de Taylor)

Soient K un corps commutatif de caractéristique nulle et $p = a_0 + a_1 X + \cdots + a_n X^n$ dans $K[X]$ de degré n. On a

$$p(X) = \sum_{k=0}^{n} \frac{1}{k!} p^{(k)}(0) X^k \quad \textit{et} \quad p(a + Y) = \sum_{k=0}^{n} \frac{1}{k!} p^{(k)}(a) Y^k .$$

Démonstration. La caractéristique de K étant nulle, pour tout $k \in \mathbb{N}$ on a $k!1 \neq 0$ dans K. Dans le corps K cet élément est inversible. Pour $1 \leqslant k \leqslant n$, la relation (1) ci-dessus donne $a_k = \frac{1}{k!} p^{(k)}(0)$, où $\frac{1}{k!}$ est l'inverse de $k!1$ dans le sous-corps premier de K, d'où l'expression de $p(X)$. En appliquant cela au polynôme $P = p(a + X)$ et compte tenu de (5), on obtient la deuxième relation. ∎

10.5 Multiplicité d'une racine

Proposition.

Soient K un corps commutatif, $a \in K[X]$ et $\lambda \in K$. Pour que λ soit racine du polynôme a, avec au moins la multiplicité $k \in \mathbb{N}^*$, il est nécessaire que

$$a(\lambda) = a'(\lambda) = \cdots = a^{(k-1)}(\lambda) = 0 .$$

Si K est de caractéristique nulle ou encore si la caractéristique de K est un nombre premier p et si on a $k \leqslant p$, la condition ci-dessus est suffisante.

Démonstration. Supposons que λ ait au moins la multiplicité $k \in \mathbb{N}*$, ce qui signifie que $a(X) = (X - \lambda)^k b(X)$ où $b \in K[X]$. La formule de Leibniz, montre que les dérivées de $a(X)$ admettent λ pour racine jusqu'à l'ordre $k - 1$ au moins.

Réciproquement supposons que $a(\lambda) = a'(\lambda) = \cdots = a^{(k-1)}(\lambda) = 0$. Considérons le polynôme $A(Y) = a(\lambda + Y)$ et son expression $A(Y) = a_0 + \cdots + a_m Y^m$. On a $a^{(r)}(\lambda) = A^{(r)}(0) = r! \, a_r$ pour tout r. Supposons la caractéristique de K nulle ou finie et supérieure à k. Pour $0 \leqslant r < k$ l'élément $(r!)1$ de K est non nul et donc $a_r = 0$. On en déduit que $A(Y) = Y^k(a_k + \cdots + a_m Y^{m-k})$ et donc que
$a(X) = A(X - \lambda) = (X - \lambda)^k [a_k + \cdots + a_m (X - \lambda^{m-k}]$.

Corollaire 1.

Soient K un corps commutatif et $a \in K[X]$. Pour que $\lambda \in K$ soit une racine multiple de a, il faut et il suffit que $a(\lambda) = a'(\lambda) = 0$.

Démonstration. D'après la proposition, la condition est nécessaire et suffisante car ici on a $2 \leqslant p$ pour tout nombre premier. ∎

Corollaire 2.

Soient K un corps commutatif de caractéristique nulle et $a \in K[X]$. Pour qu'une racine $\lambda \in K$ de $a(X)$ soit exactement de multiplicité k, il faut et il suffit que

$$a(\lambda) = a'(\lambda) = \cdots = a^{(k-1)}(\lambda) = 0 \quad \textit{et} \quad a^{(k)}(\lambda) \neq 0\,.$$

Démonstration. D'après la proposition et la formule de Taylor, la condition est nécessaire. Elle est suffisante car on obtient $a(X) = \sum_{k=0}^{n} \frac{1}{k\,!} a^{(k)}(\lambda)(X-\lambda)^k$ en utilisant la formule de Taylor. ∎

Exercice. Combien existe-t-il de dérivées successives de $a(X) = (X-l)^6 - X^6 + 1$ dans $K[X]$ nulles pour $X = 1$? Quelle est la multiplicité de cette racine ?

Solution. On a $a(1) = 0$ et $a'(X) = 6(X-1)^5 - 6X^5$. Si $p = \text{caract}(K)$ n'est ni 2 ni 3, on a $\mathrm{d}^\circ(a) = 5$, $a'(1) = -6 \times 1 \neq 0$. La multiplicité de la racine 1 est 1.
Si $p = 3$, la dérivée $a'(X)$ est le polynôme nul. Les dérivées de $a(X)$ sont toutes nulles. D'après la proposition, la multiplicité de la racine 1 est au moins 3. Cela se confirme en développant $a(X)$ à l'aide de la formule du binôme :

$a(X) = -6X^5 + 15X^4 - 20X^3 + 15X^2 - 6X + 2 = X^3 - 1 = (X-1)^3$.

Si $p = 2$, les dérivées de $a(X)$ sont toutes nulles. D'après la proposition, la multiplicité de la racine 1 est au moins 2 (mais attention, on ne peut pas dire plus). En développant,

$$\begin{aligned} a(X) &= -6X^5 + 15X^4 - 20X^3 + 15X^2 - 6X + 2 = X^4 + X^2 \\ &= X^2(X^2+1) = X^2(X^2 - 2X + 1) = X^2(X-1)^2\,. \end{aligned}$$

La multiplicité est effectivement 2.

10.6 Un exemple : les polynômes cyclotomiques

Les racines dans $\mathbb{C}$ du polynôme $X^n - 1 \in \mathbb{C}[X]$ sont les éléments de

$$\mathbb{U}_n = \{1\,,\,\zeta\,,\,\zeta^2\,,\ldots,\,\zeta^{n-1}\} \quad \text{où} \quad \zeta = \exp(i\frac{2\pi}{n})\,.$$

Ce groupe cyclique admet $\varphi(n)$ générateurs, où φ désigne la fonction d'Euler. Ce sont les racines $n^{\text{iémes}}$ primitives de l'unité, éléments de

$$\Lambda_n = \{\zeta^k\,;\ 0 \leqslant k \leqslant n-l\ ,\,,k \wedge n = 1\}\,.$$

Si $d \in \mathbb{N}^*$ divise n, alors le groupe $\mathbb{U}_d$ est un sous-groupe de $\mathbb{U}_n$ car $\zeta^d = 1$ implique $\zeta^n = 1$. Dans le groupe cyclique $\mathbb{U}_n$, pour tout diviseur d de n, il existe un unique sous-groupe d'ordre d (3-3). C'est donc $\mathbb{U}_d$. Tout élément d'ordre d de $\mathbb{U}_n$ engendre un sous-groupe d'ordre d. Ce sous-groupe est donc $\mathbb{U}_d$. Si on classe les éléments du groupe $\mathbb{U}_n$ selon leur ordre, qui est diviseur de n, on obtient donc la partition suivante de $\mathbb{U}_n$:

$$\mathbb{U}_n = \Lambda_1 \cup \cdots \cup \Lambda_d \cup \cdots \Lambda_n = U_{d|n}\,\Lambda_d\,. \tag{1}$$

En particulier, on a $n = \sum_{d I n} \varphi(d)$.

Définition.

Le polynôme unitaire $\Phi_n(X) = \prod_{\zeta \in \Lambda_n} (X - \zeta)$ *est appelé le polynôme cyclotomique d 'indice* n. *Son degré est* $\varphi(n)$.

Exemples.
$\Phi_1(X) = X - 1$ car $\mathbb{U}_1 = \{1\}$ et $\Lambda_1 = \{1\}$.
$\Phi_2(X) = X + 1$ car $\mathbb{U}_2 = \{1, -1\}$ et $\Lambda_2 = \{-1\}$.
$\Phi_3(X) = (X - j)(X - \bar{j}) = X^2 + X + 1$ car $\mathbb{U}_3 = \{1, j, j^2\}$ et $\Lambda_3 = \{j, j^2\}$.
$\Phi_4(X) = (X - i)(X + i) = X^2 + 1$ car $\mathbb{U}_4 = \{1, i, -1, -i\}$ et $\Lambda_4 = \{i, i^3\}$.
$\Phi_5(X) = X^4 + X^3 + X^2 + X + 1$ car $\Lambda_5 = \{\zeta\,,\, \zeta^2\,,\, \zeta^3\,,\, \zeta^4\}$, où $\zeta = \exp(\frac{2i\pi}{5})$.
$\Phi_6(X) = (X + j)(X + \bar{j}) = X^2 - X + 1$ car $\Lambda_6 = \{-\bar{j} = \exp(i\frac{2\pi}{6})\,,\, -j = \exp(5i\frac{2\pi}{6})\}$.
$\Phi_7(X) = X^6 + X^5 + X^4 + X^3 + X^2 + X + 1$ car 7 est premier (comme 3 et 5).
$\Phi_8(X) = X^4 + 1 = \frac{X^8 - 1}{X^4 - 1}$ car $\Lambda_5 = \{\zeta\,,\, \zeta^3\,,\, \zeta^5\,,\, \zeta^7\} = \mathbb{U}_8 \setminus \mathbb{U}_4$.
$\Phi_9(X) = \frac{X^9 - 1}{X^3 - 1} = X^6 + X^3 + 1$ car $\Lambda_9 = \mathbb{U}_9 \setminus \mathbb{U}_3$.

Proposition.

Pour tout $n \in \mathbb{N}^*$, *le polynôme cyclotomique* Φ_n *est unitaire à coefficients entiers.*

On a $X^n - 1 = \Phi_1(X) \cdots \Phi_n(X) = \prod_{d|n} \Phi_d(X)$.

Supposons $n \geqslant 2$. *On a* $\Phi_n(0) = 1$ *et* $X^{\varphi(n)} \Phi_n(\frac{1}{X}) = \Phi_n(X)$.

Supposons $n \geqslant 3$. *On a* $\Phi_n(x) > 0$ *pour tout* $x \in \mathbb{R}$ *et* $\Phi_n(x) > (|x| - 1)^{\varphi(n)}$ *pour tout* $x \in \mathbb{R}$ *tel que* $|x| > 1$.

Démonstration. Puisque $\mathbb{U}_n = \bigcup_{d|n} \Lambda_d$ est une partition, on a :

$$X^n - 1 = \prod_{\zeta \in \mathbb{U} n} (X - \zeta) = \prod_{d|n} \prod_{\zeta \in \Lambda_d} (X - \zeta) = \prod_{d|n} \Phi_d(X) .$$

Les polynômes $\Phi_1 = X - 1$ et $\Phi_2 = X + 1$ sont à coefficients entiers. Montrons par récurrence que pour tout $n > 2$ on a $\Phi_n \in \mathbb{Z}[X]$. Supposons ce résultat vrai pour tout $d \in \mathbb{N}$ tel que $2 \leqslant d < n$. On a :

$$X^n - 1 = [\Phi_1(X) \cdots \Phi_d(X) \ldots]\Phi_n(X) = b(X)\Phi_n(X) ,$$

où $b(X) = \prod_{d|n, 1 \leqslant d < n} \Phi_d(X)$ est à coefficients entiers d'après l'hypothèse de récurrence. Dans l'anneau $\mathbb{Z}[X]$, on peut diviser de $a(X) = X^n - 1$ par $b(X)$ qui est unitaire (10-2, prop.). On obtient $q \in \mathbb{Z}[X]$ et $r \in \mathbb{Z}[X]$ tels que $a = bq + r$ et $\mathrm{d}^\circ(r) < \mathrm{d}^\circ(b)$. Dans $\mathbb{C}[X]$ on a $a = b\Phi_n$. De l'unicité de la division dans $\mathbb{C}[X]$ il résulte que $\Phi_n = q \in \mathbb{Z}[X]$ et $r = 0$.

On a $\Phi_2(0) = 1$. Supposons $n \geqslant 3$. Pour tout $\zeta \in \Lambda_n$ on a $\overline{\zeta} \in \Lambda_n$. Comme $\Lambda_n \cap \mathbb{R} = \emptyset$, on peut faire une partition $\Lambda_n = \bigcup_{i \in I} \{\zeta_i, \overline{\zeta_i}\}$ par couples conjugués. On en déduit $\Phi_n(x) = \prod_{i \in I} |x - \zeta_i|^2 > 0$ pour tout $x \in \mathbb{R}$ et donc $\Phi_n(0) = \prod_{i \in I} \zeta_i \overline{\zeta_i} = 1$.

Soit $n \geqslant 2$. Puisque $\mathrm{d}^\circ(\Phi_n) = \varphi(n)$ et $\Phi_n(0) = 1$, on voit que $X^{\varphi(n)} \Phi_n(\frac{1}{X})$ est un polynôme de degré $\varphi(n)$, unitaire. Comme $\zeta \mapsto \frac{1}{\zeta} = \overline{\zeta}$ est une bijection de Λ_n sur

lui-même, l'ensemble de ses racines est Λ_n. Donc $\Phi_n(X) = \Pi_{\zeta\in\Lambda_n}(X-\zeta)$ divise ce polynôme. Etant unitaires, de même degré, les deux polynômes sont égaux.

Supposons $n \geqslant 3$. On a $\Phi_n(x) = \prod_{i\in I} |x-\zeta_i|^2$, avec $|x-\zeta_i| > x-1$ pour $x>1$ et $|x-\zeta_i| > x+1$ pour $x<-1$, d'où la dernière assertion. ∎

Exercice 1. Soient $m\in\mathbb{N}^*, n\in\mathbb{N}^*$ premiers entre eux. Montrer que $\Phi_{mn}(X) = \prod_{\alpha\in\Lambda_m}\prod_{\beta\in\Lambda_n}(X-\alpha\beta)$. Pour $n \geqslant 3$ impair, montrer que $\Phi_{2n}(X) = \Phi_n(-X)$.

Solution. Comme $m\wedge n = 1$, on sait que $f : (x,y)\mapsto xy$ est un isomorphisme de $\mathbb{U}_m\times\mathbb{U}_n$ sur $\mathbb{U}_m\mathbb{U}_n = \mathbb{U}_{mn}$, (1-11, ex.). Les générateurs de $\mathbb{U}_m\times\mathbb{U}_n$ sont les couples (α,β) où α (resp. β) est générateur de $\mathbb{U}_m$. (resp. $\mathbb{U}_n$) (3-4, prop.). On en déduit que $\Lambda_{mn} = \{\alpha\beta\,;\ \alpha\in\Lambda_m\,,\ \beta\in\Lambda_n\}$ d'où l'expression proposée de $\Phi_{mn}(X)$.

Si $n\geqslant 3$ est impair, il est premier aver $m=2$. On a $\Lambda_2 = \{-1\}$ et $\varphi(n)$ est pair car $\Lambda_n = \bigcup_{i\in I}\{\zeta_i,\overline{\zeta_i}\}$. En appliquant ce qui précède,

$$\Phi_{2n}(X) = \prod_{\alpha\in\Lambda_n}(X+\alpha) = (-1)^{\varphi(n)}\prod_{\alpha\in\Lambda_n}(-X-\alpha) = \prod_{\alpha\in\Lambda_n}(-X-\alpha) = \Phi_n(-X)\,.$$

Exercice 2. Soit $m\in\mathbb{N}^*$tel que $m\geqslant 2$ et soit $n\in\mathbb{N}^*$ dont tout facteur premier est un facteur premier de m. Montrer que $\Phi_m(X^n) = \Phi_{mn}(X)$.
Donner l'expression de $\Phi_{24}(X)$ et de $\Phi_{2^k}(X)$, où $k\in\mathbb{N}^*$.

Solution. Considérons les décompositions en facteurs premiers de n et m.
$n = p_1^{\alpha_1}\cdots p_k^{\alpha_k}$, $m = p_1^{\beta_1}\cdots p_k^{\beta_k}q_1^{\gamma_1}\cdots q_\ell^{\gamma_\ell}$, avec $\alpha_i>0$, $\beta_i>0$ pour $1\leqslant i\leqslant k$ et $\gamma_j>0$ pour $1\leqslant j\leqslant \ell$. D'après 3-4, cor. 2, le degré de $\Phi_{mn}(X)$ est

$$\begin{aligned}\varphi(mn) &= p_1^{\alpha_1+\beta_1-1}(p_1-1)\cdots p_k^{\alpha_k+\beta_k-1}(p-k-1)q_1^{\gamma_1-1}(q_1-1)\cdots q_\ell^{\gamma_\ell-1}(\gamma_\ell-1)\\ &= n\varphi(m) = \mathrm{d}^\circ(\Phi_m(X^n))\,.\end{aligned}$$

Puisque $m|mn$ on a $\mathbb{U}_m\subset\mathbb{U}_{mn}$ et $\mathbb{U}_m = \{z\in\mathbb{U}_{mn}\mid \exists z'\in\mathbb{U}_{mn}\ \ z'^n = z\}$ (3-3, prop.). L'homomorphisme $f : z'\mapsto z'^n$ est donc surjectif de $\mathbb{U}_{mn}$, sur $\mathbb{U}_m$. On a donc $f(\Lambda_{mn})\subset\Lambda_m$ (3-2, prop.). Toute racine de $\Phi_{mn}(X)$ est donc racine de $\Phi_m(X^n)$. Comme $\Phi_{mn}(X)$ est scindé simple, il divise $\Phi_m(X^n)$. Les deux polynômes étant unitaires de même degré, ils sont égaux. En utilisant cette relation,

$$\begin{aligned}\Phi_{24}(X) &= \Phi_{3\times 2^3}(X) = \Phi_{3\times 2}(X^4) = (X^4)^2 - X^4 + 1 = X^8 - X^4 + 1\,.\\ \Phi_{2^k}(X) &= \Phi_2(X^{2^{k-1}}) = X^{2^{k-1}} + 1.\end{aligned}$$

10.7 Groupe K_* lorsque K est un corps commutatif

Soit K un corps commutatif. L'application $n\mapsto n1$ de $\mathbb{N}$ dans K se prolonge en un homomorphisme d'anneaux γ de $\mathbb{Z}$ dans K de noyau $p\mathbb{Z}$ où $p = \mathrm{caract}(K)$ (voir 9-1). Tout polynôme $a = a_0+\cdots+a_nX^n$ à coefficients entiers définit donc un polynôme $\Gamma(a) = \gamma(a_0)+\cdots+\gamma(a_n)X^n\,K[X]$ et $\Gamma : a\mapsto\Gamma(a)$ est un homomorphisme d'anneaux (10-1, ex. 1). Si a est unitaire, $\Gamma(a)$ est unitaire et $\mathrm{d}^\circ(\Gamma(a)) = \mathrm{d}^\circ(a)$.

Cela s'applique aux polynômes cyclotomiques Φ_n, où $n\in\mathbb{N}^*$. Nous noterons $\Phi_{n,K}$ ou tout simplement Φ_n s'il n'y a pas de confusion possible sur le corps considéré, le polynôme $\Gamma(\Phi_n)$. Puisque Γ est un homomorphisme, pour tout $n\in\mathbb{N}^*$ on a :

$$X^n - 1 = \prod_{d|n}\Phi_{d,K}(X)\,. \tag{1}$$

Proposition.

Soient K un corps commutatif et $n \in \mathbb{N}*$. Les conditions suivantes sont équivalentes.
(i) *Il existe un sous-groupe de K_* d 'ordre n.*
(ii) *Le polynôme $X^n - 1$ est scindé simple dans $K[X]$.*
(iii) *Il existe dans K une racine de $\Phi_{n,K}(X)$ qui est une racine simple de $X^n - 1$.*
(iv) *$\Phi_{n,K}(X)$ a une racine dans K et* caract(K) *ne divise pas n.*

Si ces conditions sont vérifiées, il existe dans K_* un seul sous-groupe d 'ordre n. Il est égal à l'ensemble des racines du polynôme $X^n - 1$ et il est cyclique. Ses $\varphi(n)$ générateurs sont les racines de $\Phi_{n,K}(X)$. Pour tout diviseur d de n, les éléments d'ordre d de ce groupe sont les racines de $\Phi_{d,K}(X)$.

Démonstration. (i) $\Rightarrow$ (ii) Supposons qu'il existe un sous-groupe G d'ordre n dans K_*. D'après le th. de Lagrange, tout $x \in G$, est racine de $X^n - 1$. Ainsi $X^n - 1$ admet n racines distincts dans K et on a $X^n - 1 = \prod_{\zeta \in G} (X - \zeta)$ (10-3, cor. 3).

(ii) $\Rightarrow$ (iii) Supposons que $X^n - 1$ admet n racines distinctes $a_1, \ldots, a_n$ dans K. D'après (1), pour chacune de ces racines a_i il existe un diviseur d de n tel que $\Phi_{d,K} a_i) = 0$ et alors $(X - a_i)$ divise $\Phi_{d,K}(a_i)$. Du fait que $n = \sum_{d|n} \varphi(d)$, les n facteurs $(X - ai)$ apparaissent dans les divers termes $\Phi_{d,K}(X)$ qui sont donc scindés.

(iii) $\Leftrightarrow$(iv) Supposons que $a \in K$ soit racine de $\Phi_{n,K}(X)$ et donc de $X^n - 1$. Alors a est racine simple de $X^n - 1$ si et seulement si $na^{n-1} \neq 0$ soit si $n1 \neq 0$ puisque K est intègre et $a \neq 0$. Cette condition signifie que n n'est pas un multiple de caract(K).

(iii) $\Rightarrow$ (i) Soit $a \in K$ soit racine de $\Phi_{n,K}(X)$ et racine simple de $X^n - 1$. On a alors $a^n = 1$ donc $a \in K_*$ et l'ordre k de $a \in K_*$ divise n. Supposons $k < n$. On aurait $a^k - 1 = 0$. Comme $X^n - 1 = \Phi_{n,K}(X)(X^k - 1)R(X)$, où $R(X)$ est produit des termes $\Phi_{d,K}(X)$ avec $d|n$, $d \neq n$ et d ne divisant pas k, on voit que a serait une racine multiple de $X^n - 1$ ce qui est exclu. Donc $o(a) = n$ et $\langle a \rangle$ est un sous-groupe d'ordre n de K_*.

Supposons ces conditions équivalentes vérifiées. Si G est un sous-groupe d'ordre n de K_*, nous avons vu que G est l'ensemble des racines de $X^n - 1$ et donc unique. Comme $X^n - 1$ est scindé simple, $\Phi_{n,K}(X)$ admet $\varphi(n)$ racines distinctes et chacune des racines a de $\Phi_{n,K}(X)$ engendre un sous-groupe $\langle a \rangle$ d'ordre n et donc égal à G. Les $\varphi(n)$ générateurs de G sont donc les $\varphi(n)$ racines de $\Phi_{n,K}(X)$. Pour tout diviseur d de n, cela s'applique au polynôme $X^d - 1$ qui divise $X^n - 1$ et qui est donc scindé simple, d'où la dernière assertion. ∎

Corollaire 1

Soit K un corps commutatif. Tout sous-groupe fini de K_* est cyclique.

Corollaire 2.

Soit p un nombre premier. Le groupe Aut $(\mathbb{Z}/p\mathbb{Z}, +)$ des automorphismes du groupe additif $(\mathbb{Z}/p\mathbb{Z}, +)$ est cyclique.

Démonstration. L'application $\varphi : \overline{a} \mapsto f_{\overline{a}}$ où $f_{\overline{a}} : \overline{x} \mapsto \overline{ax}$, est un isomorphisme du corps $\mathbb{Z}/p\mathbb{Z}$ sur End $(\mathbb{Z}/p\mathbb{Z}, +)$ (voir 9-11, cor. 1 et 9-2, ex. 2). Donc φ induit un isomorphisme du groupe $(\mathbb{Z}/p\mathbb{Z})_*$ sur le groupe Aut $(\mathbb{Z}/p\mathbb{Z}, +) = [\text{End}\,(\mathbb{Z}/p\mathbb{Z}, +)]_*$. ∎

Exercice 1. a) Soit K un corps fini (commutatif), de caractéristique $p \neq 2$. Montrer que -1 est un carré dans K si et seulement si card $(K) \equiv 1 \pmod 4$.

b) Soient $x \in \mathbb{Z}$ et k un diviseur impair de x^2+1. Montrer que $k \equiv 1 \pmod 4$.

Solution. a) Pour que -1 soit un carré, il faut et il suffit qu'il existe $x \in K$ tel que $x^2 = -1$. On a alors $x^4 = 1$. L'ordre de x dans K_* doit diviser 4 et on a $x^2 \neq 1$ donc $o(x) = 4$. Le th. de Lagrange montre que si -1 est un carré alors 4 divise $[K_* : 1] =$ card $(K) - 1$. Réciproquement, puisque K_* est cyclique, si 4 divise l'ordre de K_*, il existe dans K_* un sous-groupe cyclique d'ordre 4, de la forme $\{1, x, x^2, x^3\}$ et $\{1, x^2\}$ est égal à $\{1, -1\}$ car dans le groupe cyclique K_* pour tout diviseur d de l'ordre, il existe un seul sous-groupe d'ordre d. Donc $x^2 = -1$.

b) Soit $p \neq 2$ un diviseur premier de x^2+1. Dans $\mathbb{Z}/p\mathbb{Z}$ on a $\overline{x}^2 = -\overline{1}$. D'après a), on a $p \equiv 1 \pmod 4$, d'où le résultat car k est produit de facteurs premiers impairs.

Exercice 2. (Equation diophantienne étudiée par V. A. Lebesgue)
a) En considérant les deux cas x pair et xi mpair, montrer que l'équation diophantienne $x^3 - y^2 + 7 = 0$ n'admet pas de solution $(x, y) \in \mathbb{Z}^2$.

b) Déterminer toutes les solutions $(x, y, z) \in \mathbb{Z}^3$ de $x^3 - y^2 + 7z = 0$.

Solution. a) Supposons que $x^3 - y^2 + 7 = 0$ ait une solution (x, y). Si $x = 2k$ était pair, modulo 8 on aurait $y^2 \equiv 7$. C'est impossible car $-\overline{1} = \overline{7}$ n'est pas un carré dans $\mathbb{Z}/8\mathbb{Z}$. Donc $x = 2k+1$ est impair et y est pair non nul. On a
$y^2 + 1 = x^3 + 2^3 = (x+2)(x^2 - 2x + 4) = (2k+3)(4k^2+3)$. Modulo 4 les facteurs premiers de $4k^2+3$ sont congrus à 1 ou 3 (un nombre supérieur ou égal à 3 congru à 0 ou 2 n'est pas premier). Ils ne peuvent être tous congrus à 1 sinon leur produit $4k^2+3$ serait congru à 1. Donc au moins un des facteurs premiers de $4k^2+3$ est congru à 3 modulo 4. Or les facteurs premiers de y^2+1 sont tous congrus à 1 modulo 4, d'après l'exercice précédent. Donc x ne peut être impair et $x^3 - y^2 + 7 = 0$ n'a pas de solution.

b) Comme 7 est premier, $K = \mathbb{Z}/7\mathbb{Z}$ est un corps. Soient $x \in \mathbb{Z}$, $y \in \mathbb{Z}$. Pour qu'il existe $z \in \mathbb{Z}$ tel que (x, y, z) soit solution de $x^3 - y^2 + 7z = 0$, il faut et il sufiit que

$$\overline{x}^3 = \overline{y}^2 \qquad (2)\,.$$

Si $\overline{x} = \overline{0}$ alors $\overline{y} = \overline{0}$ car le corps K est intègre. Si $\overline{x} \neq \overline{0}$ alors $\overline{y} \neq \overline{0}$. Le groupe K_* est cyclique d'ordre 6. Comme 2 et 3 divisent 6, il existe dans K_*, un unique sous-groupe H_2 d'ordre 2 et un unique sous-groupe H_3 d'ordre 3, caractérisés par

$$H_2 = \{\overline{u} \in K_* \mid \exists \overline{x} \in K_* \ \ \overline{x}^3 = \overline{u}\} = \{\overline{u} \in K_* \mid \overline{u}^2 = \overline{1}\}\,,$$

$$H_3 = \{\overline{u} \in K_* \mid \exists \overline{y} \in K_* \ \ \overline{y}^2 = \overline{u}\} = \{\overline{u} \in K_* \mid \overline{u}^3 = \overline{1}\}\,,$$

Ainsi l'élément $\overline{u} = \overline{x}^3 = \overline{y}^2$ qui apparaît en (2) appartient à H_2 et H_3 et donc à $H_2 \cap H_3$. L'ordre de $H_2 \cap H_3$ divise les ordres 2 et 3 de H_2 et H_3 donc $H_2 \cap H_3 = \{\overline{1}\}$ et on a $\overline{u} = \overline{1}$. Ainsi $\overline{x}^3 = \overline{1}$ donc $\overline{x} \in H_3$ et donc $\overline{y} \in H_2$.
Réciproquement, si $\overline{x} \in H_3$ et $\overline{y} \in H_2$ on a $\overline{x}^3 = \overline{1}$ et $\overline{x}^3 = \overline{1}$ donc $\overline{x}^3 = \overline{y}^2$. Ainsi pour avoir les solutions de (2) on peut choisir $\overline{y}$ dans $H_2 = \{\overline{1}, -\overline{1}\}$, arbitrairement et $\overline{x}$ arbitrairement dans H_3. Comme $\overline{2}^2 = \overline{4}$, $\overline{2}^3 = \overline{8} = \overline{1}$ on a $o(\overline{2}) = 3$ donc l'unique sous-groupe H_3 d'ordre 3 de K_* est $\{\overline{1}, \overline{2}, \overline{2}^2\}$. Les solutions de (2) sont donc

$$\overline{x} = \overline{0} = \overline{y} \qquad , \qquad (\overline{x} = \overline{1}, \overline{2} \text{ ou } \overline{4}) \text{ et } (\overline{y} = \overline{1} \text{ ou } -\overline{1})$$

On en déduit les solutions de (1). Dans le premier cas $x = 7k, y = 7k'$, $z = -7^2k^3 + 7k'^2$. Dans le deuxième cas $x = a + 7k$, $y = b + 7k'$, $z = \frac{1}{7}(-x^3 + y^2)$ où $k \in \mathbb{Z}$, $k' \in \mathbb{Z}$ sont arbitraires, $a = 1, 2$ ou 4, $b = 1$ ou -1.

10.8 Le polynôme d'interpolation de Lagrange

Proposition.

Soient K un corps commutatif et $n \in \mathbb{N}^*$. On considère $\alpha_1, \dots, \alpha_n \in K$ distincts et $\lambda_1, \dots, \lambda_n \in K$. Il existe un unique polynôme $P(X)$ de degré inférieur ou égal à $n-1$, tel que $P(\alpha_1) = \lambda_1, \dots, P(\alpha_n) = \lambda_n$. Il a pour expression :

$$(1) \qquad P(X) = \sum_{k=1}^{n} \lambda_k Q_k(X) \quad \text{où} \quad Q_k(x) = \frac{\prod_{i \neq k}(X - \alpha_i)}{\prod_{i \neq k}(\alpha_k - \alpha_i)} \, .$$

Démonstration. On cherche $P(X) = a_0 + \cdots + a_{n-1}X^{n-1}$ tel que

$$(2) \quad \begin{cases} a_0 + a_1\alpha_1 + \cdots + a_{n-1}\alpha_1^{n-1} = \lambda_1 \\ \cdots\cdots\cdots\cdots\cdots\cdots\cdots \\ a_0 + a_1\alpha_n + \cdots + a_{n-1}\alpha_n^{n-1} = \lambda_n \end{cases} \text{ Le déterminant } \Delta = \begin{vmatrix} 1 & \alpha_1 & \cdots & \alpha_1^{n-1} \\ \cdots & \cdots & \cdots & \cdots \\ 1 & \alpha_n & \cdots & \alpha_n^{n-1} \end{vmatrix}$$

vaut $\Delta = \prod_{i<j} (\alpha_j - \alpha_i) \neq 0$ (d'après Vandermonde) car $\alpha_1, \dots, \alpha_n$ sont distincts. Le système (2) est de Cramer. Il a une solution unique $a_0, \dots, a_{n-1}$. Le polynôme $P(X)$ d'expression (1) vérifie $P(\alpha_1) = \lambda_1$, ... , $P(\alpha_n) = \lambda_n$. C'est l'unique solution. ∎

Remarque. Soit $\mathcal{P}_n$, l'espace vectoriel des polynômes $P \in K[X]$ de degré au plus $n-1$, muni de la base canonique $\mathcal{B} = (1, X, \dots, X^{n-1})$. Dans la base $\mathcal{B}^*$ duale de $\mathcal{B}$, la forme linéaire $f_i : P \mapsto P(\alpha_i)$ a pour coordonnées $(1, \alpha_1, \dots, \alpha_1^{n-1})$. On a donc $\det_{\mathcal{B}^*}(f_1, \dots, f_n) = \Delta \neq 0$. Ainsi $(f_1, \dots, f_n)$ est une base du dual $\mathcal{P}_n^*$ de $\mathcal{P}_n$. Les polynômes $Q_k(X)$, qui sont tels que $f_i(Qk) = \delta_{ik}$, constituent dans $\mathcal{P}_n$ la base duale de $(f_1, \dots, f_n)$ et $\lambda_1 = f_1(P), \dots, \lambda_n = f_n(P)$ sont les coordonnées de P dans cette base de $\mathcal{P}_n$, ce qui explique l'existence et l'unicité de $\lambda_1, \dots, \lambda_n$.

Le polynôme d'interpolation de Lagrange est un outil très utile, aussi bien en algèbre pure qu'en analyse numérique (pour approximer des fonctions). Nous allons voir une application donnée par Lagrange lui- même : une démonstration simple des formules de Cardan-Tartaglia pour résoudre les équations du troisième degré.

10.9 Résolution des équations du troisième degré

Considérons l'équation à coefficients complexes $Y^3 + aY^2 + bY + c = 0$. Le changement de variable $Y = X - \frac{a}{3}$ ramène cette équation à la forme

$$(1) \qquad X^3 + pX + q = 0 \, .$$

Notons x_1, x_2, x_3 les trois racines (distinctes ou non) de (1) dans $\mathbb{C}$.

Proposition.

Il existe $u, v \in \mathbb{C}$ uniques tels que les racines de (1) soient

$$(2) \qquad x_1 = u + v \quad , \quad x_2 = uj^2 + vj \quad , \quad x_3 = uj + vj^2 \, ,$$

et u^3 et v^3 sont les racines du trinôme (dit résolvant)

$$(3) \qquad X^2 + qX - \frac{p^3}{27q^2} \, .$$

Démonstration. Dans $\mathbb{C}[X]$ on a :

$$\begin{aligned} X^3 + pX + q &= (X - x_1)(X - x_2)(X - x_3) \\ &= X^3 - (x_1 + x_2 + x_3)X^2 + (x_2x_3 + x_3x_1 + x_1x_2)X - x_1x_2x_3 \, . \end{aligned}$$

Utilisons le polynôme d'interpolation de Lagrange : il existe un polynôme de degré 2, soit $P(X) = uX^2 + vX + w$, unique, tel que :

$$P(1) = x_1 \quad , \quad P(j) = x_2 \quad , \quad P(j^2) = x_3 \, .$$

Dans (1) le coefficient $-(x_1 + x_2 + x_3)$ de X^2 est nul donc $0 = P(1) + P(j) + P(j^2) = 3w$. Ainsi $P(X) = vX + uX^2$, ce qui donne l'existence et l'unicité de u et v vérifiant (2). Du fait que $1 + j + j^2 = 0$ et que $(u+v)(uj + vj^2)(uj^2 + vj) = u^3 + v^3$, on a :

$$\begin{aligned} X^3 + pX + q &= (X - (u+v))(X - (uj^2 + vj))(X - (uj + vj^2)) \\ &= X^3 - 3uvX - (u^3 + v^3) \, . \end{aligned}$$

Ainsi, les nombres u, v, uniques vérifiant les relations (2), vérifient également,

(4) $$-3uv = p \quad , \quad u^3 + v^3 = -q.$$

En posant $U = u^3$, $V = v^3$ on voit que $U + V = -q$ et que $UV = -\frac{p^3}{27q^2}$ et donc que U et V sont racines du polynôme résolvant (3). ∎

Exemple. Etudions l'équation (1) dans le cas où p et q sont réels. Alors (1) a 3 racines réelles ou une racine réelle et deux racines complexes conjuguées.

a) Supposons $\Delta = 4p^3 + 27q^2 > 0$. Alors le trinôme résolvant a deux racines réelles U et V, telles que $UV = -\frac{p^3}{27q^2}$. Puisque $-3uv = p$ doit être réel, choisissons pour u l'unique racine cubique réelle de U et pour v l'unique racine cubique réelle de V. Pour ce choix les relations (4) sont vérifiées et donc u et v sont bien les uniques valeurs vérifiant (2). On obtient ainsi les formules de Cardan donnant u et v et ensuite les valeurs de x_1 , x_2 , x_3 , en utilisant les relations (2).

(5) $$u = \sqrt[3]{\frac{1}{2}\left(-q + \sqrt{q^2 + \frac{4p^3}{27}}\right)} \quad , \quad v = \sqrt[3]{\frac{1}{2}\left(-q - \sqrt{q^2 + \frac{4p^3}{27}}\right)}$$

Comme $\Delta \neq 0$, on a $u \neq v$. Donc $x_2 = uj^2 + vj$ et $x_3 = uj + vj^2$ ne sont pas réels et (1) admet une unique racine réelle x_1 et deux racines complexes conjuguées non réelles.

b) Si $\Delta = 0$, alors $u = v = \sqrt[3]{-\frac{q}{2}} \in \mathbb{R}$ et $x_1 = 2u$, $x_2 = x_3 = -u$.

c) Si $\Delta < 0$. Alors $U = u^3$ et $V = v^3$ sont conjugués non réels. En choisissant des racines cubiques u et $v = \overline{u}$ de U et V conjuguées, on aura $uv \in \mathbb{R}$ et (4) sera à nouveau vérifié. Les trois racines de (1) sont réelles d'expression :

$$x_1 = u + \overline{u} \quad , \quad x_2 = u\overline{j} + \overline{u}j \quad , \quad x_3 = uj + \overline{u}\overline{j} \, .$$

Remarque. . Au Moyen Age, les nombres complexes étaient inconnus. Bombelli (1526-1573) contemporain de Cardan (1501-1576) a remarqué que c'est justement dans le cas où l'on a $\Delta < 0$, où l'équation résolvante n'a pas de racines, que l'équation (1) a trois racines réelles. Il applique néanmoins les formules de Cardan-Tartaglia, en travaillant de manière symbolique sur des expressions de la forme $a + b\sqrt{-1}$ et il constate qu'elles donnent les valeurs exactes des racines. Il précise les règles de calcul à suivre dans le maniement de tels nombres "imaginaires". Les nombres complexes étaient nés.

A partir du Moyen Age, la recherche de formules résolvant les équations de degré cinq ou plus, a beaucoup préoccupé les mathématiciens. C'est au début du 19 ème siècle que E. Galois a démontré que ce n'est pas possible, en utilisant le fait que le groupe $\mathcal{S}_n$ n'est pas résoluble pour $n \geqslant 5$ (voir 4-5).

Exercices du chapitre 10

Ex 10 - 1

Soit A un anneau commutatif, avec unité. On appelle série formelle, une suite $a : n \mapsto a_n$ à valeurs dans A. On la note $a_0 + a_1X + a_2X^2 + \cdots + a_nX^n + \cdots$ On pose $\text{val}(a) = +\infty$ si $a = 0$ et $\text{val}(a) = \min\{p \in \mathbb{N} \mid a_p \neq 0\}$ sinon. On note $A[[X]]$ l'ensemble des séries formelles.

On appelle somme de $a, b \in A[[X]]$ la série formelle $n \mapsto a_n + b_n$. Le produit $c = ab$ est $c : n \mapsto c_n$ où pour tout n

$$c_n = a_0b_n + a_1b_{n-1} + \cdots + a_nb_0 .$$

a) Vérifier que $A[[X]]$ est une A-algèbre commutative unifère et que $A[X]$ est une sous-algèbre de $A[[X]]$.

b) Montrer que $A[[X]]$ est intègre si et seulement si A est intègre.

c) Montrer que $d(a, b) = \exp(-\text{val}(b - a))$ est une distance ultramétrique sur $A[[X]]$ pour laquelle $A[[X]]$ est le complété de $A[X]$ (on pose $e^{-\infty} = 0$).

d) Soit $b \in A[[X]]$ telle que $b_0 = 0$. Pour tout $a \in A[[X]]$, montrer que la série $\sum a_n b(X)^n$ converge.

e) Montrer que $a \in A[[X]]$ est inversible si et seulement si a_0 est inversible dans l'anneau A. Montrer que $A[[X]]$ possède un idéal maximal et un seul.

f) Définir la série formelle $a'(X)$ dérivée de $a(X)$. Etablir des règles de calcul.

g) Supposons que $A = K$ soit un corps. Notons $K(X)_0$ l'anneau des classes de fractions rationnelles $\frac{a(X)}{b(X)}$, où $b(0) \neq 0$. Montrer qu'il existe un homomorphisme injectif unique φ de $K(X)_0$ dans $K[[X]]$, égal à l'application identique sur $K[X]$.
Montrer que $\varphi(\frac{1}{1-X}) = \sum X^n$.

h) Exemple. Soit $n \in \mathbb{N}$. Calculer le nombre c_n de façons de payer n francs avec des pièces de 1 F et de 3 F.

Ex 10 - 2

Dans l'anneau $A = \mathbb{Z}/15\mathbb{Z}$ effectuer la division du polynôme $a(X) = \overline{5}X^3 + X + \overline{8}$ par $b(X) = \overline{8}X^2 + \overline{4}X + \overline{1}$.

Ex 10 - 3

Soit $p \in \mathbb{R}[X]$, tel que la fonction polynomiale associée soit périodique. Montrer que le polynôme $p(X)$ est constant. Généraliser à d'autres corps que $\mathbb{R}$.

Ex 10 - 4

Soient K un corps commutatif, algébriquement clos et $n \geqslant 2$ un entier non multiple de la caractéristique p. Montrer que dans K_*, il existe un unique sous-groupe U_n d'ordre n et que U_n est cyclique.

Ex 10 - 5

Dans l'anneau $A = \mathbb{Z}/35\mathbb{Z}$, montrer que $p(X) = X^2 - \overline{4}$ admet 4 racines et qu'il possède dans l'anneau $A[X]$ deux factorisations de la forme $(X - \alpha)(X - \beta)$.

Ex 10 - 6

Soit K un corps, avec $\text{caract}(K) \neq 2$. Dans $K[X]$, montrer que
$b(X) = X^3 + X^2 + X + 1$ divise $a(X) = X^n(X^3 + 2X^2 + 2X + 2)^n + X^{4n} - X^4 - 1$ si et seulement si n est pair.

Ex 10 - 7

Dans le plan affine euclidien, soit P une parabole. Pour tout cercle C qui rencontre P en quatre points, montrer que l'isobarycentre de ces quatre points appartient à l'axe de P.

Ex 10 - 8

a) Faire la liste de tous les polynômes de degré 1, 2 ou 3 sur le corps $K = \mathbb{Z}/2\mathbb{Z}$ et préciser pour chacun s'il est scindé, simple, irréductible.

b) Le polynôme $X^4 + X^2 + 1$ a-t-il des racines dans K ? Est-il irréductible ?

c) Montrer que $a(X) = X^4 + X + 1$ est irréductible dans $K[X]$ et dans $\mathbb{Z}[X]$.

Ex 10 - 9

Soit K un corps. Dans $K[X]$, montrer que $a(X) = (1+X)^{6n+1} - X^{6n+1} - 1$, où $n \in \mathbb{N}$, est divisible par $b(X) = (1 + X + X^2)^2$.

Ex 10 - 10

Soit $n \in \mathbb{N}^*$. Montrer que dans $\mathbb{C}$ la somme des racines $n^{\text{ièmes}}$ primitives de l'unité est $\mu(n)$, où $\mu : \mathbb{N}^* \to \mathbb{Z}$ désigne la fonction de Mœbius de valeurs $\mu(1) = 1$, $\mu(n) = 0$ si $n \geqslant 2$ a un facteur premier multiple et $\mu(n) = (-1)^k$ si n est le produit $p_1 \cdots p_k$ de k nombres premiers distincts.

Ex 10 - 11

Soient $m \in \mathbb{N}^*$ et $n \in \mathbb{N}^*$ premiers entre eux. On note $\Phi_n(X)$ le n-ième polynôme cyclotomique. Soit $d \in \mathbb{N}^*$ un diviseur de n. Montrer que pour tout $z \in \Lambda_{dm}$ on a $z^n \in \Lambda_m$. Montrer que

$$\Phi_m(X^n) = \prod_{d|n} \Phi_{dm}(X).$$

Soient $p, m \in \mathbb{N}_*$. Supposons p premier. Si p ne divise pas m, montrer que

$$\Phi_{mp}(X) = \frac{\Phi_m(X^p)}{\Phi_m(X)}.$$

Ex 10 - 12

Si p est premier, montrer que $(\mathbb{Z}/p\mathbb{Z})_*$ est un groupe cyclique. Montrer qu'il n'y a pas de réciproque à cet énoncé (considérer par exemple $\mathbb{Z}/9\mathbb{Z}$ ou $\mathbb{Z}/25\mathbb{Z}$).

Ex 10 - 13

Dans $\mathbb{Z}\,/\,17\,\mathbb{Z}$, montrer que les racines du polynôme $X^6 + X^4 + X^2 + 1$ sont toutes des carrés. Déterminer ces racines.

Ex 10 - 14

Résoudre l'équation en nombres entiers

$$x^6 - y^5 - 31z = 0.$$

Ex 10 - 15

a) Soient E un espace hermitien et u un endomorphisme normal de E. Montrer que tout $v \in \mathcal{L}(E)$ qui commute avec u commute avec l'adjoint u^* de u.

b) Soit $A \in \mathcal{M}_n(\mathbb{C})$ triangulaire supérieure et normale. Montrer que A est diagonale.

Ex 10 - 16

Soient K un corps commutatif, E un espace vectoriel sur K et $u \in \mathcal{L}(E)$.

a) Montrer que
$C(u) = \{x \in \mathcal{L}(E) \mid xu = ux\}$
est une sous-algèbre unifère de $\mathcal{L}(E)$.

b) Si $u \in \mathcal{L}(E)$ est diagonalisable, quelle est la dimension de $C(u)$ sur K ?

c) On pose $n = \dim(E)$. Montrer que les conditions suivantes sont équivalentes :
(i) $C(u)$ est commutative,
(ii) $\dim(C(u)) = n$,
(iii) $\text{card}\,(\text{sp}(u)) = n$.
(iv) $C(u) = \{\, p(u)\,;\ \ p \in K[X] \,\}$.

Ex 10 - 17

Soient E un espace vectoriel euclidien et $u \in \mathcal{L}(E)$ symétrique positif. Montrer qu'il existe $v \in \mathcal{L}(E)$, symétrique positif, unique, tel que $v^2 = u$.
Montrer que tout endomorphisme qui commute avec u commute avec v.

Ex 10 - 18

A l'aide des formules de Cardan-Tartaglia, déterminer les racines dans $\mathbb{C}$ de $a(X) = X^3 - 15X - 4$ et de $b(X) = X^3 + 6X - 2$.

Indications

Ex 10 - 1

S'inspirer de l'étude de l'anneau $K[X]$.

Ex 10 - 2

Appliquer l'algorithme de la division.

Ex 10 - 3

Si $p \in K[X]$, avec $\text{caract}(K) = 0$, alors $p(X) - p(0)$ a une infinité de racines.

Ex 10 - 4

Les éléments d'un sous-groupe d'ordre n de K_* sont racines de $X^n - 1$ d'après le th. de Lagrange (10-7, prop.).

Ex 10 - 5

$$\begin{aligned} p(X) &= (X - \overline{2})(X + \overline{2}) \\ &= (X - \overline{12})(X + \overline{12}). \end{aligned}$$

Ex 10 - 6

Raisonner modulo $b(X)$.

Ex 10 - 7

Choisir un repère orthonormé ayant le sommet de P pour origine et la tangente au sommet de P pour axe des abscisses.

Ex 10 - 8

a) Examiner l'existence de racines.

b) $X^4 + X^2 + 1 = (X^2 + X + 1)^2$.

c) $X^4 + X + 1$ est irréductible.

Ex 10 - 9

Si $\text{caract}(K) \neq 3$, vérifier que les racines de $X^2 + X + 1$ dans la clôture algébrique de K annulent $a(X)$ et $a'(X)$. Si $\text{caract}(K) = 3$, $b(X) = (X - 1)^4$.

Ex 10 - 10

Utiliser la décomposition primaire du groupe $\mathbb{U}_n$.

Ex 10 - 11

Toute racine de $\prod_{d|n} \Phi_{dm}(X)$ est racine de $\Phi_m(X^n)$. Comparer les degrés.

Ex 10 - 12

Utiliser 10-7, prop. Le groupe $(\mathbb{Z}/9\mathbb{Z})_*$ (resp. $(\mathbb{Z}/25\,\mathbb{Z})_*$) a pour générateur $\overline{2}$.

Ex 10 - 13

Les racines sont des racines de $X^8 - 1$.

Ex 10 - 14

Analogue à 10-7, ex. 2

Ex 10 - 15

Si u est normal, il est diagonalisable dans une base orthonormée. Examiner la matrice de u^* et utiliser le polynôme d'interpolation de Lagrange.

Ex 10 - 16

a) Vérification facile.

b) Un endomorphisme qui commute avec u laisse stable ses sous-espaces propres.

c) Pour (iii) $\Rightarrow$ (iv), noter qu'un endomorphisme qui commute avec u est diagonal. Utiliser le polynôme de Lagrange.

Ex 10 - 17

Il existe une base orthonormée de E qui diagonalise u, d'où l'existence d'une racine carrée positive de u, qui s'écrit $p(u)$ en utilisant le polynôme d'interpolation de Lagrange $p(X)$.

Ex 10 - 18

Appliquer 10-9 à ces exemples.

Solutions des exercices du chapitre 10

Ex 10 - 1

a) On sait que $A[[X]] = A^{\mathbb{N}}$ est un groupe commutatif pour l'addition. C'est un anneau. En effet, comme pour les polynômes, le produit est commutatif, associatif, distribue l'addition et a pour élément neutre $\mathbf{1} = (1,0,0,\ldots)$. La multiplication par les éléments de A en fait visiblement une A-algèbre. L'ensemble $A[X]$, des suites à support fini, est un sous-ensemble de $A[[X]]$, stable par addition, produit, multiplication par les éléments de A et $\mathbf{1} \in A[X]$. C'est une sous-algèbre de $A[[X]]$.

b) Soient $a, b \in A[[X]]$ non nulles, $p = \mathrm{val}(a)$, $q = \mathrm{val}(b)$. Alors

$$\begin{aligned} ab &= (a_pX^p + a_{p+1}X^{p+1} + \cdots)\,(b_qX^q + b_{q+1}X^{q+1} + \cdots) \\ &= a_pb_qX^{p+q} + (a_pb_{q+1} + a_{p+1}b_q)X^{p+q+1} + \cdots \end{aligned}$$

Si A est intègre, on a $a_pb_q \neq 0$. Donc $A[[X]]$ est intègre. On a, y compris si l'une des séries est nulle, l'inégalité suivante, avec égalité si A est intègre,

$$\mathrm{val}(ab) \geqslant \mathrm{val}(a) + \mathrm{val}(b)\,. \tag{1}$$

Réciproquement si $A[[X]]$ est intègre, le sous-anneau A est intègre.

c) Pour tous $a, b, c \in A[[X]]$ on a $\min(\mathrm{val}(a), \mathrm{val}(b)) \leqslant \mathrm{val}(a+b)$, d'où :

$$\begin{aligned} d(a,c) &= \exp[-\mathrm{val}(c-a)] = \exp[-\mathrm{val}((c-b)+(b-a))] \\ &\leqslant \max\{\exp[-\mathrm{val}(c-b)], \exp[-\mathrm{val}(b-a)]\} = \max[d(b,c), d(a,b)]\,. \end{aligned}$$

Il est clair que d est une distance. Toute série formelle $a = \sum a_nX^n$ est la limite, pour d, de la suite des polynômes $a_n = a_0 + \cdots + a_nX^n$ car le fait que $d(a,a_n) \to 0$ signifie que $\mathrm{val}(a-a_n) \to \infty$. Donc $A[X]$ est partout dense dans $A[[X]]$. Cette remarque, montre aussi qu'une suite (a_n) de $A[[X]]$ est de Cauchy pour cette distance, si pour tout $n_0 \in \mathbb{N}$ il existe $p_0 \in \mathbb{N}$ tel que pour pour tout $q \geqslant p_0$ la série formelle a_q a les mêmes coefficients que a_{p_0} de l'indice 0 jusqu'à l'indice n_0. On voit donc que toute suite de Cauchy a une limite dans $A[[X]]$. Ainsi $A[[X]]$ est complet. C'est le complété de $A[X]$ car $A[X]$ est partout dense dans $A[[X]]$.

d) Puisque $b \in A[[X]]$ est telle que $b_0 = 0$, on a $\mathrm{val}(b) \geqslant 1$. D'après (1), on obtient $\mathrm{val}(b^n) \geqslant n$ pour tout $n \in \mathbb{N}$. La suite de séries formelles $\sum_{k=0}^{n} a_k[b(X)]^k$ est donc de Cauchy. Elle converge dans $A[[X]]$.

e) Si $a \in A[[X]]$ a un inverse b on a $ab = 1$, soit

$$1 = a_0b_0 + (a_0b_1 + a_1b_0)X + \cdots \quad \text{d'où} \quad a_0b_0 = 1 \quad \text{et} \quad a_0 \in A_*\,.$$

Réciproquement, si $a_0 \in A_*$ on a $a = a_0(1 - \alpha_1X - \alpha_2X^2 + \cdots)$ où $\alpha_i = -a_0^{-1}a_i$ pour $i = 1,2,\ldots$ Posons $\alpha = \alpha_1X + \alpha_2X^2 + \cdots$ D'après d), on peut considérer la série formelle $\beta = 1 + \alpha + \alpha^2 + \cdots$ C'est un inverse pour $1 - \alpha$. En effet, pour tout $n \in \mathbb{N}_*$, le $n^{\text{ième}}$ coefficient de $(1-\alpha)\beta$ est nul car les coefficients $\beta_0, \beta_1, \cdots, \beta_n$ de β sont les mêmes que ceux de la somme finie $1 + \alpha + \cdots + \alpha^n$ et $(1-\alpha)(1+\alpha+\cdots+\alpha^n) = 1 - \alpha^{n+1}$. Donc $a = a_0(1-\alpha)$ a pour inverse $a_0^{-1}\beta$.

Dans tout anneau commutatif unifère, le groupe des éléments inversibles est le complémentaire de la réunion des idéaux maximaux (voir Ex. 9-8). Dans $A[[X]]$, c'est le complémentaire de l'idéal $(X) = \{a \in A[[X]] \mid \mathrm{val}(a) \geqslant 1\}$ engendré par X. Donc (X) est maximal et il est unique.

f) Si $a(X) = \sum a_n X^n$, posons $a'(X) = \sum (n+1)a_{n+1}X^n$. Il est évident que l'opération de dérivation $\frac{d}{dX} : a \mapsto a'$ est A-linéaire. Elle est continue : si $a_n \to a$, alors $\mathrm{val}(a - a_n) \to \infty$ et $\mathrm{val}(a' - a'_n) \to \infty$. Vérifions que $(ab)' = a'b + ab'$. D'après 10-4, cela est vrai sur $A[X]$. Par densité dans $A[[X]]$, la formule se prolonge car

$$\begin{aligned} d(ab\,,\,a_nb_n) &\leqslant \max[\,d(ab\,,\,ab_n)\,,\,d(ab_n\,,\,a_nb_n)\,] \\ &\leqslant \max\,[\,e^{-\mathrm{val}(a)-\mathrm{val}(b-b_n)}\,,\,e^{-\mathrm{val}(a-a_n)-\mathrm{val}(b_n)}\,] \\ &\leqslant \max\,[\,d(b,b_n),d(a,a_n)\,]\,. \end{aligned}$$

g) Dans $K[X]$, l'idéal (X) est maximal et donc premier. Son complémentaire $S = \{p \in K[X] \mid p(0) \neq 0\}$ est donc multiplicativement stable. On peut considérer l'anneau $K(X)_0$ des fractions $\frac{a(X)}{b(X)}$, où $a \in K[X]$ et $b \in S$. La propriété universelle de $K(X)_0$ montre que l'homomorphisme $p \mapsto p$ de $K[X]$ dans $K(X)$ se prolonge à $K(X)_0$ ce qui permet d'identifier $K(X)_0$ avec un sous-anneau de $K(X)$.

Par ailleurs, $\varphi : a \mapsto a$ de $K[X]$ dans $K[[X]]$ est un homomorphisme d'anneaux injectif. D'après d), il est tel que $\varphi(S) \subset K[[X]]_*$. Il existe donc (9-10, prop.), un homomorphisme injectif Φ de $K(X)_0$ dans $K[[X]]$ prolongeant φ, unique.

Notons que si on décompose $\frac{a}{b} \in K(X)_0$ en éléments simples, alors $\Phi(\frac{a}{b})$ est somme des images de ces éléments. D'après e), où on prend $\alpha = X$, $\varphi(\frac{1}{1-X}) = \Sigma X^n$.

h) D'après e), $\begin{aligned}(1-X)^{-1} &= 1 + X + X^2 + \cdots + X^p + \cdots = \Sigma\, a_n X^n \\ (1-X^2)^{-1} &= 1 + X^2 + X^4 + \cdots + X^{2q} + \cdots = \Sigma\, b_n X^n\end{aligned}$

L'inverse de $1 - X - X^2 + X^3 = (1-X)(1-X^2)$ sera $(1-X)^{-1}(1-X^2)^{-1}$, soit

$$\sum_{n=0}^{\infty} c_n X^n \qquad \text{où} \qquad c_n = a_0b_n + a_1b_{n-1} + \cdots + a_nb_0 = 1 + \cdots + 1\,,$$

somme où 1 apparaît autant de fois qu'il existe $(p,q) \in \mathbb{N}^2$ tels que $p + 2q = n$. C'est le nombre de façons de payer n francs avec des pièces de $1F$ ou de $2F$. Pour calculer la suite (c_n), décomposons en éléments simples dans le corps $\mathbb{C}(X)$:

$$r(X) = \frac{1}{(1-X)(1-X^2)} = \frac{1}{(1-X)^2(1+X)} = \frac{a}{(1-X)^2} + \frac{b}{1-X} + \frac{c}{1+X}.$$

Prenons $X = 1$ dans $(1-X)^2 r(X)$ et $X = -1$ dans $(1+X)r(X)$. Il vient $a = \frac{1}{2}$ et $c = \frac{1}{4}$. Enfin $X = 0$ donne $b = \frac{1}{4}$. D'où le développement de $r(X)$:

$$1 + \cdots + \left(\frac{n+1}{2} + \frac{1}{4} + \frac{(-1)^n}{4}\right) X^n + \cdots$$

Ainsi, pour n pair on a $c_n = \frac{n}{2} + 1$, et pour n impair $c_n = \frac{n+1}{2}$.

Ex 10 - 2

Dans $\mathbb{Z}/15\mathbb{Z}$, $\overline{8}$ est inversible car $\overline{2} \times \overline{8} = \overline{1}$. On peut donc effectuer la division euclidienne de $a(X)$ par $b(X)$. On obtient, $q(X) = \overline{10}\,X + \overline{10}$, $r(X) = \overline{11}\,X + \overline{13}$.

Ex 10 - 3

Supposons qu'il existe $T \in \mathbb{R}^*$ tel que $a(\lambda + T) = a(\lambda)$ pour tout $\lambda \in \mathbb{R}$. Le polynôme $b(X) = a(X) - a(0)$ admet pour racine kT, pour tout $k \in \mathbb{Z}$. La caractéristique de $\mathbb{R}$ étant nulle, pour $k \neq k'$ on a $(k - k')T \neq 0$. Le polynôme $b(X)$ admet une infinité de racines. C'est le polynôme nul (10-3, cor. 3). Plus généralement, ce raisonnement est valable sur un corps de caractéristique nulle.

Ex 10 - 4

Comme K est algébriquement clos, $X^n - 1$ admet n racines, distinctes ou confondues, dans K. Si λ est l'une de ces racines, alors λ n'annule pas le polynôme dérivé nX^{n-1} (sinon on aurait $0 = n\lambda^n = n1$ ce qui est exclu par l'hypothèse faite sur la caractéristique). Les racines sont donc simples. D'après 10-7, prop., l'ensemble des racines de $X^n - 1$ est un sous-groupe U_n d'ordre n de K_*. C'est le seul sous-groupe d'ordre n de K_*. Il est cyclique. Dans $\mathbb{N}^* \backslash \mathbb{Z}p$, les conditions $m \mid n$ et $U_m \subset U_n$ sont équivalentes.

Ex 10 - 5

On a $X^2 - \overline{4} = (X - \overline{2})(X + \overline{2})$. Si $p(X) = (X - \alpha)(X - \beta)$ est une autre factorisation, on aura $\alpha + \beta = \overline{0}$, $\alpha\beta = -\overline{4}$, soit $\beta = -\alpha$, $\alpha^2 = \overline{4}$. Or $\overline{4}$ admet quatre racines carrées $\overline{2}$, $-\overline{2}$, $\overline{12}$, $-\overline{12}$ dans $\mathbb{Z}/35\mathbb{Z}$ (voir Ex. 12-1). Il existe donc deux factorisations $X^2 - \overline{4} = (X - \overline{2})(X + \overline{2}) = (X - \overline{12})(X + \overline{12})$, chose impossible sur un corps.

Ex 10 - 6

Modulo l'idéal (b) de $K[X]$ engendré par $b(X) = X^3 + X^2 + X + 1$, on a
$X^3 + 2X^2 + 2X + 2 = 2b(X) - X^3 \equiv -X^3$ et $X^4 \equiv 1$ car $X^4 - 1 = (X - 1)b(X)$.
On en déduit :

$$X^n(X^3 + 2X^2 + 2X + 2)^n \equiv X^n(-X^3)^n = (-1)^n X^{4n} \equiv (-1)^n \quad , \quad X^{4n} - X^4 - 1 \equiv -1 .$$

On en déduit $a(X) \equiv (-1)^n - 1 = 0$, d'où la conclusion.

Ex 10 - 7

Plaçons-nous dans le repère orthonormé $(O, \overrightarrow{\imath}, \overrightarrow{\jmath})$ où O est le sommet de P, où $\overrightarrow{\imath}$ dirige la tangente au sommet. L'équation de P est alors de la forme $y = kx^2$ et celle du cercle C est $x^2 + y^2 - 2ax - 2by + c = 0$. Les abscisses x_1, x_2, x_3, x_4 des points d'intersection sont les solutions de l'équation :

$$k^2x^4 + (1 - 2bk)x^2 - 2ax + c = 0 .$$

Les relations entre coefficients et racines du polynôme, montrent que $x_1 + x_2 + x_3 + x_4 = 0$. L'abscisse de G est donc $x_G = \frac{1}{4}\sum x_i = 0$ et G appartient à l'axe de P.

Ex 10 - 8

a) Un polynôme de degré 2 ou 3, est irréductible si et seulement s'il ne s'annule pas. (Ce n'est plus vrai pour les degrés supérieurs ou égaux à 4.)

degré 1 :	X , $X+\overline{1}$	irréductibles
degré 2 :	X^2 , $X^2+\overline{1}=(X+\overline{1})^2$, $X^2+X=X(X+\overline{1})$	scindés
	$X^2+X+\overline{1}$	irréductible
degré 3 :	X^3	scindé
	$X^3+\overline{1}=(X+\overline{1})(X^2+X+\overline{1})$	non scindé
	$X^3+X=X(X+\overline{1})^2$	scindé
	$X^3+X+\overline{1}$	irréductible
	$X^3+X^2=X^2(X+\overline{1})$	scindé
	$X^3+X^2+\overline{1}$	irréductible
	$X^3+X^2+X=X(X^2+X+\overline{1})$	non scindé
	$X^3+X^2+X+\overline{1}=(X+\overline{1})^3$	scindé

b) On a $X^4+X^2+\overline{1}=(X^2+X+\overline{1})^2$ sans racine mais réductible.

c) Le polynôme $X^4+X+\overline{1}$ n'a pas de facteur de degré 1 car il ne s'annule ni pour $X=\overline{0}$, ni pour $X=\overline{1}$. Supposons qu'il admette la factorisation

$$X^4+X+\overline{1}=(aX^2+bX+c)\,(a'X^2+b'X+c')\,.$$

On a $aa'=\overline{1}$, d'où $a\neq 0$ et $a'\neq 0$ et donc $a=\overline{1}=a'$. De même, $c=\overline{1}=c'$. Aux degrés 3 et 1, il vient $b+b'=0$, $b+b'=\overline{1}$, absurde. Cette factorisation de $X^4+X+\overline{1}$ est impossible. Ce polynôme est irréductible dans $K[X]$.

Si $a(X)$ était réductible dans $\mathbb{Z}[X]$, de la forme

$$X^4+X+1=(a_pX^p+\cdots+a_0)\,(b_qX^q+\cdots+b_0)\,,$$

avec $1\leqslant p\leqslant 3$, $p+q=4$, $a_i,b_j\in\mathbb{Z}$, on en déduirait sur $\mathbb{Z}/2\mathbb{Z}$ (10-1, ex. 1),

$$X^4+X+\overline{1}=(\overline{a}_pX^p+\cdots+\overline{a}_0)\,(\overline{b}_qX^q+\cdots+\overline{b}_0)\,,$$

avec $\overline{a}_p\overline{b}_q=\overline{1}$ et donc $\overline{a}_p\neq\overline{0}$ et $\overline{b}_q\neq\overline{0}$. Or nous venons de voir que dans $K[X]$ cela est impossible. Le polynôme est donc irréductible dans $\mathbb{Z}[X]$.

Ex 10 - 9

Premier cas. Supposons $\text{caract}(K)\neq 3$. Dans la clôture algébrique K_0 de K, le polynôme $p(X)=X^3-1$ admet trois racines $1,j,j'$. Elles sont distinctes car elles n'annulent pas $p'(X)=3X^2$ puisque $3\times\mathbf{1}\neq 0$. Le produit des racines de $p(X)$ est 1 donc $j'=j^{-1}$. On a aussi $j^3=1$ et donc $j^{-1}=j^2$, comme dans $\mathbb{C}$ (voir Ex. 10-4 à ce sujet). On en déduit $X^3-1=(X-1)(X-j)(X-j')=(X-1)(X^2+X+1)$. L'anneau $K[X]$ étant intègre, $X^2+X+1=(X-j)(X-j')$. Pour montrer le résultat, vérifions que j et j' sont racines d'ordre deux au moins de $a(X)$. Faisons-le pour j par exemple, en montrant que $a(j)=0$ et $a'(j)=0$. Comme la somme des racines de $p(X)$ est $1+j+j'=0$, on a

$$a(j)=(j+1)^{6n+1}-j^{6n+1}-1=(-j')^{6n+1}-j^{6n+1}-1=-j'-j-1=0\,,$$

$$a'(j)=(6n+1)(j+1)^{6n}-(6n+1)j^{6n}=(6n+1)(-j')^{6n}-(6n+1)j^{6n}=0\,.$$

Deuxième cas. Supposons $\text{caract}(K)=3$. Les arguments précédents ne s'appliquent plus car $3X^2$ est le polynôme nul. On a $(X^2+X+1)^2=(X^2-2X+1)^2=(X-1)^4$. Posons $Y=X-1$ et vérifions que Y^4 divise $a(1+Y)$. On a :

$$(1+Y)^{6n+1} = 1 + C^1_{6n+1}Y + \tfrac{1}{2}(6n+1)6n\,Y^2 + C^3_{6n+1}Y^3 + C^4_{6n+1}Y^4 + \cdots$$
$$(-1+Y)^{6n+1} = -1 + C^1_{6n+1}Y - \tfrac{1}{2}(6n+1)6n\,Y^2 + C^3_{6n+1}Y^3 - C^4_{6n+1}Y^4 + \cdots$$

Puisque $3n = 0$ on obtient :

$$a(1+Y) = (-1+Y)^{6n+1} - (1+Y)^{6n+1} - 1 = -2\,C^4_{6n+1}Y^4 + \cdots = Y^4 a_1(Y)\,.$$

Ex 10 - 10

Pour $n = 1$ la formule est vraie. Supposons $n \geqslant 2$. Soit $n = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$ sa décomposition en facteurs premiers. D'après 3-6, cor. 3, $\mathbb{U}_n$ est le produit direct de ses composantes primaires $H_1, \ldots, H_k$. D'après 3-3, prop., pour $i = 1, \ldots, k$ il existe dans le groupe cyclique $\mathbb{U}_n$ un unique sous-groupe d'ordre p^{α_i}. On a donc $H_i = \mathbb{U}_{p^{\alpha_i}}$. Ainsi, l'application $f : (z_1, \ldots, z_k) \mapsto z_1 \cdots z_k$ est un isomorphisme de $G = \mathbb{U}_{p^{\alpha_1}} \times \cdots \times \mathbb{U}_{p^{\alpha_k}}$ sur $\mathbb{U}_n$. Pour $i = 1, \ldots, k$, notons Λ_i l'ensemble des générateurs de $\mathbb{U}_{p^{\alpha_i}}$. Alors f induit une bijection de l'ensemble $\Lambda_1 \times \cdots \times \Lambda_k$ des générateurs de G sur l'ensemble Λ des générateurs de $\mathbb{U}_n$. On a donc

$$\sum_{z\in\Lambda} z = \sum_{z_1\in\Lambda_1} \cdots \sum_{z_k\in\Lambda_k} z_1 \cdots z_k = \Big(\sum_{z_1\in\Lambda_1} z_1\Big) \cdots \Big(\sum_{z_k\in\Lambda_k} z_k\Big)\,.$$

D'après 10-6, ex. 2, si n admet un facteur multiple, par exemple si $\alpha_1 \geqslant 2$, alors on a $\Phi_{p_1^{\alpha_1}}(X) = \Phi_{p_1^{\alpha_1-1}}(X^{p_1})$ et donc $\sum_{z_1\in\Lambda_1} z_1 = 0$ et $\sum_{z\in\Lambda} z = 0 = \mu(n)$.
Si pour tout $i = 1, \ldots, k$ on a $a_i = 1$, alors $\Phi_{p_i}(X) = X^{p_i-1} + X^{p_i-2} + \cdots + X + 1$ et $\sum_{z_i\in\Lambda_i} z_i = -1$ donc $\sum_{z\in\Lambda} z = (-1)^k = \mu(n)$.

Ex 10 - 11

Si $d \mid n$ et si $m \wedge n = 1$, alors $m \wedge d = 1$. On a $\mathrm{d}^\circ(\Phi_{dm}) = \varphi(dm) = \varphi(d)\varphi(m)$ (3-4, cor. 2). Puisque $n = \prod_{d\mid n} \varphi(n)$, on en déduit que $\mathrm{d}^\circ(\prod_{d\mid n} \Phi_{dm}(X))$ a pour valeur :

$$\sum_{d\mid n} \mathrm{d}^\circ(\Phi_{dm}(X)) = \Big[\sum_{d\mid n} \varphi(d)\Big]\varphi(m) = n\varphi(m) = n\,\mathrm{d}^\circ(\Phi_m(X)) = \mathrm{d}^\circ(\Phi_m(X^n))\,.$$

Soit $z \in \Lambda_{dm}$. Son ordre est $o(z) = dm$ et $\langle z\rangle = \mathbb{U}_{dm}$. D'après 3-1, $o(z^n) = \frac{dm}{dm\wedge n}$. Comme d divise n, il existe $n_1 \in \mathbb{N}$, tel que $n = dn_1$ et on a $m \wedge n_1 = 1$ car $m \wedge n = 1$. On en déduit $dm \wedge n = dm \wedge dn_1 = d(m \wedge n_1) = d$ et $o(z^n) = m$, soit $z^n \in \Lambda_m$. Ainsi, pour tout diviseur d de n, tout $z \in \Lambda_{dm}$ est racine de $\Phi_m(X^n)$. Les polynômes $\Phi_{dm}(X)$, où $d \mid n$, ont des racines simples. Les ensembles Λ_{dm} de leurs racines sont disjoints. Donc $\prod_{d\mid n} \Phi_{dm}(X)$ est un polynôme simple de $\mathbb{C}[X]$, dont tous les facteurs $X - \zeta$ apparaissent dans $\Phi_m(X^n)$. Il divise donc $\Phi_m(X^n)$. Ces deux polynômes étant unitaires de même degré, ils sont égaux.

Si $p \in \mathcal{P}$ ne divise pas m, on a $m \wedge p = 1$. D'après ce qui précède,

$$\Phi_m(X^p) = \prod_{d\mid p} \Phi_{dm}(X) = \Phi_m(X)\Phi_{pm}(X) \quad \text{d'où} \quad \Phi_{pm}(X) = \frac{\Phi_m(X^p)}{\Phi_m(X)}\,.$$

Ex 10 - 12

On sait que p est premier si et seulement si $K = \mathbb{Z}/p\mathbb{Z}$ est un corps (9-11, cor. 1). Alors le groupe fini K_* est cyclique (10-7, cor. 1). Puisque 9 n'est pas premier, l'anneau $A = \mathbb{Z}/9\mathbb{Z}$ n'est pas un corps. On a $[A_* : 1] = \varphi(3^2) = 3^2 - 3 = 6$. On a $\overline{2} \in A_*$ car $\overline{2} \times \overline{5} = \overline{1}$. L'ordre $o(\overline{2})$ de $\overline{2}$ divise $[A_* : 1]$ donc $o(\overline{2}) \in \{2, 3, 6\}$. On a $\overline{2}^2 = \overline{4} \neq \overline{1}$,

$\overline{2}^3 = \overline{8} = -\overline{1} \neq \overline{1}$ donc $o(\overline{2}) = 6$. Ainsi $\overline{2}$ engendre A_* qui est cyclique. On vérifie de même que $(\mathbb{Z}/25\mathbb{Z})_*$ est cyclique, engendré par $\overline{2}$.

Ex 10 - 13

Puisque 17 est premier, $K = \mathbb{Z}/17\,\mathbb{Z}$ est un corps. D'après 10-7, cor. 1, K_* est cyclique, d'ordre 16. D'après 3-3, prop., K_* possède un unique sous-groupe d'ordre 8 qui est cyclique,

$$H = \{x \in K_* \mid x^8 = 1\} = \{x \in K_* \mid \exists\, y \in G \quad x = y^2\}.$$

Ainsi, H est l'ensemble des racines de $X^8 - 1 = (X^2 - 1)(X^6 + X^4 + X^2 + 1)$ et c'est également l'ensemble des carrés de K_*. Ces carrés sont :

$$\overline{1}^2 = \overline{1}\ ,\ \overline{2}^2 = \overline{4}\ ,\ \overline{3}^2 = \overline{9}\ ,\ \overline{4}^2 = -\overline{1}\ ,\ \overline{5}^2 = \overline{8}\ ,\ \overline{6}^2 = \overline{2}\ ,\ \overline{7}^2 = \overline{15}\ ,\ \overline{8}^2 = \overline{13}.$$

Les racines de $a(X)$ sont les racines de $X^8 - 1$ autres que $\overline{1}$ et $-\overline{1}$, c'est-à-dire $\overline{4}$, $\overline{9}$, $\overline{8}$, $\overline{2}$, $\overline{15}$, $\overline{13}$. (On peut aussi vérifier que $\overline{2}$ est d'ordre 8 et donc générateur de H. Les racines de $X^8 - 1$ sont donc les puissances de $\overline{2}$.)

Ex 10 - 14

Soient $x, y \in \mathbb{Z}$. Il existe $z \in \mathbb{Z}$ vérifiant (1) si et seulement si dans $\mathbb{Z}/31\mathbb{Z}$ les classes $\overline{x}, \overline{y}$ de x, y sont telles que $\overline{x}^6 = \overline{y}^5$. Comme 31 est premier, $K = \mathbb{Z}/31\mathbb{Z}$ est un corps et donc intègre. Si $\overline{y} = \overline{0}$ on a donc $\overline{x} = \overline{0}$ et si $\overline{x} = \overline{0}$ on a $\overline{y} = \overline{0}$.

Supposons $\overline{x} \neq \overline{0}$ et $\overline{y} \neq \overline{0}$ et considérons $\overline{a} = \overline{x}^6 = \overline{y}^5 \in K_*$. Comme K est un corps fini, K_* est un groupe cyclique d'ordre $30 = 5 \times 6$. D'après 3-3, prop., il existe un sous-groupe d'ordre 5 unique, soit :

$$H_5 = \{\overline{k} \in K_* \mid \exists\, \overline{x} \in K_* \quad \overline{k} = \overline{x}^6\} = \{\overline{k} \in K_* \mid \overline{k}^5 = \overline{1}\}.$$

De même, il existe dans K_* un sous-groupe d'ordre 6 unique, soit :

$$H_6 = \{\overline{k} \in K_* \mid \exists\, \overline{y} \in K_* \quad \overline{k} = \overline{y}^5\} = \{\overline{k} \in K_* \mid \overline{k}^6 = \overline{1}\}.$$

On voit que $\overline{a} = \overline{x}^6 = \overline{y}^5$ appartient à $H_5 \cap H_6 = \{\overline{1}\}$. Ainsi $\overline{a} = \overline{1}$. On a donc $\overline{x}^6 = \overline{1}$ soit $\overline{x} \in H_6$ et $\overline{y}^5 = \overline{1}$ soit $\overline{y} \in H_5$. Tout choix de $\overline{x} \in H_6$ et $\overline{y} \in H_5$ donnera des solutions pour l'équation $\overline{x}^6 = \overline{y}^5$. Pour déterminer les sous-groupes H_5 et H_6 de K_*, cherchons un générateur de K_*. Un essai avec $\overline{2}$ montre que l'ordre est $o(\overline{2}) = 5$ donc $H_5 = \langle\overline{2}\rangle = \{\overline{1}, \overline{2}, \overline{4}, \overline{8}, \overline{16}\}$. L'ordre de $\overline{3}$ doit diviser l'ordre 30 de K_* et ne peut être que 2 , 3 , 5 , 6 , 10 , 15 ou 30 . On a

$$\overline{3}^2 = \overline{9}\ \ ,\ \ \overline{3}^3 = -\overline{4}\ \ ,\ \ \overline{3}^5 = -\overline{5}\ \ ,\ \ \overline{3}^6 = \overline{16}\ \ ,\ \ \overline{3}^{10} = -\overline{6}\ \ ,\ \ \overline{3}^{15} = -\overline{1},$$

donc $o(\overline{3}) = 30$ et $\langle\overline{3}\rangle = K_*$. Alors H_6 engendré par $\overline{3}^5 = -\overline{5}$, a pour éléments

$$\overline{1}\ \ ,\ \ \overline{3}^5 = -\overline{5}\ \ ,\ \ \overline{3}^{10} = \overline{25}\ \ ,\ \ \overline{3}^{15} = -\overline{1}\ \ ,\ \ \overline{3}^{20} = \overline{5}\ \ ,\ \ \overline{3}^{25} = \overline{6}.$$

Les solutions de (1) s'obtiennent en choisissant x_0, y_0 tels que $\overline{x}_0 \in H_5$ et $\overline{y}_0 \in H_6$, puis $k, k' \in \mathbb{Z}$. On prend alors $x = x_0 + k31$, $y = y_0 + k'31$ et z est le quotient de $x^6 - y^5$ par 31 (on a $x^6 - y^5$ multiple de 31 car $x_0^6 - y_0^5$ est multiple de 31).

Ex 10 - 15

a) Si u est normal, c'est-à-dire si $u^*u = uu^*$, il existe une base orthonormée $\mathcal{B}$ de E dans laquelle la matrice M_u de u est diagonale (voir 13-2, cor. 2), soit

$$M_u = \begin{pmatrix} \lambda_1 & \cdots & 0 \\ \cdots & \cdots & \cdots \\ 0 & \cdots & \lambda_n \end{pmatrix} \qquad \text{d'où} \qquad M_{u^*} = \begin{pmatrix} \overline{\lambda}_1 & \cdots & 0 \\ \cdots & \cdots & \cdots \\ 0 & \cdots & \overline{\lambda}_n \end{pmatrix}.$$

Si le spectre de u est $\{\lambda_1, \cdots, \lambda_k\}$, celui de u^* est $\{\overline{\lambda_1}, \ldots, \overline{\lambda_k}\}$. Dans $\mathbb{C}[X]$, soit $p(X) = a_0 + \cdots + a_{k-1}X^{k-1}$ le polynôme d'interpolation de Lagrange, unique polynôme de degré au plus $k-1$ tel que $p(\lambda_1) = \overline{\lambda}_1, \ldots, p(\lambda_k) = \overline{\lambda}_k$. Dans la base $\mathcal{B}$, la matrice de $p(u)$ est égale à celle de u^* donc $u^* = p(u)$. On en déduit que tout $v \in \mathcal{L}(E)$ qui commute avec u, commute également avec u^*.

b) Soit $t \in \mathcal{L}(\mathbb{C}^n)$ dont A est la matrice dans la base canonique $\mathcal{B}_0 = (e_1, \cdots, e_n)$ de $\mathbb{C}^n$. Alors A est triangulaire supérieure si et seulement si t laisse stable les sous-espaces vectoriels $V_1 = \text{Vect}(e_1)$, $V_2 = \text{Vect}(e_1, e_2), \ldots, V_{n-1} = \text{Vect}(e_1, \ldots, e_{n-1})$. Si A est normale, alors on a vu en a) que $t^* = p(t)$, où $p \in \mathbb{C}[X]$. Donc t^* laisse stable $V_1, V_2, \ldots, V_{n-1}$. La matrice A^* de t^* dans $\mathcal{B}_0$ est donc elle aussi triangulaire supérieure. Or A^* est la conjuguée de la transposée de A. Donc A est diagonale.

Ex 10 - 16

a) Pour tous $x, y \in C(u)$ on a

$$\begin{aligned} (x+y)u &= xu + yu = ux + uy = u(x+y), \\ (xy)u &= x(yu) = x(uy) = (xu)y = (ux)y = u(xy), \end{aligned}$$

donc $x + y \in C(u)$ et $xy \in C(u)$. On a aussi $(\lambda 1)u = u(\lambda 1)$ donc $\lambda 1 \in C(u)$, pour tout $\lambda \in K$. Ainsi, $C(u)$ est une sous-algèbre unifère de $\mathcal{L}(E)$.

b) Supposons u diagonalisable, de valeurs propres $\lambda_1, \ldots, \lambda_k$, de sous-espaces propres $E_1, \ldots, E_k$. Tout $v \in C(u)$ laisse stable $E_i = \text{Ker}\,(u - \lambda_i \,\text{Id}_E)$, pour $i = 1, \ldots, k$ car v commute avec $u - \lambda_i \,\text{Id}_E$. Choisissons des bases de $E_1, \ldots, E_k$. Leur réunion $\mathcal{B}$ est une base de E. Dans cette base, les matrices A de u et M_v de v sont

$$A = \begin{pmatrix} \lambda_1 I_{n_1} & \cdots & 0 \\ \cdots & \cdots & \cdots \\ 0 & \cdots & \lambda_k I_{n_k} \end{pmatrix} \quad , \quad M_v = \begin{pmatrix} A_1 & \cdots & 0 \\ \cdots & \cdots & \cdots \\ 0 & \cdots & A_k \end{pmatrix},$$

où $A_i \in \mathcal{M}_{n_i}(k)$, $n_i = \dim(E_i)$. Réciproquement, si la matrice M_v de v est de ce type, elle commute avec A. On voit que $\varphi : v \mapsto M_v$ donne un isomorphisme d'algèbres de C_u sur $\mathcal{M}_{n_1} \times \cdots \times \mathcal{M}_{n_k}$. On a donc $\dim(C(u)) = n_1^2 + \cdots + n_k^2$.

c) $(i) \Rightarrow (iii)$ $C(u)$ est commutative si et seulement si $\mathcal{M}_{n_1}, \ldots, \mathcal{M}_{n_k}$ sont commutatives, c'est-à-dire si $n_1 = 1, \ldots, n_k = 1$. Cela nécessite $n = k$ car on a :

$$(1) \qquad n = \dim(E) = \dim(E_1) + \cdots + \dim(E_n) = n_1 + \cdots + n_k,$$

(iii) $\Rightarrow$ (ii) Si $k = n$, d'après (1) on a $n_1 = 1, \ldots, n_k = 1$ et $\dim(C(u)) = n$.

(ii) $\Rightarrow$ (i) Si on a $n = n_1 + \cdots + n_k = n_1^2 + \cdots + n_k^2 = \dim(C(u))$, on voit que $n_1 = 1, \ldots, n_k = 1$ et $k = n$. Alors $C(u)$ est commutative.

(iii) $\Rightarrow$ (iv) La sous-algèbre $\{\, p(u) \,;\ p \in K[X] \,\}$ de $\mathcal{L}(E)$ engendrée par u est contenue dans le commutant $C(u)$ de u. Si (iii) est vérifiée, u a n valeurs propres distinctes $\lambda_1, \ldots, \lambda_n$. Soit $v \in C(u)$. D'après b), dans la base $\mathcal{B}$, on a

$$A = \begin{pmatrix} \lambda_1 & \cdots & 0 \\ \cdots & \cdots & \cdots \\ 0 & \cdots & \lambda_n \end{pmatrix} \quad , \quad M_v = \begin{pmatrix} \mu_1 & \cdots & 0 \\ \cdots & \cdots & \cdots \\ 0 & \cdots & \mu_n \end{pmatrix} .$$

Introduisons le polynôme d'interpolation de Lagrange $p(X)$, de degré au plus $n-1$, tel que $\mu_1 = p(\lambda_1), \ldots, \mu_n = p(\lambda_n)$. On voit alors que $M_v = M_{p(u)}$ et donc que $v = p(u)$. Ainsi $C(u)$ est égale à la sous-algèbre $\{ p(u) ; \ p \in K[X] \}$ engendrée par u.

$(iv) \Rightarrow (i)$ est évident.

Ex 10 - 17

On sait, et cela sera revu en 13-2, cor. 1, que si u est symétrique, il existe une base orthonormée $\mathcal{B} = (e_1, \ldots, e_n)$ de E dans laquelle la matrice de u est

$$A = \begin{pmatrix} \lambda_1 & \cdots & 0 \\ \cdots & \cdots & \cdots \\ 0 & \cdots & \lambda_n \end{pmatrix} . \text{ Posons } \quad B = \begin{pmatrix} \sqrt{\lambda_1} & \cdots & 0 \\ \cdots & \cdots & \cdots \\ 0 & \cdots & \sqrt{\lambda_n} \end{pmatrix} .$$

Cela est possible car ici on a $\lambda_1 = (u(e_1)|e_1) \geqslant 0, \ldots, \lambda_n = (u(e_n)|e_n) \geqslant 0$. Notons $u^{1/2}$ l'endomorphisme de matrice B dans la base $\mathcal{B}$. On a évidemment $(u^{1/2})^2 = u$. Soit $\{\lambda_1, \ldots, \lambda_k\}$ le spectre de u et soit $p(X)$ le polynôme d'interpolation de Lagrange, de degré $k-1$, tel que $p(\lambda_i) = \sqrt{\lambda_i}$ pour $i = 1, \ldots, k$. Alors $p(A) = B$ donc $p(u) = u^{1/2}$. Tout endomorphisme de E qui commute avec u commute donc avec $u^{1/2}$.

Soit $v \in \mathcal{L}(E)$ symétrique et positif tel que $v^2 = u$. Montrons que $v = u^{1/2}$. Comme v commute avec $v^2 = u$, il commute avec $u^{1/2} = p(u)$. Il laisse stable les sous-espaces propres $E_1, \ldots, E_k$ de u et induit sur $E_1, \ldots, E_k$ des endomorphismes symétriques positifs. Pour $i = 1, \ldots, k$, il existe une base orthonormée $\mathcal{B}_i$ de E_i qui diagonalise $v|_{E_i}$, avec les valeurs propres $\mu_1, \ldots, \mu_s$. Comme $v^2 = u = (u^{1/2})^2$, sur les vecteurs de $\mathcal{B}_i$ on obtient $\mu_1^2 = (\sqrt{\lambda_1})^2, \ldots, \mu_s^2 = (\sqrt{\lambda_1})^2$, d'où $\mu_1 = \cdots = \mu_s = \sqrt{\lambda_1}$ car ces réels sont positifs. Ainsi, $v|_{E_i} = u^{1/2}|_{E_i}$ pour $i = 1, \ldots, k$ et $v = u^{1/2}$.

Ex 10 - 18

$a(X) = X^3 + pX + q$, avec $p = -15$, $q = -4$. Le trinôme résolvant :

$$r(X) = X^2 + qX - \tfrac{p^3}{27} = X^2 - 4X + 125 = (X-2)^2 + 11^2$$

a un discriminant $\Delta < 0$. Donc $p(X)$ a trois racines réelles. Les racines de $r(X)$ sont $U = 2 + 11i$, $V = \overline{U} = 2 - 11i$ et on a $\overline{U}U = 125 = 5^3$. Déterminons une racine cubique $u = x + iy$ de U. On doit avoir $(|u|^3)^2 = |U|^2 = 5^3$ donc $|u|^2 = 5$. Les parties réelle et imaginaire de $u^3 = U$ étant entières, on peut espérer qu'il en est de même pour u. En fait, $u = 2 + i$ convient. Posons $v = \overline{u} = 2 - i$. Les formules de Cardan-Tartaglia donnent les racines de $a(X)$:

$$\begin{aligned} x_1 &= u + v = 4 , \\ x_2 &= u\bar{j} + \overline{u}\, j = 2\mathcal{R}\mathrm{e}(u\bar{j}) = \mathcal{R}\mathrm{e}((2+i)(-1-i\sqrt{3})) = -2 + \sqrt{3} , \\ x_3 &= uj + \overline{u}\bar{j} = 2\mathcal{R}\mathrm{e}(uj) = \mathcal{R}\mathrm{e}((2+i)(-1+i\sqrt{3})) = -2 - \sqrt{3} . \end{aligned}$$

On a $b(X) = X^3 + pX + q$, avec $p = 6$, $q = -2$, d'où le trinôme résolvant

$$r(X) = X^2 + qX - \tfrac{p^3}{27} = X^2 - 2X - \tfrac{6^3}{27} = (X-1)^2 - 3^2 ,$$

et ensuite $U = 4$, $V = -2$, $u = \sqrt[3]{4}$, $v = -\sqrt[3]{2}$, puis les racines de $b(X)$,

$$x_1 = \sqrt[3]{4} - \sqrt[3]{2} \quad , \quad x_2 = \sqrt[3]{4}\, j - \sqrt[3]{2}\ \bar{j} \quad , \quad x_3 = \sqrt[3]{4}\, \bar{j} - \sqrt[3]{2}\, j = \overline{x}_2 .$$

Chapitre 11

Anneaux principaux

11.1 Idéaux principaux, anneaux principaux

Soit A un anneau commutatif avec unité. L'idéal engendré par un élément a de A est l'ensemble $aA = \{ax\,;\ x \in A\}$ des multiples de a. Supposons A intègre. Les générateurs de l'idéal aA sont les éléments associés de a, de la forme au où $u \in A_*$. En effet,
- si $aA = \{0\}$, c'est vrai puisque 0 est le seul générateur.
-si $aA \neq \{0\}$, on a $a \neq 0$. Si I= $aA = bA$, il existe $u \in A$ tel que $b = au$ car $b \in I = aA$ et il existe $v \in A$ tel que $a = bv$ car $a \in I = bA$. On en déduit que $a = auv$ et ensuite que $1 = uv$; car A est intègre. Ainsi $u \in A_*$ et a et b sont associés.

Définitions.

Soit A un anneau commutatif avec unité.

Un idéal I de A est dit principal s'il existe $a \in A$ tel que $I = aA$.

L'anneau A est dit principal s'il est intègre et si tout idéal de A est principal.

Dans un anneau commutatif unifère A, les idéaux $\{0\} = 0A$ et A = 1A sont principaux. Un corps commutatif K est un anneau principal au sens de notre définition car $\{0\}$ et K sont ses seuls idéaux. On exclut parfois les corps commutatifs de la définition des anneaux principaux. Nous ne le ferons pas.

Proposition 1.

Soit A un anneau principal. Toute suite croissante $I_0 \subset I_1 \subset \cdots$ d idéaux de A est stationnaire : il existe $k \in \mathbb{N}$ à partir duquel la suite est constante.

Démonstration. Puisque (I_p) est totalement ordonnée, $\cup I_p$ est un idéal de A. Cet idéal est de la forme aA puisque l'anneau A est principal. Il existe donc $k \in \mathbb{N}$ tel que $a \in l_k$. On a $aA \subset I_k$ et donc $aA = I_k$ et $I_k = i_\ell$, pour tout $\ell \geqslant k$. ∎

Définition.

Soit A un anneau commutatif avec unité. On dit que A est noethérien si tout idéal de A est de type fini, c'est-à-dire engendré par un nombre fini d'éléments.

Proposition 2.

Un anneau principal est noethérien.

Exercice. Soit A un anneau avec unité. Montrer l'équivalence des propriétés,

(i) A est noethérien.
(ii) Toute suite croissante d'idéaux est stationnaire.
(iii) Toute famille non vide $\mathcal{F}$ d'idéaux, possède un élément, maximal dans$\mathcal{F}$.

Si A est noethérien, montrer que tout quotient A/I est noethérien.
Donner un exemple d'anneau qui ne soit pas noethérien.

Solution. (i)$\Rightarrow$ (ii) Raisonner comme dans la proposition.

(non (i)) $\Rightarrow$ (non (ii)) Supposons qu'il existe un idéal I de A qui ne soit pas de type fini. Soit $x_1 \in I$. On a donc $x_1A \neq I$. Il existe $x_2 \in I \setminus (x_1A)$. On a$x_1A + x_2A \neq I$. Il existe $x_3 \in I \setminus (x_1A + x_2A)$. En continuant ainsi, on construit par récurrence une suite strictement croissante d'idéaux dans I ce qui contredit (ii).

(non (iii)) $\Rightarrow$ (non (ii)) Supposons qu'il existe une famille non vide $\mathcal{F}$ d'idéaux de A sans élément maximal. Soit $I_1 \in \mathcal{F}$. Puisque I_1 n'est pas maximal dans $\mathcal{F}$, il existe $I_2 \in \mathcal{F}$ tel que $I_1 \subset I_2$ et $I_1 \neq I_2$. On peut continuer par récurrence et construire une suite strictement croissante d'idéaux de $\mathcal{F}$ ce qui contredit (ii).

(iii) $\Rightarrow$ (ii) Soit $I_1 \subset I_2 \subset \cdots$ une suite croissante d'idéaux de A. D'après (iii), il existe dans cette suite un élément I_k maximal. Alors pour tout $n \geqslant k$, on a $I_k \subset I_n$ et donc $I_k = I_n$ par maximalité de I_k.

, Soit J un idéal de A/I. Soit $\varphi : A \to A/I$ l'homomorphisme canonique. Si A est noethérien, il existe une famille finie $(x_1, \ldots, x_k)$ qui engendre l'idéal $\varphi^{-1}(J)$ de A. Alors $\varphi(x_1), \ldots, \varphi(x_k)$ engendrent $J = \varphi(\varphi^{-1}(J))$. Donc A/I est noethérien.

L'algèbre $A = \mathcal{F}(\mathbb{R})$ n'est pas un anneau noethérien car la suite infinie des idéaux $I_k = \{ f \in A \mid \forall x \in [k, +\infty[\ f(x) = 0 \}$ est strictement croissante.

11.2 Exemples classiques : les anneaux euclidiens

L'anneau $\mathbb{Z}$ est principal. En effet, il est intègre et nous avons vu en 1-13, que tout sous-groupe du groupe additif $(\mathbb{Z}, +)$ est un idéal de la forme $n\mathbb{Z}$. La démonstration repose sur la division euclidienne. Il en est de même pour l'anneau $K[X]$, où K est un corps commutatif. Formalisons cela. Un ensemble A est dit bien ordonné si toute partie non vide de A possède un plus petit élément. Par exemple, $\mathbb{N}$ est bien ordonné mais $\mathbb{R}$ ne l'est pas. Un ensemble bien ordonné est en particulier totalement ordonné.

Définition.

On appelle anneau euclidien, un anneau A commutatif, intègre, avec unité, possédant une division euclidienne, dans le sens suivant : il existe une application φ, appelée stathme euclidien, de A dans un ensemble bien ordonné $\in$, ayant la propriété que pour tout $a \in A$ et pour tout $b \in A$ non nul, il existe $q, r \in A$, tels que :

$$(1) \qquad a = bq + r \qquad \text{avec} \qquad \varphi(r) < \varphi(b)\,.$$

Puisque $\in$ est bien ordonné, l'ensemble des valeurs de φ possède un plus petit élément λ. Pour tout $b \neq 0$, on a $\lambda < \varphi(b)$ d'après (1), donc $\lambda = \varphi(0)$.

Proposition.

Tout anneau euclidien est principal. En particulier, $\mathbb{Z}$ et l'anneau $K[X]$ des polynômes à coefficients dans le corps commutatif K sont des anneaux principaux.

Démonstration. Si l'anneau A est euclidien, il est intègre. Vérifions que tout idéal I de A est principal. Si $I = \{0\}$, c'est vrai. Supposons $I \neq \{0\}$. Comme $\in$ est bien ordonné, il existe $b \in I \setminus \{0\}$ tel que $\varphi(b)$ soit la plus petite valeur de $\{\varphi(x)\,;\ x \in I \text{ et } x \neq 0\}$. On a $bA \subset I$. Par ailleurs, pour tout $a \in I$, la division euclidienne par b donne $q, r \in A$ tels que $a = bq + r$ et $\varphi(r) < \varphi(b)$. On a $r = a - bq \in I$. Le minimum de φ sur les éléments non nuls de I étant $\varphi(b)$, on obtient $r = 0$, $a = bq \in bA$ et donc $I = bA$.

La fonction $\varphi : n \mapsto |n|$ de $\mathbb{Z}$ dans l'ensemble bien ordonné $\mathbb{N}$, est un stathme. L'anneau intègre $\mathbb{Z}$ est donc euclidien. Pour tout $a \in \mathbb{Z}$, tout $b \in \mathbb{Z} \setminus \{0\}$, on a deux façons de définir la division de a par b, l'une $a = bq + r$ avec $0 \leqslant r < |b|$ correspond au choix du multiple bq de b le plus proche de a et inférieur à a, l'autre $a = bq + r$ avec $-|b| < r \leqslant 0$ correspond au choix du multiple bq de b le plus proche de a et supérieur à a. Pour a et b positifs, on choisit habituellement la première de ces deux divisions, pour avoir $r \in \mathbb{N}$. Tout idéal non nul $I = k\mathbb{Z}$ de $\mathbb{Z}$ a deux générateurs k et $-k$ car $\mathbb{Z}_* = \{1, -1\}$ et un seul générateur positif. Il existe donc pour tout idéal, un choix canonique de générateur. Sauf mention du contraire, c'est celui-là que l'on considère.

La fonction $\varphi : a \mapsto \mathrm{d}^\circ(a)$ de $K[X]$ dans l'ensemble bien ordonné $\{-\infty\} \cup \mathbb{N}$, est un stathme. L'anneau intègre $K[X]$ est euclidien. Tout idéal non nul pA a pour générateurs les polynômes ap, où $a \in K_*$ associés à p. Il existe donc un unique polynôme unitaire générateur de I. On a un choix canonique de générateur. ∎

Corollaire.

Soient A une algèbre avec unité sur le corps commutatif K et $\alpha \in A$. Pour tout polynôme $f(X) = a_n X^n + \cdots + a_0$ de $K[X]$, posons $f(\alpha) = a_n \alpha^n + \cdots + a_0 1 \in A$. Supposons qu'il existe $f \in K[X]$ non nul tel que $f(\alpha) = 0$. Il existe alors un polynôme unitaire de degré minimum tel que $f_\alpha(\alpha) = 0$ et f_α est unique. Tout polynôme $f \in K[X]$ tel que $f(\alpha) = 0$ est multiple de f_α.

Démonstration. L'application $\varphi : f \mapsto f(\alpha)$ est un homomorphisme d'algèbres de $K[X]$ sur la sous-algèbre $K(a) = \{f(\alpha)\,;\ f \in K[X]\}$ de A engendrée par 1 et a. Le noyau de φ est un idéal $J_\alpha = \{f \in K[X] \mid f(\alpha) = 0\}$ de l'anneau principal $K[X]$. Il admet donc un unique générateur unitaire f_α, et $J_\alpha = f_\alpha K[X]$. ∎

Définition.

Si $J_0 = \{f \in K[X] \mid f(\alpha) = 0\} \neq \{0\}$, le générateur unitaire f_α de J_α est appelé le polynôme minimal de α (polynôme unitaire de plus petit degré tel que $f_\alpha(\alpha) = 0$).

Exercice. On veut montrer qu'un sous-anneau d'un anneau principal n'est en général pas principal. On considère le sous-anneau $A = \mathbb{Z}[X]$ de l'anneau principal $\mathbb{Q}[X]$, les éléments $a(X) = 2$ et $b(X) = X$ de A et les idéaux principaux $a\mathbb{Z}[X]$ et $b\mathbb{Z}[X]$ de A. Montrer que l'idéal $I = a\mathbb{Z}[X] + b\mathbb{Z}[X]$ de A n'est pas principal.

Solution. Supposons qu'il existe $c \in \mathbb{Z}[X]$ tel que $I = c\mathbb{Z}[X]$. On aurait $a \in I = c\mathbb{Z}[X]$, $b \in c\mathbb{Z}[X]$. Ainsi c serait un diviseur commun de a et b, ce qui nécessite $c = 1$ ou $c = -1$. On aurait donc $1 \in a\mathbb{Z}[X] + b\mathbb{Z}[X]$ et il existerait donc des polynômes $u, v \in \mathbb{Z}[X]$ tels que $1 = au + bv$ soit $1 = 2(u_0 + u_1 X + \cdots + u_k X^k) + Xv(X)$. Cela implique notamment $1 = 2u_0$ avec $u_0 \in \mathbb{Z}$. C'est impossible.

11.3 Entiers d'un corps quadratique

Tout sous-corps K de $\mathbb{C}$ est de caractéristique nulle. Son sous-corps premier est $\mathbb{Q}$ et K est un espace vectoriel sur $\mathbb{Q}$. Les "plus petits" de ces sous-corps de $\mathbb{C}$, autres que $\mathbb{Q}$, sont ceux de dimension 2 sur $\mathbb{Q}$. Nous avons vu en 9-9, ex. 2, qu'ils sont deux à deux non isomorphes, de la forme $\mathbb{Q}(\delta)$ où $\delta \in \mathbb{C}$ est racine d'un polynôme $X^2 - d$ avec $d \in \mathbb{Z} \setminus \{0,1\}$ sans facteur carré autre que 1. De plus, d est unique, $(1,\delta)$ est une base sur $\mathbb{Q}$ de $\mathbb{Q}(\delta) = \{x + y\delta\,;\ x \in \mathbb{Q}, y \in \mathbb{Q}\}$ et les seuls automorphismes de $\mathbb{Q}(\delta)$ sont $\mathrm{Id}_{\mathbb{Q}(\delta)}$ et $\sigma : x + y\delta \mapsto x - y\delta$. Ce dernier laisse fixe tout élément de $\mathbb{Q}$.

Plongeons $\mathbb{Q}(\delta)$ dans $\mathcal{L}(\mathbb{Q}(\delta))$ en associant à tout $z = x + y\delta \in \mathbb{Q}(\delta)$ l'endomorphisme $f_z : z' \mapsto zz'$ du $\mathbb{Q}$-espace vectoriel $\mathbb{Q}(\delta)$. Si $z' = x' + y'\delta \in \mathbb{Q}(\delta)$ on a :
$(x + y\delta)(x' + y'\delta) = (xx' + dyy') + (yx' + xy')\delta$ d'où la matrice $M = \begin{pmatrix} x & dy \\ y & x \end{pmatrix}$ de f_z dans la base $(1,\delta)$. D'après le th. de Cayley-Hamilton, le polynôme caractéristique

$$P(X) = X^2 - \mathrm{tr}(M)X + \det(M) = X^2 - 2xX + x^2 - dy^2$$

est tel que $P(f_z) = 0$. D'après 11-2, cor., il est divisible par le polynôme minimal de f_z. D'après 8-2, lemme 2, si $z \notin \mathbb{Q}(\delta)$ il est irréductible. Il est donc égal au polynôme minimal de f_z. L'application $f : z \mapsto f_z$ de $\mathbb{Q}(\delta)$ dans $\mathcal{L}(\mathbb{Q}(\delta))$ est un homomorphisme d'algèbres injectif. C'est un isomorphisme de $\mathbb{Q}(\delta)$ sur $f(\mathbb{Q}(\delta))$ donc $P(X)$ est également le polynôme minimal de $z \in K \setminus \mathbb{Q}$ sur $\mathbb{Q}$.

Définitions.

Si $z = x + y\delta \in \mathbb{Q}(\delta)$, on note $\bar{z}$ l'élément $\sigma(z) = x - y\delta$. On l'appelle le conjugué de z. Si on a $d < 0$, alors $\bar{z}$ est le complexe conjugué usuel de $z \in \mathbb{C}$.

Le déterminant $z\bar{z} = x^2 - dy^2$ de f_z, noté $n(z)$, est appelée la norme de $z \in K$.

On dit que $z \in \mathbb{Q}(\delta)$ est un entier de $\mathbb{Q}(\delta)$, si $P(X) = X^2 - 2xX + x^2 - dy^2$ est à coefficients dans $\mathbb{Z}$, c'est-à-dire si

$$\mathrm{tr}(f_z) = 2x \in \mathbb{Z} \quad \textit{et} \quad n(z) = \det(f_z) = x^2 - dy^2 \in \mathbb{Z}\,.$$

Proposition.

Soit $d \in \mathbb{Z} \setminus \{0,1\}$ sans diviseur carré et soit δ une racine carrée de d dans $\mathbb{C}$. L'ensemble A_d des entiers de $\mathbb{Q}(\delta)$ est un sous-anneau de $\mathbb{Q}(\delta)$ qui engendre $\mathbb{Q}(\delta)$.

Si $d \equiv 2$ ou $d \equiv 3 \pmod 4$, on a $A_d = \mathbb{Z} + \mathbb{Z}\delta$.

Si $d \equiv 1 \pmod 4$, on a $A_d = \mathbb{Z} + \mathbb{Z}\theta$ où $\theta = \frac{1+\delta}{2}$.

Pour $d < 0$, la norme $n : z \mapsto z\bar{z}$ est un stathme euclidien sur A_d si et seulement si $d \in \{-1,-2,-3,-7,-11\}$. En particulier, l'anneau $A_{-1} = \mathbb{Z} + i\mathbb{Z}$ est euclidien.

Démonstration. Si $z = x + y\delta \in A_d$ on a $2x \in \mathbb{Z}$. Selon la parité de $2x$, on a deux possibilités : ou bien $x \in \mathbb{Z}$, ou bien $x = \frac{2p+1}{2}$ avec $p \in \mathbb{Z}$.

Supposons que $x \in \mathbb{Z}$. Alors $y \in \mathbb{Q}$ s'écrit $y = \frac{a}{b}$ avec $a \in \mathbb{Z}$, $b \in \mathbb{N}^*$, $a \wedge b = 1$. On a $da^2 = b^2(x^2 - n(z))$ avec $n(z) \in \mathbb{Z}$. Du fait que $a \wedge b = 1$, nécessairement $b^2 | d$. Comme d est sans carré, on a $b = 1$ et $y \in \mathbb{Z}$.

Supposons que $x = \frac{2p+1}{2}$ où $p \in \mathbb{Z}$. Alors $2z = 2x + 2y\delta \in A_d$, avec $2x \in \mathbb{Z}$. Nous venons de voir que $2y \in \mathbb{Z}$. On ne peut avoir $y \in \mathbb{Z}$, sinon $x^2 = dy^2 + n(z) \in \mathbb{Z}$. C'est exclu car $x^2 = p^2 + p + \frac{1}{4}$. On a donc $y = \frac{2q+1}{2}$ avec $q \in \mathbb{Z}$. On obtient

$$n(z) = x^2 - dy^2 = \left(\frac{2p+1}{2}\right)^2 - d\left(\frac{2q+1}{2}\right)^2 = p^2 + p - dq^2 - dq + \frac{1-d}{4}$$

Puisque $n(z) \in \mathbb{Z}$, nécessairement $d \equiv 1 \pmod 4$.
Pour $d \equiv 2$ ou $d \equiv 3 \pmod 4$., les éléments de A_d appartiennent donc à $\mathbb{Z} + \mathbb{Z}\delta$. Réciproquement tout élément de $\mathbb{Z} + \mathbb{Z}\delta$ appartient à A_d. Pour $d < 0$, les éléments de A_d sont alors les points d'un réseau de $\mathbb{C}$ à mailles rectangulaires.

Si $d \equiv 1 \pmod 4$ pour tout $x + y\delta \in A_d$ on a x et y dans $\mathbb{Z}$, ou $x = \frac{2p+1}{2}$ et $y = \frac{2q+1}{2}$ avec $p \in \mathbb{Z}$ et $q \in \mathbb{Z}$ et donc $x + y\delta \in \mathbb{Z} + \mathbb{Z}\theta$. Réciproquement, tout élément de $\mathbb{Z} + \mathbb{Z}\theta$ appartient à A_d. On a donc $A_d = \mathbb{Z} + \mathbb{Z}\theta$. C'est aussi l'ensemble $\mathbb{Z}\theta + \mathbb{Z}\sigma(\theta)$. Pour $d < 0$, c'est le réseau $\mathbb{Z}\theta + \mathbb{Z}\bar{\theta}$ de $\mathbb{C}$. Ses mailles sont des losanges.

Puisque δ et θ sont racines d'un polynôme de degré 2, le lecteur vérifiera que $\mathbb{Z} + \mathbb{Z}\delta$, et $\mathbb{Z} + \mathbb{Z}\theta$ lorsque $d \equiv 1 \pmod 4$, sont des sous-anneaux de $\mathbb{Q}(\delta)$ (voir 9-9, ex. 2).

Supposons $d < 0$. Supposons que $A_d = \mathbb{Z} + \delta\mathbb{Z} = \mathbb{Z} + i|\delta|\mathbb{Z}$. Alors n est un stathme si pour tout $b \in A_d$ non nul et pour tout $a \in A_d$, il existe $q \in A_d$ et $r \in A_d$ tels que $a = bq + r$ et $n(r) < n(b)$. Cela signifie encore que pour tout $\frac{a}{b} \in \mathbb{Q} + i|\delta|\mathbb{Q}$, il existe $q \in A_d$ et $\frac{r}{b} \in \mathbb{Q} + i|\delta|\mathbb{Q}$ tels que $|\frac{a}{b} - q| = |\frac{r}{b}| < 1$. Comme les éléments de $\mathbb{Q} + i|\delta|\mathbb{Q}$ sont partout denses dans $\mathbb{C}$ et comme les éléments de $A_d = \mathbb{Z} + \delta\mathbb{Z}$ sont les points d'un réseau à mailles rectangulaires, cela signifie que tout point du rectangle $[0,1] \times [0,|\delta|]$ de $\mathbb{R}^2$ est à une distance, de l'un des sommets, inférieure à 1. La plus grande distance à un sommet, obtenue au centre du rectangle, est $(\frac{1}{2})^2 + (\frac{|\delta|}{2})^2 = \frac{1+|d|}{4}$. Donc n est un stathme sur A_d si et seulement si $\frac{1+|d|}{4} < 1$, soit pour $d = -1$ ou $d = -2$. Pour $d = -1$ on obtient l'anneau $\mathbb{Z} + i\mathbb{Z}$ des entiers de Gauss qui est donc euclidien.

Dans le cas où $A - d = \mathbb{Z} + \mathbb{Z}\theta$, la même question est à étudier pour le losange de $\mathbb{R}^2$ construit sur $\overrightarrow{OA}$ et $\overrightarrow{OB}$ où A et B ont pour affixes $\theta = \frac{1}{2} + i\frac{|\delta|}{2}$ et $\bar{\theta}$, ou encore, pour des raisons de symétrie, pour le triangle isocèle OAI où I a pour afiixe 1. Il faut voir à quelle condition tout point du triangle est à une distance inférieure à 1 de l'un des sommets. Les cercles de centre O et I, de rayon 1, coupent la hauteur AH en K tel que $HK = \frac{\sqrt{3}}{2}$. La condition est donc $HA < \frac{\sqrt{3}}{2}$ ou $(HA > \frac{\sqrt{3}}{2}$ et $\frac{|\delta|}{2} - \frac{\sqrt{3}}{2} < 1)$ (voir sur une figure). Cela impose $|d| < 13$, d'où $d = -3, -7, -11$.

11.4 Divisibilité dans un anneau principal

Définitions.

Soient a, b deux éléments d'un anneau commutatif avec unité A. On dit que a divise b, ou que b est multiple de a, s'il existe $c \in A$ tel que $ac = b$. On note cela $a|b$.

On dit que $a \in A$ est irréductible (ou premier), si a est non nul, non inversible et si les seuls diviseurs de a sont 1, a et les associés de ces éléments.

Deux éléments a, b de A sont dits premiers entre eux, si les seuls diviseurs communs à a et b sont les éléments de A_* . Nous noterons cela $a \wedge b = 1$.

Des éléments $a_1, \ldots, a_k$ de A sont dits premiers dans leur ensemble si les éléments de A_* sont leurs seuls diviseurs communs.

La relation binaire de divisibilité se traduit par une inclusion d'idéaux :

$$a|b \quad \Leftrightarrow \quad b \in aA \quad \Leftrightarrow \quad bA \subset aA\,.$$

Par exemple, l'inclusion $aA \subset A = 1A$ traduit le fait que 1 divise a. De même, l'inclusion $\{0\} = 0A \subset aA$ traduit le fait que 0 est multiple de a.

La relation binaire $a|b$ soit $bA \subset aA$ est un préordre sur A. Ce n'est pas une relation d'ordre. L'étude de l'antisymétrie introduit la relation d'équivalence :

$$a|b \text{ et } b|a \quad \Leftrightarrow \quad bA \subset aA \text{ et } aA \subset bA \quad \Leftrightarrow \quad bA = aA.$$

Elle exprime que a et b sont générateurs d'un même idéal de A, c'est-à-dire associés. Les notions qui touchent à la divisibilité s'expriment modulo le fait d'être associé.

Soit p un élément irréductible de A. La condition $p \in EA_*$ signifie que $pA \neq A$. Le fait que alp nécessite $a = p$ ou $a = 1$ (modulo être associé), signifie que la condition $pA \subset aA$ implique $aA = pA$ ou $aA = A$. Ainsi, dans un anneau principal, un idéal pA est maximal si et seulement si son générateur p est irréductible.

Soit $a \in A$ avec $a \notin A_*$. On a alors $aA \neq A$. D'après 9-8, prop. il existe un idéal maximal pA contenant aA. Donc a admet au moins un diviseur irréductible p.

Deux éléments a et b de A ne sont pas premiers entre eux s'ils ont un diviseur commun $c \in A$.. Alors, l'idéal cA, distinct de A, contenant aA et bA, contient $aA + bA$. D'après 9-8, cA est contenu dans un idéal maximal, on peut donc dire que a et b ne sont pas premiers entre eux si et seulement s'ils ont un facteur irréductible commun.

Proposition.

Soit A un anneau principal et soient $a, b \in A$ non nuls.
(i) Un générateur m de l 'idéal $aA \cap bA$ est un plus petit multiple de a et b.
(ii) Un générateur d de l'idéal $aA + bA$ est un plus grand diviseur de a et b.

Démonstration. (i) $x \in A$ est un multiple commun de a et b si et seulement si $x \in aA \cap bA = mA$. En particulier, m est un multiple commun de a et b et tout multiple commun x de a et b est élément de $aA \cap bA = mA$ et donc multiple de m. Au sens de la relation de divisibilité (préordre), m est un plus petit multiple. Notons que tout autre générateur de l'idéal $aA \cap bB$ est associé à m. Le ppcm m de a et b est donc unique modulo la relation d'équivalence "être associés".

(ii) $x|a$ et $x|b \Leftrightarrow (aA \subset xA)$ et $(bA \subset xA) \Leftrightarrow dA = aA + bA \subset xA \Leftrightarrow x|d$.

On a $aA \subset dA$ et $bA \subset dA$ donc d est diviseur commun de a et b. Tout autre diviseur commun x est diviseur de d. En ce sens d est le plus grand diviseur commun. Les autres générateurs de l'idéal $aA + bA$ sont les associés de d. Le pgcd de a et b est unique modulo la relation "être associés". ∎

Remarques. Pour simplifier, nous nous sommes limités au cas de deux éléments a et b de A. Mais sans rien changer à la démonstration, si $a_1, \ldots, a_k \in A$ sont non nuls, on voit que leurs multiples communs sont les éléments de l'idéal $mA = \bigcap_{1 \leqslant i \leqslant k} a_i A$ et que leurs diviseurs communs sont les éléments de l'idéal $dA = a_1 A + \cdots + a_k A$. Les conclusions de la proposition sont encore valables.

Cette caractérisation du pgcd de a et b comme générateur de $aA + bA$ conduit à convenir que pgcd $(0, x) = x$ pour tout $x \in A$. En particulier, on a pgcd $(0, 0) = 0$.

La notation $a \wedge b$ du pgcd de a et b, a un sens clair dans $\mathbb{Z}$, ou $K[X]$, puisque parmi les divers générateurs de $aA + bA$ il existe un choix canonique (élément positif, ou polynôme unitaire). On peut exprimer que a et b sont premiers entre eux en écrivant $a \wedge b = 1$. Il est commode d'utiliser encore cette notation familière dans un anneau principal quelconque, bien que $a \wedge b$ soit ici une classe d'éléments associés.

Corollaire 1.

Soient $a_1, \ldots, a_k$, des éléments d'un anneau principal A. Un diviseur commun d de $a_1, \ldots, a_k$ est pgcd de $a_1, \ldots, a_k$, si et seulement s'il existe $u_1, \ldots, u_k \in A$ vérifiant :

$$d = a_1 u_1 + \cdots + a_k u_k \quad \textit{(relation de Bezout).}$$

Démonstration. Si d est pgcd, il est élément de $a_1A + \cdots + a_kA$ d'où l'existence de $u_1, \ldots, u_k$. Réciproquement, supposons que $d = a_1u_1 + \cdots + a_ku_k$. Soit d_0 un pgcd à $a_1, \ldots, a_k$. On a $d \in a_1A + \cdots + a_kA = d_0A$ et donc $d_0|d$. De plus, d est diviseur commun de $a_1, \ldots, a_k$ et donc diviseur de d_0 d'après la proposition. Finalement d et $d_0$sont associés et d est générateur de $a_1A + \cdots + a_kA$, c'est-à-dire un pgcd. ∎

Corollaire 2. (th. de Bezout)

Pour que des éléments $a_1, \ldots, a_k$, de 1'anneau principal A soient premiers dans leur ensemble, il faut et il suffit qu'i1 existe $u_1, \ldots, u_k \in A$ tels que

$$1 = a_1u_1 + \cdots + a_ku_k \,.$$

Démonstration. On applique le cor.1 avec $d = 1$ qui divise $a_1, \ldots, a_k$. ∎

Corollaire 3. (Lemme de Gauss)

Soit A un anneau principal et $a, b, c \in A$. Si $a|bc$ et si $a|b = 1$, alors $a|c$.

Démonstration. Il existe $q \in A$ tel que $bc = aq$ et $u, v \in A$ tels que $1 = ua + vb$. On en déduit $c = uac + vbc = a(uc + vq)$. ∎

Corollaire 4.

Soient A un anneau principal et $a, b, c \in A$. Si $a \wedge b = 1$ et $a \wedge c = 1$, alors $a \wedge bc = 1$. En particulier, si $a \wedge b = 1$, alors $a^m \wedge b^n = 1$ pour tous $m, n \in \mathbb{N}^*$.

Démonstration. Il existe $u, v \in A$ tels que $1 = ua + vb$ et $x, y \in A$ tels que $1 = xa + yc$. Le cor.2 s'applique car en multipliant membre à membre on obtient :

$$1 = (uxa + uyc + vxb)a + (vy)bc \,.$$ ∎

Remarques. Soient a_1, a_2 des éléments non nuls de $\mathbb{Z}$, ou de $K[X]$ (où K est un corps commutatif), ou plus généralement d'un anneau euclidien. L'algorithme d'Euclide permet de calculer un pgcd de a_1 et a_2 et d'obtenir une relation de Bezout.

Plaçons-nous par exemple dans $\mathbb{Z}$. Si a_1 ou a_2 est négatif, on le remplacera par son opposé. Si $a_1 = 0$ ou $a_2 = 0$ le pgcd est évident. Supposons donc $0 < a_2 \leqslant a_1$. Tout diviseur commun de a_1 et a_2 divise également le reste a_3 de la division euclidienne $a_1 = a_2q_2 + a_3$ et on a $0 \leqslant a_3 < a_2$. Réciproquement tout diviseur commun de a_2 et a_3 divise aussi a_1. Le couple $a_1 \geqslant a_2$ a donc les mêmes diviseurs que le couple $a_2 > a_3$. Si $a_3 \neq 0$, on effectue la division de a_2 par a_3, soit $a_2 = a_3q_3 + a_4$ et on remplace $a_2 > a_3$ par $a_3 > a_4$. On continue ainsi par récurrence. La suite $a_1 > a_2 > a_3 > \cdots$ de $\mathbb{N}$ aboutit nécessairement à zéro. L'algorithme s'arrête alors. Le dernier reste non nul a_k, est le pgcd. En éliminant $a_{k-1}, a_{k-2}, \ldots, a_3$ de la dernière égalité jusqu'à la première, on obtient une relation de Bezout $d = a_k = ua_1 + va_2$.

Quand on connaît une relation de Bezout $d = ua_1 + va_2$, où $d = \text{pgcd}(a_1, a_2)$, les autres relations de Bezout $d = u'a_1 + v'a$ s'en déduisent. Par différence, en posant $U = u' - u$, $V = v' - v$, on a $Ua_1 = -Va_2$. Comme $a_1 = db_1$, $a_2 = db_2$, avec $b_1 \wedge b_2 = 1$, on obtient $Ub_1 = -Vb_2$. Le lemme de Gauss montre que $b_1|V$, $b_2|U$. Finalement $U = kb_2$, $V = -kb_1$, avec k arbitraire, et $u' = u + kb_2$, $v' = v - kb_1$.

Exercice 1. Déterminer le pgcd de $a_1 = 2214$ et $a_2 = 522$ et une relation de Bezout reliant ces nombres.

Solution. Par divisions successives on obtient :

$$\begin{array}{lllllll} a_1 & = & a_2 \times 4 + a_3 & \text{où} & a_3 & = & 126 \quad (1) \\ a_2 & = & a_3 \times 4 + a_4 & \text{où} & a_4 & = & 18 \quad (2), \\ a_3 & = & a_4 \times 7. & & & & \end{array}$$

Le pgcd est $d = a_4 = 18$. D'après (2) on a $d = a_2 - 4a_3$. On utilise (1) pour éliminer a_3. Il vient $d = a_2 - 4(a_1 - 4a_2) = -4a_1 + 17a_2$.

Exercice 2. A quelle condition le polynôme $a(X) = X^3 + pX + q \in \mathbb{C}lX]$ a-t-il une racine multiple dans $\mathbb{C}$?

Solution. D'après 10-5, cor.1, $\lambda \in \mathbb{C}$ est racine multiple de $a(X)$, si et seulement si λ annule $a(X)$ et $a'(X) = 3X^2 + p$, c'est-à-dire si $X - \lambda$ est un facteur commun pour $a(X)$ et $a'(X)$. Comme $\mathbb{C}$ est algébriquement clos, pour cela il faut et il sufiit que $d^\circ(\text{pgcd}(a, a')) > 1$. Appliquons l'algorithme d'Euclide.

$$\begin{aligned} X^3 + pX + q &= (3X^2 + p)(\frac{1}{3}X) + \frac{2p}{3}X + q \\ 3x^2 + p &= \left(\frac{2p}{3}X + q\right)\left(\frac{9}{2p}X - \frac{27q}{4p^2}\right) + \frac{27q^2}{4p^2} + p \end{aligned}$$

Ces divisions sont valables si $p \neq 0$. Si $p \neq 0$, pour que $a(X)$ et $a'(X)$ ne soient pas premiers entre eux, il faut et il suffit que $4p^3 + 27q^2 = 0$. Si $p = 0$, alors $X^3 + q$ a une racine multiple si et seulement si $q = 0$. Ainsi, la condition $4p^3 + 27q^2 = 0$ caractérise l'existence d'une racine multiple de $a(X) \in \mathbb{C}[X]$ dans tous les cas.

11.5 Décomposition en facteurs irréductibles

Proposition.

Soit A un anneau principal. Tout élément non nul a de A qui n'est pas une unité a une décomposition, $a = p_1 \cdots p_k$, comme produit d'éléments irréductibles. Modulo l'équivalence "être associés", les éléments $p_1, \ldots, p_k$, sont uniques.

Démonstration. *Existence.* Montrons d'abord que a possède un diviseur irréductible (sans utiliser le th. de Zorn comme en 11-4). Si a est irréductible, c'est vrai. Sinon, il existe $a_1, b_1 \in A$ avec $a_1 \notin A_*$ et $b_1 \notin A_*$ tels que $a = a_1 b_1$.

Si a_1 est irréductible, l'assertion est vérifiée. Sinon, il existe $a_2 \notin A_*$, et $b_2 \notin A_*$. tels que $a_1 = a_2 b_2$. Si a_2 est irréductible, l'assertion est vérifiée. Sinon... On poursuit le raisonnement, par récurrence. Si le processus se déroulait indéfiniment, on obtiendrait une suite infinie $a_1, a_2, \ldots$ où chaque terme est multiple du suivant et non associé à ce suivant. On aurait alors une suite infinie d'idéaux $a_1 A \subset a_2 A \subset a_3 A \subset \cdots$, strictement croissante. C'est impossible d'après 11-1. La suite $a_1, a_2, \ldots$ est donc finie. Le dernier terme a_k est alors irréductible. C'est un diviseur irréductible de a.

On a donc $a = p_1 a_1$ avec p_1 irréductible. Si $a_1 \in A_*$, alors $p_1 a_1$ est irréductible. Si $a_1 \notin A_*$, de même $a_1 = p_2 a_2$ avec p_2 irréductible. On continue ainsi par récurrence. Ce processus s'arrête en un nombre fini d'étapes, sinon on arrive à nouveau à une suite infinie strictement croissante aA , $a_1 A$, $a_2 A, \ldots$ d'idéaux de A. Donc $a = p_1 p_2 \cdots p_k u$, où $p_1, \ldots, p_k$, sont irréductibles et $u \in A_*$. Alors $p_k u$ est irréductible d'où le résultat.

Montrons l'unicité par récurrence sur le nombre minimum k de facteurs irréductibles dans les diverses décompositions $a = p_1 \cdots p_k$ de a en produit d'éléments irréductibles.

Si $k = 1$, on a $a = p_1$. Considérons une autre expression $a = q_1 \cdots q_m$ où $q_1, \ldots, q_m$ sont irréductibles. Supposons $m > 1$. Alors q_1 divise p_1. Il existe $u \in A_*$ tel que $p_1 = uq_1$. En simplifiant la relation $p_1 = up_1q_2 \cdots q_k$ par p_1, ce qui est possible car A est intègre, on obtiendrait que $1 = uq_2 \cdots q_m$ et q_2 serait inversible. C'est absurde. Donc $m = 1$ et $p_1 = a = q_1$.

Supposons $k \geqslant 2$. Admettons l'unicité pour les éléments de A qui sont produit d'au plus $k-1$ facteurs irréductibles. Considérons un élément $a = p_1 \cdots p_k$ produit de k facteurs irréductibles. Soit $a = q_1 \cdots q_m$ une autre expression de a. D'après 11-4, cor.4, si p_1 était premier avec $q_1, \ldots, q_m$, il serait premier avec leur produit et donc avec a. C'est absurde donc p_1 divise l'un des q_i. Quitte à permuter les q_i, on peut supposer que p_1 divise q_1. Comme q_1 est irréductible, on a $q_1 = up_1$ avec $u \in A_*$. Puisque A est intègre, on peut simplifier par p_1 la relation $a = p_1p_2 \cdots p_k = up_1q_2 \cdots q_m$. On obtient $p_2 \cdots p_k = uq_2 \cdots q_m$. D'après l'hypothèse de récurrence, $k-1 = m-1$ donc $k = m$ et il existe une permutation s de $\{2, \ldots, k\}$ telle que p_i soit associé à q_{s_i} pour $i = 2, \ldots, k$, d'où la conclusion. ∎

Remarque. Dans un anneau principal A, on n'a pas toujours, comme dans $\mathbb{Z}$ ou $K[X]$, un choix canonique de représentant dans chaque classe d'éléments irréductibles associés de A. Il sera commode de faire un tel choix. La décomposition en facteurs irréductibles de $a \in A$, donnée par la proposition, se fera alors de manière unique sous la forme $a = up_1 \cdots p_k$ où $u \in A_*$ et où $p_1, \ldots, p_k$ appartiennent à la famille $\mathcal{P}$ choisie. Pour tout idéal I de A, on pourra parler "du générateur" de I, élément de $\mathcal{P}$.

Définition.

Nous appellerons système d'irréductibles dans l'anneau principal A une famille $\mathcal{P}$ d'éléments irréductibles de A telle que tout irréductible de A soit associé à un élément de $\mathcal{P}$ et un seul. Nous supposons fait un tel choix dans les corollaires suivants.

Corollaire 1.

Soit $a = up_1^{\alpha_1} \cdots p_k^{\alpha_k}$ un élément non nul de A, avec $u \in A_*$, $p_1, \ldots, p_k \in \mathcal{P}$ distincts et $\alpha_1, \ldots, \alpha_k \in \mathbb{N}^*$. Les diviseurs de a sont les éléments de la forme $b = vp_1^{\beta_1} \cdots p_k^{\beta_k}$ où $v \in A_*$ et où $\beta_1, \ldots, \beta_k \in \mathbb{N}$ vérifient, $\beta_i \leqslant \alpha_i$ pour $i = 1, \ldots, k$.

Démonstration. Si b divise a, il existe $c \in A$ tel que $a = bc$. Soit $b = vp_1^{\beta_1} \cdots p_k^{\beta_k}$ et $c = wp_1^{\gamma_1} \cdots p_k^{\gamma_k}$ les décompositions irréductibles de b et c, avec $0 \leqslant \beta_i$, $0 \leqslant \gamma_i$ pour $i = 1, \ldots, k$ et où $p_1, \ldots, p_k \in \mathcal{P}$ est la liste de tous les facteurs irréductibles des expressions de b et de c. Le produit $vwp_1^{\beta_1+\gamma_1} \cdots p_k^{\beta_k+\gamma_k}$ doit donner l'unique décomposition irréductible de $bc = a$, d'où le résultat. ∎

Corollaire 2.

Soient $a = up_1^{\alpha_1} \cdots p_k^{\alpha_k}$ et $b = vp_1^{\beta_1} \cdots p_k^{\beta_k}$ deux éléments non nuls de A, décomposés comme produits de facteurs irréductibles de $\mathcal{P}$, où interviennent tous les facteurs irréductibles de a et de b, avec des exposants $\alpha_i \geqslant 0$, $\beta_i \geqslant 0$ et où $u, v \in A_*$. Pour $i = 1, \ldots, k$ posons $\gamma_i = \min(\alpha_i, \beta_i)$, $\eta_i = \max(\alpha_i, \beta_i)$ Alors $d = p_1^{\gamma_1} \cdots p_k^{\gamma_k}$ est pgcd de a et b et $m = p_1^{\eta_1} \cdots p_k^{\eta_k}$ est ppcm de a et b. Il existe $w \in A_*$ tel que $ab = wdm$. En particulier, $a \wedge b = 1$ si et seulement si ab est ppcm de a et b.

Démonstration. Cela résulte immédiatement du corollaire précédent. La relation $ab = wdm$ est due au fait que $\max(\alpha_i, \beta_i) + \min(a_i, \beta_i) = \alpha_i + \beta_i$. ∎

Exercice 1. Sur les idéaux d'un anneau principal A, montrer que les opérations $(I,J) \mapsto I \cap J$ et $(I,J) \mapsto I+J$ sont associatives et que chacune distribue l'autre.

Solution. Il est classique et facile à vérifier que dans $\mathbb{N}$, les opérations $(\alpha,\beta) \mapsto \max(\alpha,\beta)$ et $(\alpha,\beta) \mapsto \min(\alpha,,\beta)$ sont associatives et que chacune distribue l'autre. Le résultat découle donc de 11-4, prop. et 11-5 cor.2. Notons que $\{0\}$ et A sont un plus petit élément et un plus grand élément de l'ensemble des idéaux de A.

Exercice 2. Déterminer les éléments irréductibles des anneaux $\mathbb{C}[X]$ et $\mathbb{R}[X]$.

Solution. Comme $\mathbb{C}$ est algébriquement clos, tout polynôme non constant est produit de facteurs de degré un. Un tel polynôme n'est irréductible que s'il est de degré un. L'ensemble $\mathcal{P}$ des polynômes unitaires de degré un, de la forme $X+a$, est un système d'irréductibles de l'anneau $\mathbb{C}[X]$.
Soit $p \in \mathbb{R}[X]$ de degré $n \geqslant 1$. Ses racines dans $\mathbb{C}$ sont réelles, ou complexes non réelles deux à deux conjuguées. En regroupant les termes conjugués on obtient les polynômes $(X-\alpha-i\beta)(X-\alpha+i\beta) = (X-\alpha^2)^2+\beta^2$ de degré 2 irréductible de $\mathbb{R}[X]$. Les polynômes irréductibles de $\mathbb{R}[X]$ sont donc les polynômes de degré un et les polynômes de degré deux, à discriminant strictement négatif.

11.6 Anneau des entiers de Gauss

Lemme.

Soit $d \in \mathbb{Z} \setminus \{0,1\}$ sans facteur carré et $\delta \in \mathbb{C}$ une racine carrée de d. Pour que $u = x+y\delta \in A_d$ soit une unité de l'anneau A_d des entiers de $\mathbb{Q}(\delta)$, il faut et il suffit que $n(u) = \varepsilon$, où $\varepsilon = \pm 1$. L'inverse de u est alors $u^{-1} = \varepsilon(x-y\delta)$.
Le groupe des unités de l'anneau $\mathbb{Z}+i\mathbb{Z}$ est $\{1,i,-1,-i\}$.

Démonstration. Si $n(u) = u\overline{u} = \varepsilon$, où $\varepsilon = \pm 1$, alors $\varepsilon\overline{u}$ est un inverse pour u. Réciproquement, si $u \in A_d$ est inversible d'inverse v, on a $1 = uv$ et donc $1 = n(u)n(v)$, avec $n(u) \in \mathbb{Z}$ et $n(v) \in \mathbb{Z}$. On en déduit que $n(u) = \pm 1$ car $\mathbb{Z}_* = \{1,-1\}$.

Prenons $d = -1$. Alors $u = x+iy$ vérifie $1 = n(u) = x^2+y^2$ si et seulement si x ou y est nul, l'autre terme valant ± 1, d'où le groupe des unités $\{1,i,-1,-i\}$. ∎

Proposition.

Soient d et δ comme dans le lemme. On suppose que l'anneau A_d est principal. Pour tout nombre premier $p > 2$, les conditions suivantes sont équivalentes.

(i) *p n'est pas irréductible dans l'anneau A_d.*

(ii) *Il existe $z = x+y\delta \in A_d$ tel que $p = \pm n(z) = z(\pm\overline{z})$, où $\overline{z} = x-y\delta$*

(iii) *Dans le corps $\mathbb{Z}/p\mathbb{Z}$, la classe $\hat{d}$ de d est un carré.*

Si (ii) est vérifiée, alors $p = z(\pm\overline{z})$ est la décomposition de p en facteurs irréductibles dans A_d (unique modulo les unités de A_d).

Démonstration. (i)⇒(ii) Si $p = zz'$, avec z, z'qui ne sont pas des unités de A_d, on a $p^2 = n(p) = n(z)n(z')$, où $n(z) \neq \pm 1$ et $n(z') \neq \pm 1$ sont des entiers. Il est exclu que $p_2 | n(z)$ car on en déduirait $1 = kn(z')$ et donc $n(z') = \pm 1$. De même, p_2 ne divise pas $n(z')$. Donc $p|n(z)$ et $p|n(z')$ et de ce fait $n(z) = \pm p$ et $n(z') = \pm p$.

(ii) $\Rightarrow$ (iii) Supposons qu'il existe $z = x + y\delta \in A_d$ tel que $p = \pm n(z) = \pm (x^2 - dy^2)$. D'après 11-3, $X = 2x \in \mathbb{Z}, Y = 2y \in \mathbb{Z}$ et $4p = \pm (X^2 - dY^2)$. Dans $\mathbb{Z}/p\mathbb{Z}$ on obtient $\hat{0} = \hat{X}^2 - d\hat{Y}^2$. On a $\hat{Y} \neq \hat{0}$, sinon p diviserait y et diviserait x puisque $p = x^2 - dy^2$ et après simplification on aurait $1 = p(x^2 - dy^2)$ ce qui est absurde. Donc $\hat{d} = [(\hat{X})(\hat{Y})^{-1}]^2$ est un carré dans $\mathbb{Z}/p\mathbb{Z}$.

$(iii) \Rightarrow (i)$ Supposons que $\hat{d} = \hat{a}^2$ dans $\mathbb{Z}/p\mathbb{Z}$. Alors p divise $a^2 - d$ dans $\mathbb{Z}$. Dans l'anneau principal A_d, si p était irréductible, étant diviseur de $a^2 - d = (a - \delta)(a + \delta)$, il diviserait $a - \delta$, ou $a + \delta$. Alors, $p = \overline{p}$ diviserait le conjugué $a - \delta$ de $a + \delta$, ou le conjugué $a + \delta$ de $a - \delta$. Ainsi, p diviserait $(a + \delta) - (a - \delta) = 2\delta$ et p^2 diviserait $4d$ dans A_d. On a $p > 2$ donc p^2 diviserait d. C'est impossible car d est sans facteur carré. Donc p n'est pas irréductible.

Soit ζ un facteur irréductible de p. On a $p = z(\pm\overline{z})$ dans A_d. D'après le lemme de Gauss, ζ doit diviser z ou $\overline{z}$. Supposons par exemple qu'il existe $\alpha \in A_d$ tel que $z = \zeta\alpha$. On en déduit $p = z(\pm\overline{z}) = \pm(\zeta\overline{\zeta})(\alpha\overline{\alpha})$. On a alors $\zeta\overline{\zeta} \in \mathbb{Z}$ et $\zeta\overline{\zeta} \neq 1$ car ζ n'est pas une unité. Donc $\zeta\overline{\zeta} = \pm p$ et $\alpha\overline{\alpha} = \pm 1$. Ainsi α est une unité et z associé de ζ est irréductible. Il en est de même pour $\overline{z}$. ∎

Corollaire 1.

Dans l'anneau euclidien $A = \mathbb{Z} + i\mathbb{Z}$ des entiers de Gauss, les éléments irréductibles sont les nombres premiers $p \in \mathbb{N}$ congrus à $3 \pmod 4$ et leurs associés et les éléments $z = a + ib$ tels que $n(z)$ soit un nombre premier égal à 2 ou congru à $1 \pmod 4$, ou de manière équivalente somme de deux carrés dans $\mathbb{N}$.

Démonstration. On a $2 = (1 + i)(1 - i)$ - avec $n(1 + i) = 2 \neq \pm 1$ donc 2 n'est pas irréductible. Soit $p > 2$ un nombre premier. D'après la proposition, p n'est pas irréductible dans A si et seulement si -1 est un carré dans $\mathbb{Z}/p\mathbb{Z}$. On a vu en 10-7, ex.1 (et nous reverrons en 12-3), que -1 est un carré dans $\mathbb{Z}/p\mathbb{Z}$ si et seulement si $p \equiv 1 \pmod 4$. Ainsi p est irréductible dans A si et seulement si p est congru à $3 \pmod 4$ (si $p > 2$ est congru à 0 ou 2 il est pair et n'est pas premier).

Soit $p > 2$, premier, qui ne soit pas irréductible dans A ($p = 2$ ou $p \equiv 1 \pmod 4$). D'après la proposition (ii), il existe $a + ib \in A$ irréductible tel que $p = (a + ib)(a - ib) = a^2 + b^2$. Et on a $a \neq 0$ et $b \neq 0$ sinon p ne serait pas premier.

Réciproquement, considérons $z = a + ib \in A$ irréductible avec $a \neq 0$ et $b \neq 0$. Montrons que $n(z) = a^2 + b^2$ est un nombre premier. Si $a = \pm 1$ et $b = \pm 1$, c'est vrai. Sinon, soit $n(z) = p_1 \dots p_k$ la décomposition en facteurs premiers de $n(z)$ dans $\mathbb{N}$. D'après le lemme de Gauss, z (irréductible dans A) divise l'un de ces facteurs, par exemple p_1 et $\overline{z}$ également, avec $\overline{z}$ non associé de z (voir ex. 3). Alors p_1 multiple de $z\overline{z}$ est égal à $z\overline{z}$. Ainsi $n(z) = p_1$ est premier. ∎

Corollaire 2.

Un nombre premier $p \in \mathbb{N}$ est somme de deux carrés, si et seulement si $p = 2$ ou si $p \equiv 1 \pmod 4$. La décomposition $p = a^2 + b^2$ est alors unique.

Démonstration. La première assertion est établie dans le cor.1. Montrons l'unicité de l'expression $p = a^2 + b^2$. D'après la proposition, $a + ib$ et $a - ib$ sont irréductibles. Soit $p = a'^2 + b'^2 = (a' + ib')(a' - ib')$ une autre expression. Alors $a + ib$ irréductible divise $a' + ib'$ ou $a' - ib'$. Si par exemple $a' + ib' = (a + ib)u$ on a
$p^2 = n(a' + ib') = n(a + ib)n(u) = p^2 n(u)$ donc $n(u) = 1$ et donc $u \in \{1, i, -1, -i\}$. Alors (a'^2, b'^2) est l'un des couples (a^2, b^2) ou (b^2, a^2). ∎

Corollaire 3.

Un entier $n \in \mathbb{N}$ est somme de deux carrés si et seulement s'il existe $z \in \mathbb{Z}+i\mathbb{Z}$ tel que $n = n(z)$ et pour cela il faut et il suffit que les facteurs premiers de n congrus à $3 \pmod 4$ figurent dans n avec un exposant pair.

Démonstration. Soit $n = p_1^{k_1}\cdots p_s^{k_s} q_1^{m_1}\cdots q_s^{m_s}$ la décomposition en facteurs premiers de n dans $\mathbb{N}$, où l'on a écrit d'abord les facteurs premiers p_i qui sont congrus à $3 \pmod 4$ et ensuite les facteurs premiers q_j égaux à 2 ou congrus à $1 \pmod 4$. Pour $1 \leqslant j \leqslant t$ il existe $(\alpha_j + i\beta_j)$ irréductible dans A, tel que $q_j = (\alpha_j + i\beta_j)(\alpha_j - i\beta_j)$. Si $k_1 = 2\ell_1, \ldots, k_s = 2\ell_s$, sont pairs, alors $\zeta = p_1^{\ell_1}\cdots p_s^{\ell_s}(\alpha_1 + i\beta_1)^{m_1}\cdots(\alpha_t + i\beta_t)^{m_t}$ est tel que $n = \zeta\overline{\zeta}$. Donc n est somme de deux carrés. Réciproquement, si $n = a^2 + b^2 = (a+ib)(a-ib)$, la décomposition en irréductibles dans $\mathbb{Z}+i\mathbb{Z}$ de $\zeta = a + ib$ conduit à une expression $\zeta = p_1^{\ell_1}\cdots p_s^{\ell_s}(\alpha_1 + i\beta_1)^{m_1}\cdots(\alpha_t + i\beta_t)^{m_t}$ donnant $n = \zeta\overline{\zeta} = p_1^{2\ell_1}\cdots p_s^{2\ell_s}(\alpha_1^2+\beta_1^2)^{m_1}\cdots(\alpha_t^2+\beta_t^2)^{m_t}$ où les facteurs premiers congrus à $3 \pmod 4$ ont des exposants pairs. ∎

Exercice 1. Dans l'anneau $A = \mathbb{Z}+i\mathbb{Z}$ déterminer la décomposition en facteurs irréductibles de $z = 69 + 45i$ et le pgcd de z et $\zeta = 12 + 18i$.

Solution. Puisque 3 divise 69 et 45, on a $z = 3z_1$, où $z_1 = 23 + 15i$. On a $3 \equiv 3 \pmod 4$ donc 3 est un irréductible de A. On a $n(z_1) = z_1\overline{z_1} = 23^2 + 15^2 = 754 = 2\times 377 = 2\times 13\times 29$. Puisque $2 = (1+i)(1-i)$ est premier, $1+i$ ou $1-i$ est facteur irréductible de z_1. Comme $1 - i = -i(1+i)$ est un associé de $1+i$, nécessairement $1+i$ divise z_1. On obtient $z = 3(1+2i)z_2$, avec $z_2 = \frac{23+15i}{1+i} = \frac{(23+15i)(1-i)}{2}$ et $n(z_2) = 13\times 29$. Puisque $13 = 2^2 + 3^2 = (2+3i)(2-3i)$, où $2+3i$ et $2-3i$ sont irréductibles puisque 13 est premier, l'un de ces termes divise z_2. On a $\frac{19-4i}{2+3i} = 2 - 5i$, d'où la décomposition en facteurs irréductibles $z = 3(1+i)(2+3i)(2-5i)$. Ces facteurs irréductibles sont uniques modulo le fait d'être associés, c'est-à-dire modulo un facteur multiplicatif égal à 1, i, -1 ou $-i$.

$\zeta = 3(4+6i) = 3\times 2(2+3i) = -i[3(1+i)^2(2+3i)]$, où $-i$ est une unité et où les autres termes sont irréductibles. Donc $3(1+i)(2+3i)$ est pgcd de z et ζ.

Exercice 2. Décomposer comme somme de deux carrés $N = 260$.

Solution. $N = 4x5x13 = 2^2(2^2+1^2)(3^2+2^2) = 2^2[(2+i)(2-i)][(3+2i)(3-2i)] = 2^2[4+7i][4-7i] = 2^2(4^2+7^2) = 8^2 + 14^2$.

Cette décomposition n'est pas unique car on a aussi

$N = 2^2[(2+i)(2+3i][(2-i)(2-3i)] = 2^2(1+8i)(1-8i) = 2^2(1^2+8^2) = 2^2 + 16^2$.

Exercice 3 Si $z = a + ib$ est irréductible dans $A = \mathbb{Z}+i\mathbb{Z}$, avec $b \neq 0$, peut-on avoir z et$\overline{z}$ associés ?

Solution. D'après le cor.2, $p = a^2 + b^2$ est premier dans $\mathbb{N}$. S'il existe $u \in A_*$ tel que $a + ib = u(a - ib)$, on ne peut avoir $u = 1$ (sinon $b = 0$ et $p = a^2$), ni $u = -1$ (sinon $a = 0$ et $p = b^2$). Si $u = i$ ou $u = -i$, on a $a = b$ ou $a = -b$ et donc $p = 2a^2$. Comme p est premier on a $p = 2$. Réciproquement, $p = 2$ s'écrit $p = (1+i)(1-i)$, avec $1+i$ et $1-i$ associés car $1 + i = i(l - i)$. Ainsi, seul $1+i$ et ses associés conviennent.

11.7 Théorème chinois

Proposition.

Soient A un anneau commutatif unifère, I et J des idéaux de A tels que $I+J=A$. L'application associant à la classe $\widehat{x}$ de $x\in A$ modulo $I\cap J$ le couple $(\overline{x},\overset{\circ}{x})$ des classes de x modulo I et modulo J, est un isomorphisme de l'anneau $A/(I\cap J)$ sur l'anneau $(A/I)\times(A/J)$.

Démonstration. Si $I+J=A$ on a $I\cap J=IJ$ (9-6, ex.). On vérifie facilement que $f:x\mapsto(\overline{x},\overset{\circ}{x})$ est un homomorphisme de A dans $(A/I)x(A/J)$. On a :

$$x\in\mathrm{Ker}\,(f)\quad\Leftrightarrow\quad\overline{x}=\overline{0}\ \text{et}\ \overset{\circ}{x}=\overset{\circ}{0}\quad\Leftrightarrow\quad x\in I\ \text{et}\ x\in J\quad\Leftrightarrow\quad x\in I\cap J\,.$$

Cela prouve que $\mathrm{Ker}\,(f)=I\cap J$. Par factorisation de f on obtient un homomorphisme injectif $\overline{f}:A/(I\cap J)\to(A/I)\times(A/J)$ tel que $\overline{f}(\widehat{x})=(\overline{x},\overset{\circ}{x})$ pour tout $x\in A$. Puisque $I+J=A$, il existe $u\in I$ et $v\in J$ tels que $1=u+v$. Considérons $\overline{a}\in A/I$ et $\overset{\circ}{b}\in A/J$, où $a,b\in A$. Posons $x=va+ub$. On a $\overline{v}=\overline{1}$ et $\overline{x}=\overline{va}=\overline{a}$ et de même $\overset{\circ}{u}=\overset{\circ}{1}$ et $\overset{\circ}{x}=\overset{\circ}{u}\,\overset{\circ}{b}=\overset{\circ}{b}$. Donc $\overline{f}$ est surjective. C'est un isomorphisme. ∎

Corollaire.

Soient Aun anneau principal, $m\in A$ et $n\in A$ premiers entre eux. Considérons $u\in A$, $v\in A$ tels que $1=um+vn$. L'application $\widehat{k}\mapsto(\overline{k},\overset{\circ}{k})$ est un isomorphisme de l'anneau A/mnA sur l'anneau $(A/mA)\times(A/nA)$. L'isomorphisme réciproque associe à $(\overline{a},\overset{\circ}{b})\in(A/mA)\times(A/nA)$ la classe $\widehat{x}\in A/mnA$ de $x=vna+umb$.

Démonstration. On applique la proposition avec $I=mA$, $J=nA$. La condition $I+J=A$ signifie que $m\wedge n=1$ (11-4, cor.2). Dans ce cas, $\mathrm{ppcm}(m,n)$, générateur de $I\cap J$, est égal à mn. ∎

Remarque. . Si $m\wedge n=1$, le corollaire montre que $\begin{cases}k&\equiv&a&(\mathrm{mod}\,mA)\\k&\equiv&b&(\mathrm{mod}\,nA)\end{cases}$ a une solution unique modulo mnA. Si l'anneau A est euclidien, on peut déterminer une relation de Bezout par l'algorithme d'Euclide et obtenir une solution x. Les autres solutions s'obtiennent en ajoutant à x un multiple de mn.

Ces résultats, se généralisent au cas de p équations $k\equiv ai\,(\mathrm{mod}\,m_iA)$, où $m_1,\dots,m_p$ sont deux à deux premiers entre eux. En posant $M_k=\prod_{i\neq k}m_i$ on obtient des éléments premiers dans leur ensemble. Si on détermine une relation de Bezout, soit $1=M_1u_1+\cdots+M_pu_p$, alors $x=M_1u_1a_1+\cdots+M_pu_pa_p$ sera une solution particulière. Les autres s'en déduisent en ajoutant un multiple de $m_1\cdots m_p$.

Exercice 1. Résoudre $x\equiv 2\,(\mathrm{mod}\,4)c\quad,\quad x\equiv\,(\mathrm{mod}\,5)\quad,\quad x\equiv 1\,(\mathrm{mod}\,9)$.

Solution. Le th. chinois s'applique car 4, 5, 9 sont deux à deux premiers entre eux. Posons $M_1=5\times9=45$, $M_2=4\times9=36$, $M_3=4\times5=20$. Déterminons u_1 , u_2 , u_3 tels que $\sum_{i=1}^{3}u_iM_i=1$. On a $\mathrm{pgcd}(M_2,M_3)=4$ et la relation de Bezout $4=(-1)\times36+2\times20$. On a $M_1\wedge4=1$ et la relation de Bezout $1=45-11\times4$, d'où $1=45-11[(-1)x36+2x20]=45+11x36-22x20$. On en déduit une solution $x_0=2\times45+3\times11\times36-22\times20=838$. Les autres solutions sont :
$x=838+k\,4\times5\times9=838+k\,180$ où $k\in\mathbb{Z}$ soit $x=118+k'\,180$ où $k'\in\mathbb{Z}$.

Exercice 2. Soit K un corps commutatif. On connaît les restes $r_1(X)$ et $r_2(X)$ de la division d'un polynôme unitaire $p(X)$, de degré quatre, par $a(X) = X^2 - 1$ et par $b(X) = X^2 - 2$. Montrer que le polynôme $p(X)$ est parfaitement déterminé.

Solution. On a la relation de Bezout $a(X) - b(X) = 1$ donc $a(X)$ et $b(X)$ sont premiers entre eux. On peut utiliser le th. chinois. Le système

$$a \equiv r_1 \ (\bmod\,(X^2-1)\,) \qquad , \qquad b \equiv r_2 \ (\bmod\,(X^2-2)\,)$$

admet pour solution particulière

$$p_0(X) = a(X)r_2(X) - b(X)r_1(X) = (X^2-1)r_2(X) - (X^2-2)r_1(X\,.$$

Les autres solutions sont les éléments de la classe de $p_0(X)$ modulo l'idéal engendré par $a(X)b(X)$, de la forme :

$$P(X) = (X^2-1)r_2(X) - (X^2-2)r_1(X) + k(X)a(X)b(X)\,.$$

On a $\mathrm{d}^\circ(r_1) < \mathrm{d}^\circ(a) = 2$, $\mathrm{d}^\circ(r_2) < \mathrm{d}^\circ(b) = 2$ d'où $\mathrm{d}^\circ(p_0) \leqslant 3$. Pour que p soit unitaire et $\mathrm{d}^\circ(p) = 4$, il faut et il suffit que $k(X) = 1$. On a donc $p = ar_2 - br_1 + ab$.

11.8 Quotients dans les anneaux principaux

Lemme.

Considérons un élément a, non nul, non inversible, de l'anneau principal A. Soit $b \in A$. Pour que $\overline{b} \in A/aA$ soit une unité de l'anneau A/aA, il faut et il suffit que $a \wedge b = 1$.

Démonstration.

$$\overline{b} \in (A/aA)_* \quad \Leftrightarrow \quad \exists v \in A \ \ \overline{v}\overline{b} = \overline{1} \quad \Leftrightarrow \quad \exists v \in A \ \ \exists u \in A \ \ 1 = vb + ua\,.$$

D'après le th. de Bezout, cela caractérise les éléments $b \in A$ premiers avec a. ∎

Proposition.

Soient A un anneau principal et $p \in A$ non nul. Les conditions suivantes sont équivalentes.

(i) *p est irréductible.*

(ii) *pA est un idéal maximal de A.*

(iii) *pA est un idéal premier de A.*

(iv) *A/pA est un corps.*

Démonstration. (i) ⇔ (ii) Cela a été vu en 11-4.

(ii) ⇔ (iv) d'après 9-11.

(iv) ⇒ (iii) car un corps est intègre (Voir 9-11).

(iii) ⇒ (i) Soient $a, b \in A$ tels que $p = ab$. On a $ab \in pA$. Si pA est premier, alors on a $a \in pA$ ou $b \in pA$, ou encore $p|a$ ou $p|b$. Comme on avait $a|p$ et $b|p$, on voit que a est associé à p ou que b est associé à p. Donc p est irréductible. (Notons que cette implication est valable dans tout anneau commutatif unifère.) ∎

Exercice. Dans l'anneau $A = \mathbb{Z} + i\mathbb{Z}$ des entiers de Gauss, étudier les idéaux maximaux et le quotient par un tel idéal.

Solution. D'après 11-3, l'anneau A est euclidien et donc principal. D'après 11-6, les éléments irréductibles sont les nombres premiers p congrus à 3 modulo 4 et les éléments $\zeta = \alpha + i\beta$ où $\beta \neq 0$ et $a^2 + b^2 = q$ est premier. Les idéaux maximaux sont donc de la forme $I = pA$ ou $J = \zeta A$. D'après la proposition, A/I ou A/J est un corps.

Comme $I = pA$ est un réseau à mailles carrées de bords parallèles aux axes, on voit que A/I possède p^2 éléments, autant que de points à coordonnées entières dans le carré $[0, p[\times[0, p[$. Les classes de 1, 2, ..., $p-1$ ne sont pas nulles car ces éléments n'appartiennent pas au réseau. Celle de p est $\overline{p} = \overline{0}$. La caractéristique du corps A/I est donc p, le sous-corps premier est $F_p = \{\overline{1}, \ldots, \overline{p-1}\} \simeq \mathbb{Z}/p\mathbb{Z}$. Les éléments de A/I sont $\overline{x}\overline{1} + \overline{y}\overline{i}$ où $0 \leqslant x \leqslant p-1$, $0 \leqslant y \leqslant p-1$. Ainsi, le corps $A/I = F_p + F_p\overline{i}$ est une extension de F_p de dimension 2 sur F_p.

Le réseau $\zeta A = \{x\zeta + yi\zeta \,;\ x \in \mathbb{Z}\,,\, y \in \mathbb{Z}\}$ est à mailles carrées non parallèles aux axes. Le carré construit sur ζ et $i\zeta$ est de surface $|\zeta|^2 = \alpha^2 + \beta^2 = q$. Il contient q points de coordonnées entières donc $A/\zeta A$ possède q éléments. La caractéristique de ce corps divise q (voir 9-12, cor.). C'est donc q. Ainsi le sous-corps premier $F_q \simeq \mathbb{Z}/q\mathbb{Z}$ de $A/\zeta A$ est égal à $A/\zeta A$. On a $A/\zeta A \simeq \mathbb{Z}/q\mathbb{Z}$ (avec ici $q = 2$ ou $q \equiv 1 \pmod 4$ d'après 11-6, cor.1).

Application. *Donnons une construction du corps $\mathbb{C}$ des nombres complexes.*

Dans l'anneau $A = \mathbb{R}[X]$, tout polynôme $p(X) = X^2 + bX + c$ à discriminant strictement négatif est irréductible (voir 11-5, ex. 2). L'anneau quotient $K = A/pA$ est donc un corps. Identifions $\mathbb{R}$ avec le sous-anneau de $\mathbb{R}[X]$ constitué des polynômes constants. Sur $\mathbb{R}$, l'homomorphisme canonique $\varphi : A \to A/pA = K$ est injectif car $\mathbb{R}$ est un corps. De ce fait, on peut identifier tout $a \in \mathbb{R}$ avec l'élément de K, classe du polynôme constant égal à a. Soit α la classe du polynôme X. La classe de $p(X)$ dans K étant nulle, on a $\overline{0} = \alpha^2 + b\alpha + c$. Ainsi, K est un corps contenant $\mathbb{R}$ comme sous-corps et dans lequel le polynôme p admet pour racine la classe α de X.

Appliquons cela avec $p(X) = X^2 + 1$. Notons $\mathbb{C}$ le quotient $\mathbb{R}[X]/(X^2+1)$, où (X^2+1) désigne l'idéal principal engendré par le polynôme p dans l'anneau $A = \mathbb{R}[X]$. La classe i de X est telle que $i^2 = -1$. Pour tout $a \in \mathbb{R}[X]$, la division par p donne $a(X) = (X^2+1)q(X) + \beta X + \alpha$. La classe de a dans $\mathbb{C}$ est donc $\overline{a} = \beta i + \alpha$. On retrouve l'expression d'un nombre complexe. Cette construction de $\mathbb{C}$ présente un intérêt considérable car elle se généralise.

Si K est un corps commutatif, si $p \in K[X]$ est irréductible (et donc sans racine dans K), on peut construire par ce procédé un corps "de rupture" pour p, c'est-à-dire un corps K_1 contenant K dans lequel p admet au moins une racine. Et si p ne se décompose pas entièrement en produit de facteurs de degré un sur ce nouveau corps, rien n'empêche de recommencer avec un facteur irréductible de p et d'agrandir le corps K_1 pour que les facteurs irréductibles de $p \in K_1[X]$ aient des racines... C'est la construction imaginée par E. Galois pour étudier les nombres algébriques qui sont racines de polynômes à coefficients entiers. En particulier, l'étude des racines de $X^n - 1$, lui a permis de caractériser le fait qu'une équation soit résoluble à l'aide de formules avec des radicaux, comme le sont les polynômes du second degré, les polynômes de degré trois, ou quatre, par les formules de Cardan (Voir 10-9) ou de Ferrari.

Exercices du chapitre 11

Ex 11 - 1

Soient A un anneau commutatif et unifère, $I = aA$, $J = bA$ les idéaux engendrés par $a \in A$ et $b \in A$.

Montrer que $\overline{a} \in A/J$ est inversible si et seulement si $\overline{b} \in A/I$ est inversible.

Soient K un corps commutatif. Dans $K[X]$, cette condition est-elle vérifiée si $a(X) = X^4 + 1$ et $b(X) = X^2 + X + 1$?

Dans l'anneau $K[X, Y]$, est-elle vérifiée si $a(X, Y) = X$, $b(X, Y) = Y$? Montrer que X et Y sont premiers entre eux. En déduire que $K[X, Y]$ n'est pas un anneau principal.

Ex 11 - 2

Montrer que l'anneau $\mathbb{D}$ des nombres décimaux est principal. Généraliser.

Ex 11 - 3

Soient A un anneau principal et J un idéal de A distinct de $\{0\}$ et de A. Dans quel cas J est-il l'intersection des idéaux maximaux de A qui le contiennent ?

Ex 11 - 4

Soient I, J des idéaux d'un anneau principal. Dans quel cas a-t-on $IJ = I \cap J$?

Ex 11 - 5

Soient K un corps, K_0 un sous-corps de K et $a, b \in K_0[X]$. Montrer que le pgcd de a et b est le même dans les anneaux $K_0[X]$ et $K[X]$.

Soient $m, n \in \mathbb{N}^*$. Dans $\mathbb{R}[X]$, calculer $\operatorname{pgcd}(X^m - 1,\ X^n - 1)$.

Ex 11 - 6

Soit $d < 0$ un entier sans facteur carré. On pose $\delta = \sqrt{|d|}$. Quel est le groupe $(A_d)_*$ des unités de l'anneau A_d des entiers algébriques du corps $\mathbb{Q}(i\delta)$?

Ex 11 - 7

Soit $d < 0$ un entier sans facteur carré. On pose $\delta = \sqrt{|d|}$. Soit A_d l'anneau des entiers algébriques du corps $\mathbb{Q}(i\delta)$.

Pour $d < 0$ congru à 2 ou 3 modulo 4, on a vu en 11-3, prop. que A_d est euclidien si et seulement si $d = -1$ ou $d = -2$. On peut se demander si A_d est principal pour les autres valeurs de d. Supposons donc $d < -2$.

a) Soit I un idéal principal de A_d. Montrer que $\{n(z)\,;\ z \in I \backslash \{0\}\}$ a un plus petit élément $k_I = n(a)$, où $a \in I$.

b) On suppose $d \equiv 2 \pmod 4$. Montrer que A_d n'est pas principal. Pour cela, considérer l'idéal $I = (2, i\delta)$ engendré par 2 et $i\delta$. En supposant que $I = aA_d$, montrer que $n(a) \leqslant 4$. En déduire que $a \in \{1, -1, 2, -2\}$ et faire apparaître une contradiction.

c) On suppose $d \equiv 3 \pmod 4$. En considérant $I = (1 + i\delta, 1 - i\delta)$, montrer de même que A_d n'est pas principal.

Ex 11 - 8

Dans l'anneau $\mathbb{Z}[i]$ des entiers de Gauss, déterminer un quotient q et un reste r pour la division euclidienne de $a = 5 + 6i$ par $b = 2 + i$. Calculer $\operatorname{ppcm}(a, b)$.

Ex 11 - 9

a) Soit $A = \{m + n\sqrt{10}\,;\quad m, n \in \mathbb{Z}\}$. Montrer que A est un sous-anneau de $\mathbb{R}$ et que $\sigma : m + n\sqrt{10} \mapsto m - n\sqrt{10}$ est un automorphisme de A.

b) Montrer que l'équation $2x^2 - 5y^2 = \pm 1$ est sans solution dans $\mathbb{Z} \times \mathbb{Z}$.

c) Montrer que l'idéal I de A engendré par 2 et $\sqrt{10}$ n'est pas principal.

Ex 11 - 10

Montrer que $z \mapsto |n(z)|$ est un stathme euclidien sur l'anneau A_3 des entiers algébriques du corps $\mathbb{Q}(\sqrt{3})$.

Montrer que $u = 2 + \sqrt{3}$ appartient au groupe $(A_3)_*$ et que c'est le plus petit élément de $\{ z \in (A_3)_* \mid z > 1 \}$. En déduire que $\mathbb{R}_+ \cap (A_3)_* = \{u^n ;\ n \in \mathbb{Z}\}$ et que $(A_3)_*$ est isomorphe à $\mathbb{Z} \times (\mathbb{Z}/2\mathbb{Z})$.

Ex 11 - 11

Soient A un anneau commutatif avec unité et $k \in \mathbb{N}^*$. On note S_k l'ensemble des éléments de A de la forme $x_1^2 + \cdots + x_k^2$, somme de k carrés d'éléments de A.

a) Montrer que S_2 et S_4 sont des parties de A multiplicativement stables.

b) Soit $A = \mathbb{Z}/8\mathbb{Z}$. Donner la liste des éléments de S_1, de S_2, de S_3.

c) Soit $A = \mathbb{Z}$. Montrer que $15 \notin S_3$. En déduire que S_3 n'est pas multiplicativement stable.

d) Soient a, b, c, d des entiers tels que

$$a^2 + b^2 + c^2 + d^2 \equiv 0 \pmod 8.$$

Montrer que a, b, c, d sont pairs.

e) Soit $n \in \mathbb{Z}$ tel que $n \equiv -1 \pmod 8$. Montrer que ni dans $\mathbb{Q}$, ni dans $\mathbb{Z}$, il n'est somme de trois carrés.

Ex 11 - 12

Soient p, q deux nombres premiers distincts, différents de 2.

a) Montrer que dans l'anneau $A = \mathbb{Z}/pq\mathbb{Z}$, il existe quatre éléments idempotents. En déduire qu'il existe quatre endomorphismes dans l'anneau $\mathbb{Z}/589\,\mathbb{Z}$.

b) Montrer que le groupe $(\mathbb{Z}/pq\mathbb{Z})_*$ n'est pas cyclique. Donner la décomposition cyclique canonique de $(\mathbb{Z}/589\,\mathbb{Z})_*$. Déterminer un élément d'ordre maximum dans ce groupe multiplicatif.

Ex 11 - 13

Déterminer les solutions $n \in \mathbb{Z}$ du système :

$$\begin{cases} n \equiv 3 \pmod 6 \\ n \equiv 2 \pmod 5 \\ n \equiv 6 \pmod 7 \end{cases}.$$

Indications

Ex 11 - 1

L'inversibilité de $\overline{a} \in A/bA$ équivaut à l'existence d'une relation de Bezout entre a et b. Cette condition est satisfaite dans le premier exemple et ne l'est pas dans le second. ($f : p(X,Y) \mapsto p(X,0)$ est un homomorphisme surjectif de $K[X,Y]$ sur $K[X]$, de noyau l'idéal (Y).)

Ex 11 - 2

Identifier $\mathbb{Z}$ avec un sous-anneau de $\mathbb{D}$. Alors $I \cap \mathbb{Z}$ est un idéal de $\mathbb{Z}$ pour tout idéal I de $\mathbb{D}$.

Ex 11 - 3

D'après 11-4, les idéaux maximaux qui contiennent $J = aA$, sont $p_1A, \ldots, p_kA$, où $p_1, \ldots, p_k$ sont les facteurs premiers de a.

Ex 11 - 4

Si $I = aA$, $J = bA$, alors $IJ = (ab)A$ et $I \cap J = \text{ppcm}(a,b)A$.

Ex 11 - 5

Par unicité de la division euclidienne dans $K[X]$, l'algorithme d'Euclide (voir 11-4, rem.) donne le même résultat dans $K[X]$ et dans $K_0[X]$.

Ex 11 - 6

Pour $d = -1$, $(A_d)_* = \mathbb{U}_4$.
Pour $d = -3$, $(A_d)_* = \mathbb{U}_6$.
Pour $d \neq -1, -3$, $(A_d)_* = \mathbb{U}_2$.

Ex 11 - 7

a) Si $I = aA_d$, alors $n(a) = k_I$.

b) Si $I = aA_d$, comme $2 \in I$, on a $n(a) \leqslant n(2)$, d'où $a = \pm 1$ ou $a = \pm 2$. Etudier alors la condition $a \in I$.

c) Mêmes raisonnements qu'en b).

Ex 11 - 8

On a $q = 3 + i$, $r = i$.
Ici, a et b sont irréductibles.

Ex 11 - 9

a) Comme $10 \equiv 2 \pmod 4$, A est l'anneau d'entiers algébriques A_{10}.

b) $2\overline{x}^2 = \pm\overline{1}$ est sans solution dans $\mathbb{Z}/5\mathbb{Z}$.

c) Si $I = aA$ alors $a|2$ et $a|\sqrt{10}$ donc $n(a)|n(2)$ et $n(a)|n(\sqrt{10})$ dans $\mathbb{Z}$.

Ex 11 - 10

Soient $a, b \in A_3$, avec $b \neq 0$. Si $\frac{a}{b} = x + y\sqrt{3} \in \mathbb{Q}(\sqrt{3})$, il existe α et β dans $\mathbb{Z}$ à distance au plus $\frac{1}{2}$ de x et y.

Ex 11 - 11

a) $(a^2+b^2)(c^2+d^2)$
$= (ac-bd)^2 + (ad+bc)^2$.

b) $S_1 = \{\overline{0}, \overline{1}, \overline{4}\}$, (ensemble des carrés de $\mathbb{Z}/8\mathbb{Z}$), d'où S_2, S_3 par additions.

c) Si on avait $15 = x + y + z$, avec $x \leqslant y \leqslant z$ éléments de S_1, on aurait $5 \leqslant z \leqslant 15$ et donc $z = 9$.

d) Par exemple, si d est impair, $\overline{d}^2 = \overline{1}$ dans $\mathbb{Z}/8\mathbb{Z}$. On aurait $\overline{a}^2 + \overline{b}^2 + \overline{c}^2 = \overline{7}$.

e) Résulte de d).

Ex 11 - 12

Applications du th. chinois.

Ex 11 - 13

Application du th. chinois.

Solutions des exercices du chapitre 11

Ex 11 - 1

$\overline{a} \in (A/J)_* \quad \Leftrightarrow \quad \exists\, u \in A \quad \overline{1} = \overline{a}\,\overline{u} \quad \Leftrightarrow \quad \exists\, u \in A \quad \exists\, v \in A \quad 1 = au + bv\,.$

De même, $\overline{b} \in A/I$ est inversible dans A/I si et seulement s'il existe une relation de Bezout reliant a et b (soit si $aA + bA = A$). Les conditions sont équivalentes.

Si l'anneau A est principal, ces conditions sont vérifiées si et seulement si a et b sont premiers entre eux. C'est le cas dans $K[X]$ pour $a(X) = X^4 + 1$ et $b(X) = X^2 + X + 1$. En effet, par divisions successives l'algorithme d'Euclide donne

$$X^4 + 1 \;=\; (X^2 + X + 1)(X^2 - X) + X + 1 \qquad , \qquad X^2 + X + 1 \;=\; (X+1)X + 1\,.$$

d'où la relation de Bezout :

$$\begin{aligned} 1 \;&=\; b(X) - X(X+1) \;=\; b(X) - X[a(X) - (X^2 - X)b(X)] \\ &=\; -Xa(X) + (X^3 - X^2 + 1)b(X)\,. \end{aligned}$$

Dans $K[X]/J$ l'inverse de la classe de $a(X)$ est la classe du polynôme $-X$. Dans $K[X]/I$, l'inverse de la classe de $b(X)$ est la classe de $X^3 - X^2 + 1$.

Il est clair que $f : p(X,Y) \mapsto p(X,0)$ est un homomorphisme d'anneaux surjectif de $K[X,Y]$ sur $K[X]$, de noyau l'idéal $J = (Y)$ engendré par le polynôme Y. Par factorisation, on obtient un isomorphisme de $K[X,Y]/J$ sur $K[X]$. L'image de X est le polynôme X de $K[X]$. Cette image n'est pas inversible. D'après a), il n'existe pas de relation de Bezout entre X et Y. Pourtant, X et Y sont premiers entre eux. En effet, en ordonnant un polynôme des deux variables X et Y par rapport à X, on peut le voir comme un polynôme de la variable X, à coefficients dans l'anneau $K[Y]$. Autrement dit les anneaux $K[X,Y]$ et $K[X][Y]$ sont isomorphes. Un diviseur commun à X et Y devrait donc être de degré 1 ou 0 par rapport à X et de même par rapport à Y. On voit que les éléments de K_* sont les seuls diviseurs communs de X et Y. L'anneau $K[X,Y]$ n'est donc pas principal. Bien entendu, il n'est pas difficile de démontrer directement qu'il n'existe pas de relation de Bezout entre X et Y dans $K[X,Y]$.

Ex 11 - 2

Considérons plus généralement, un anneau principal A, une partie S de A multiplicativement stable, telle que $0 \notin S$ et $1 \in S$, l'anneau K des fractions de A à dénominateur dans S (voir 9-10). Identifions A avec son image dans K par l'homomorphisme injectif $x \mapsto \overline{(x,1)}$, où $\overline{(x,1)}$ est la classe de la fraction $(x,1) \in A \times S$. D'après 9-10, prop. (iii), puisque A est intègre, l'anneau K est intègre. Montrons que tout idéal I de K est principal. Il est clair que $I_0 = I \cap A$ est un idéal de A. Pour tout $y \in I$ et pour toute fraction $(x,s) \in A \times S$ qui représente y, on a $x = sy \in I \cap A = I_0$. Réciproquement, pour tout $x \in I_0$ et pour tout $s \in S$ on a $\overline{(x,s)} = \overline{(1,s)}\,x \in I$ car $x \in I_0 \subset I$. Ainsi, $I = \{\overline{(x,s)} \in K \;\; x \in I_0\}$. Comme A est principal, il existe $u \in I_0$ tel que $I_0 = uA$. Donc I est l'ensemble des $\overline{(ua,s)} = \overline{(u,1)}\,\overline{(a,s)}$, où $a \in A$, $s \in S$. En identifiant u avec $\overline{(u,1)}$ comme nous l'avons fait, on a $I = uK$ et l'anneau K est principal.

Ex 11 - 3

Soient a un générateur de J. Puisque $J \neq \{0\}$ et $J \neq A$ on a $a \neq 0$ et $a \notin A_*$. Soit $a = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$ sa décomposition en facteurs irréductibles. Les idéaux maximaux de A contenant J sont les idéaux Ap, où p est irréductible tel que $Aa = J \subset Ap$ c'est-à-dire tel que p divise a. Ce sont donc les idéaux $Ap_1, \ldots, Ap_k$. D'après 11-4, prop., $I = A_{p_1} \cap \cdots \cap A_{p_k}$ a pour générateur le ppcm $p_1 \cdots p_k$ de $p_1, \ldots, p_k$. On aura $I = J$ si et seulement si $a = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$ est associé à $p_1 \cdots p_k$, soit si $\alpha_1 = 1, \ldots, \alpha_k = 1$ c'est-à-dire si tout facteur irréductible de a est sans multiplicité.

Ex 11 - 4

Puisque A est principal, il existe $a \in A$ et $b \in A$ tels que $I = aA$ et $J = bA$. Considérons $x = \sum_{i=1}^{k} x_i y_i \in IJ$, où $k \in \mathbb{N}^*$ et $x_i \in I$, $y_i \in J$ pour $i = 1, \ldots, k$. Pour tout $i = 1, \ldots, k$, il existe $u_i, v_i \in A$ tels que $x_i = au_i$, $y_i = bv_i$ donc $x = \sum_{i=1}^{k} x_i y_i = ab(\sum_{i=1}^{k} u_i v_i) \in (ab)A$. Réciproquement, tout $(ab)x \in (ab)A$ s'écrit $a(bx)$ avec $a \in I$ et $bx \in J$ donc $IJ = (ab)A$ et IJ admet ab pour générateur.

Les générateurs de $I \cap J$ sont les ppcm de a et b (11-4, prop.). On a donc $IJ = I \cap J$ si et seulement si ab est ppcm de a et b. Or, si m est ppcm de a et b si d est pgcd de a et b, alors md et ab sont associés. Donc ab est ppcm de a et b si et seulement si d est une unité, soit si $a \wedge b = 1$. Donc $IJ = I \cap J$ si et seulement si $a \wedge b = 1$.

Ex 11 - 5

Soit $a = bq + r$, avec $q, r \in K_0[X]$ et $\mathrm{d}^\circ(r) < \mathrm{d}^\circ(b)$, le résultat de la division de a par b dans l'anneau euclidien $K_0[X]$. Dans $K[X]$, q et r sont encore le quotient et le reste en raison de l'unicité de la division de a par b dans $K[X]$. De même, si on effectue la division de b par r, (algorithme d'Euclide de recherche du pgcd), on obtient le même quotient et le même reste dans les deux anneaux. On voit par récurrence, que le dernier reste non nul, c'est-à-dire le pgcd, est le même dans $K[X]$ et dans $K_0[X]$.

Le pgcd de $a(X) = X^m - 1$ et $b(X) = X^n - 1$ est donc le même dans $\mathbb{R}[X]$ et dans $\mathbb{C}[X]$. Dans $\mathbb{C}$ ces polynômes ont pour racines simples les éléments de $\mathbb{U}_m$ et $\mathbb{U}_n$. Leurs facteurs irréductibles communs sont les polynômes $X - \lambda$, où $\lambda \in \mathbb{U}_m \cap \mathbb{U}_n = \mathbb{U}_d$, où $d = \mathrm{pgcd}(m, n)$ (voir 1-7, ex.). Donc $X^d - 1 = \mathrm{pgcd}(X^n - 1, X^m - 1)$.

Sur des exemples, l'algorithme d'Euclide conduit aussi à ce résultat. Par exemple, si $m = 15$ et $n = 9$, les divisions successives donnent :

$$X^{15} - 1 = (X^9 - 1)X^6 + X^6 - 1 \quad , \quad X^9 - 1 = (X^6 - 1)X^3 + X^3 - 1 .$$

La division de $X^6 - 1$ par $X^3 - 1$ tombe juste donc $X^3 - 1$ est le pgcd.

Ex 11 - 6

D'après 11-6, lemme, $(A_d)_* = \{z \in A_d \mid n(z) = 1\}$, où $n(z) = z\bar{z}$.

1°) Supposons $d \equiv 2 \pmod 4$ ou $d \equiv 3 \pmod 4$.
Si $d = -1$, les unités de l'anneau $\mathbb{Z} + i\mathbb{Z}$ des entiers de Gauss, sont $1, i - 1, -i$.

Si on a $d \leqslant -2$, d'après 11-3, prop., les éléments de A_d sont de la forme $z = x + iy\delta$ avec $x, y \in \mathbb{Z}$. La condition $n(z) = x^2 + |d|y^2 = 1$ nécessite $y = 0$. Donc $(A_d)_* = \{1, -1\}$.

2°) Supposons $d \equiv 1 \pmod 4$. D'après 11-3, prop., $A_d = \{x + y\frac{1+i\delta}{2}\,;\ x, y \in \mathbb{Z}\}$.

Pour $d < -4$, $n(z) = (x + \frac{y}{2})^2 + |d|\frac{y^2}{4} = 1$ nécessite $y = 0$. On a donc $(A_d)_* = \{1, -1\}$.

Pour $d = -3$, la condition $n(z) = (x + \frac{y}{2})^2 + |d|\frac{y^2}{4} = x^2 + xy + y^2 = 1$ nécessite $|y| \leqslant 1$.
- Si $y = 0$ on obtient $x = \pm 1$ d'où deux unités $z = 1$ ou -1.
- Si $y = 1$, alors $x^2 + x = 0$, d'où deux unités $z = \frac{1+i\sqrt{3}}{2}$ ou $z = -1 + \frac{1+i\sqrt{3}}{2} = \frac{-1+i\sqrt{3}}{2}$.
- Si $y = -1$ alors $x^2 - x = 0$, d'où deux unités $z = -\frac{1+i\sqrt{3}}{2}$ ou $z = 1 - \frac{1+i\sqrt{3}}{2} = \frac{1-i\sqrt{3}}{2}$.

Donc $(A_{-3})_*$ est le groupe $\mathbb{U}_6$ des racines sixièmes de l'unité.

Ex 11 - 7

a) Si $I = aA_d$ est principal, pour tout $z \in I$, il existe $b \in A_d$ tel que $z = ab$. Si $z \neq 0$, on a $b \neq 0$, d'où $n(b) = |b|^2 \neq 0$, avec $n(b) \in \mathbb{N}$ et donc $n(z) \geqslant n(a)$.

b) Si $I = aA_d$ est principal, puisque $2 \in I$, on a $k_I = n(a) \leqslant n(2) = 4$. Puisque $d < -2$ et $d \equiv 2 \pmod 4$, on a $d \leqslant -6$. D'après 11-3, prop., il existe $\alpha \in \mathbb{Z}$, $\beta \in \mathbb{Z}$ tels que $a = \alpha + i\beta\delta$. La condition $n(a) = \alpha^2 + |d|\beta^2 \leqslant 4$ nécessite $\beta = 0$ et donc $a = \pm 2$ ou $a = \pm 1$. On peut supposer $a = 1$ ou 2, quitte à remplacer a par $-a$.

Si $a = 2$, alors $I = 2A_d$ doit contenir $i\delta \in I$. C'est impossible car alors $d = (i\delta)^2$ serait multiple de 4. Or d est sans facteur carré.

Si $a = 1$, il existe $x + iy\delta \in A_d$, $u + iv\delta \in A_d$ tels que

$$1 = (x + iy\delta)2 + (u + iv\delta)i\delta\,,$$

d'où $1 = 2x + vd$, $0 = 2y + u$. Comme $d \equiv 2 \pmod 4$, est pair, la première relation est impossible : I n'est pas principal. Ainsi A_d n'est pas un anneau principal.

c) On a $2 = (1 + i\delta) + (1 - i\delta) \in I$. Comme en b), si I est principal, il a pour générateur $a = 2$ ou $a = 1$. Le cas $a = 2$ est exclu car $1 + i\delta \in I$ serait tel que $\frac{1+i\delta}{2} \in A_d$, ce qui n'est pas le cas d'après 11-3, prop.

Supposons que $a = 1$. Il existe $x + iy\delta \in A_d$ et $u + iv\delta \in A_d$ tels que

$$1 = (x + iy\delta)(1 + i\delta) + (u + iv\delta)(1 - i\delta)\,,$$

d'où $1 = x + dy + u - dv$, $0 = x + y - u + v$. En ajoutant membre à membre, $1 = 2x + (1 + d)y + (1 - d)v$. Comme $d \equiv 3 \pmod 4$ est impair, le second membre est pair. C'est impossible : I n'est pas principal et A_d n'est pas un anneau principal.

Ex 11 - 8

Conformément à 11-3, prop., on obtient un quotient q pour la division de a par b, en prenant un point du réseau $\mathbb{Z} + i\mathbb{Z}$ à distance minimum de $\frac{a}{b}$. Ici on a

$$\frac{a}{b} = \frac{5+6i}{2+i} = \frac{(5+6i)(2-i)}{2^2+1^2} = \frac{16+7i}{5} = (3 + \tfrac{1}{5}) + i(1 + \tfrac{2}{5})\,.$$

Dans cet exemple, $q = 3 + i$ est le point de $\mathbb{Z} + i\mathbb{Z}$ le plus proche de $\frac{a}{b}$. Le reste sera alors $r = a - bq = i$. On a $n(r) = 1 < n(b) = 5$, conformément au fait que la norme $z \mapsto n(z)$ est le stathme pour cette division.

Comme $n(a) = a\overline{a} = 61$ est premier et $61 \equiv 1 \pmod 4$, a est irréductible dans l'anneau $\mathbb{Z} + i\mathbb{Z}$ (11-6, cor. 1,). De même, $n(b) = 5$ est premier et $5 \equiv 1 \pmod 4$ donc b est irréductible. Comme $n(b) \neq n(a)$, ces éléments irréductibles ne sont pas associés. Donc $ab = 4 + 17i$ est ppcm de a et b dans $\mathbb{Z} + i\mathbb{Z}$.

Ex 11 - 9

a) On a $10 \equiv 2 \pmod 4$ donc A est l'anneau des entiers algébriques de $\mathbb{Q}(\sqrt{10})$ (11-3, prop.). D'après 9-9, ex. 2, σ est l'unique automorphisme de $\mathbb{Q}(\sqrt{10})$ distinct de Id . Il laisse stable A et on a $\sigma^2 = \text{Id}$.

b) Dans $\mathbb{Z}/5\mathbb{Z}$, pour tout $x \in \mathbb{Z}$ on a $2\overline{x}^2 \in \{\overline{0}, \overline{2}, -\overline{2}\}$ car $\overline{0}^2 = \overline{0}$, $\overline{1}^2 = \overline{4}^2 = \overline{1}$, $\overline{2}^2 = \overline{3}^2 = -\overline{1}$. Donc $2x^2 - 5y^2 = \pm 1$ est sans solution dans $\mathbb{Z} \times \mathbb{Z}$.

c) Supposons qu'il existe $a \in A$ tel que $I = \mathbb{Z}\,2 + \mathbb{Z}\sqrt{10}$ soit égal à aA. Il existe alors $u, v \in \mathbb{Z}$ tels que $a = 2u + v\sqrt{10}$. Puisque a divise $2 \in I$ dans A, on voit que $n(a) = 4u^2 - 10v^2$ divise $n(2) = 4$ et donc $2u^2 - 5v^2$ divise 2.

De même, $n(a) = 4u^2 - 10v^2$ divise $n(\sqrt{10}) = 10$ et donc $2u^2 - 5v^2$ divise 5.

Finalement, $2u^2 - 5v^2$ divise $\text{pgcd}(2,5) = 1$ donc $2u^2 - 5v^2 = \pm 1$. C'est impossible d'après b). Donc l'idéal I n'est pas principal et A n'est pas un anneau principal.

Ex 11 - 10

D'après 11-3, prop., puisque $3 \equiv 3 \pmod 4$ on a $A_3 = \mathbb{Z} + \mathbb{Z}\sqrt{3}$ et la norme de $x + y\sqrt{3} \in A_3$ a pour expression $n(x + y\sqrt{3}) = (x + y\sqrt{3})(x - y\sqrt{3}) = x^2 - 3y^2$. Soient $a, b \in A_3$, avec $b \neq 0$. Cherchons un quotient $q \in A_3$ et un reste r, selon la méthode employée dans l'anneau des entiers de Gauss. Considérons $\frac{a}{b} = x + y\sqrt{3} \in \mathbb{Q}(\sqrt{3})$. Il existe $\alpha, \beta \in \mathbb{Z}$ tels que $|x - \alpha| \leqslant \frac{1}{2}$ et $|y - \beta| \leqslant \frac{1}{2}$. Posons $q = \alpha + \beta\sqrt{3}$. On a

$$-\tfrac{3}{4} \leqslant (x-\alpha)^2 - 3(y-\beta)^2 \leqslant \tfrac{1}{4} \quad \text{d'où} \quad |\,(x-\alpha)^2 - 3(y-\beta)^2\,| \leqslant \tfrac{3}{4}\,.$$

On en déduit $|n(a - bq)| = n(b)n(\frac{a}{b} - q) \leqslant \frac{3}{4}n(b) < n(b)$. Ainsi, n est un stathme et A_3 est un anneau euclidien. Comme $n(2 + \sqrt{3}) = (2 + \sqrt{3})(2 - \sqrt{3}) = 1$, on voit que $u = 2 + \sqrt{3} \in (A_3)_*$ et que $u^{-1} = \sigma(u) = 2 - \sqrt{3}$ (utilisé en 12-5, ex. 3).

On ne peut avoir $-1 = n(z) = x^2 - 3y^2$ car -1 n'est pas un carré dans $\mathbb{Z}/3\mathbb{Z}$. D'après 10-6, lemme, on a donc $(A_3)_* = \{z \in A_3 \mid n(z) = \pm 1\} = \{z \in A_3 \mid n(z) = 1\}$. Pour tout $z \in (A_3)_*$ on a $-z \in (A_3)_*$ car $n(-z) = n(z)$. Vérifions que le sous-groupe $G = \{\, z \in \mathbb{R}_+^* \;\; n(z) = 1 \,\}$ de $(A_3)_*$ est monogène engendré par u. Montrons d'abord que u est le plus petit élément de $G_0 = \{\, z \in A_3 \;\; z > 1 \;,\; n(z) = 1 \,\}$. Considérons $z = x + y\sqrt{3} \in G_0$ et supposons que l'on ait $1 < x + y\sqrt{3} < 2 + \sqrt{3}$ d'où pour les inverses $0 < x - y\sqrt{3} < 1$. En ajoutant ces inégalités, il vient $1 < 2x < 3 + \sqrt{3}$ donc $x = 1$ ou $x = 2$. Pour $x = 1$ on aurait $y = 0$ car $x^2 - 3y^2 = 1$. C'est exclu car on a $z > 1$. Donc $x = 2$ et $y = \pm\sqrt{3}$ Du fait que $z > 1$ on voit que $z = u$.

Considérons alors $z \in G_0$. Il existe $k \in \mathbb{Z}$ unique tel que $u^k \leqslant z < u^{k+1}$. On a alors $1 \leqslant zu^{-k} < u$ et $zu^{-k} \in G$ et donc $zu^{-k} = 1$ puisque u est le plus petit élément de G_0. Ainsi, on a $G_0 = \{\, u^k ; \;\; k \in \mathbb{N}^* \,\}$ d'où $G = \{\, u^k ; \;\; k \in \mathbb{Z} \,\} \simeq \mathbb{Z}$ et $(A_3)_* = \{\, \varepsilon u^k ; \;\; \varepsilon \in \{1, -1\} \;, k \in \mathbb{Z} \,\} \simeq (\mathbb{Z}/2\mathbb{Z}) \times \mathbb{Z}$. L'équation diophantienne $x^2 - dy^2 = 1$, que nous avons résolue pour $d = 3$, est l'équation de Pell-Fermat.

Ex 11 - 11

a) Dans $\mathbb{C}$, l'étude des entiers de Gauss nous a habitué à la relation :

$$\begin{aligned}(a^2+b^2)(c^2+d^2) &= n(a+ib)n(c+id) = n[(a+ib)(c+id)] \\ &= n[(ac-bd)+i(ad+bc)] = (ac-bd)^2+(ad+bc)^2\,.\end{aligned}$$

Dans un anneau commutatif quelconque, si on développe les deux membres extrêmes, on voit qu'ils sont égaux. Cette identité montre que S_2 est multiplicativement stable.

Pour S_4, il existe pareillement une identité, due à Euler (naturelle dans le calcul de la norme d'un produit de deux quaternions, comme la précédente dans $\mathbb{C}$) qui montre que S_4 est multiplicativement stable :

$$\begin{aligned}&(a^2+b^2+c^2+d^2)(x^2+y^2+z^2+t^2)\\ &= (ax+by+cz+dt)^2+(ay-bx+ct-dz)^2+(az-cx+dy-bt)^2+(at-dx+bz-cy)^2.\end{aligned}$$

Nous verrons (Ex. 12-15), que tout $p \in \mathbb{N}$ premier est somme de quatre carrés. Puisque S_4 est stable, tout $n \in \mathbb{N}$ est somme de quatre carrés (dû à Lagrange).

b) $S_1 = \{\overline{0}\,,\,\overline{1}\,,\,\overline{4}\}$, $S_2 = \{\overline{0}\,,\,\overline{1}\,,\,\overline{2}\,,\,\overline{4}\,,\,\overline{5}\}$, $S_3 = \{\overline{0}\,,\,\overline{1}\,,\,\overline{2}\,,\,\overline{3}\,,\,\overline{4}\,,\,\overline{5}\,,\,\overline{6}\}$.

c) Dans $\mathbb{Z}$ on a $S_1 = \{0\,,\,1\,,\,4\,,\,9\,,\,16\,,\ldots\}$. Si on avait $15 = x+y+z$ avec $x \leqslant y \leqslant z$ éléments de S_1, on aurait $z \geqslant 5$ (car $z \leqslant 4$ implique $y \leqslant 4$ et $x \leqslant 4$ et donc $x+y+z < 15$) et $z < 16$, d'où $z = 9$. Il en résulterait $x+y = 15-9 = 6$, absurde car 6 n'est pas somme de deux carrés (11-6, cor. 3). Comme $3 = 1^2+1^2+1^2 \in S_3$ et $5 = 0^2+1^2+2^2 \in S_3$, on voit que S_3 n'est pas stable par multiplication.

d) Supposons l'un des nombres impair, par exemple d. Dans $\mathbb{Z}/8\mathbb{Z}$, on aurait $\overline{d}^2 = \overline{1}$ car on a $S_1 = \{\overline{0}\,,\,\overline{1}\,,\,\overline{4}\}$ et les valeurs $\overline{0}\,,\,\overline{4}$ sont exclues puisque d n'est pas pair. On en déduirait $\overline{a}^2+\overline{b}^2+\overline{c}^2 = -\overline{d}^2 = -\overline{1} = \overline{7}$. D'après b), c'est impossible car $\overline{7} \notin S_3$.

e) Supposons que $n = x^2+y^2+z^2$, où $x,y,z \in \mathbb{Q}$. Soient $\frac{x'_1}{x_1}, \frac{y'_1}{y_1}, \frac{z'_1}{z_1}$ les fractions réduites qui représentent x,y,z. Réduisons-les au plus petit dénominateur commun (le ppcm de x_1,y_1,z_1). On obtient $x = \frac{a}{d}\,,\ y = \frac{b}{d}\,,\ z = \frac{c}{d}$ avec a,b,c,d premiers dans leur ensemble et tels que $nd^2 = a^2+b^2+c^2$. Dans $\mathbb{Z}/8\mathbb{Z}$ on en déduit $-\overline{d}^2 = \overline{a}^2+\overline{b}^2+\overline{c}^2$. D'après d), a,b,c,d doivent être tous pairs. Cela contredit le fait qu'ils soient premiers entre eux. Donc $n \notin S_3$ dans $\mathbb{Q}$ et a fortiori dans $\mathbb{Z}$.

Ex 11 - 12

a) D'après 9-2, ex. 2, tout endomorphismes du groupe additif $(\mathbb{Z}/n\mathbb{Z},+)$ est de la forme $\overline{x} \mapsto \overline{k}\overline{x}$. C'est un endomorphismes de l'anneau $\mathbb{Z}/n\mathbb{Z}$ si et seulement si $\overline{k}^2 = \overline{k}$.

D'après le th. chinois, les anneaux $A = \mathbb{Z}/pq\mathbb{Z}$ et $B = (\mathbb{Z}/p\mathbb{Z}) \times (\mathbb{Z}/q\mathbb{Z})$ sont isomorphes. Pour que $X = (x,y) \in B$ soit idempotent, il faut et il suffit que $x^2 = x$ et $y^2 = y$. Comme p,q sont premiers, $\mathbb{Z}/p\mathbb{Z}$ et $\mathbb{Z}/q\mathbb{Z}$ sont des corps. Le polynôme $x^2-x = x(x-\overline{1})$ a donc pour racines $\overline{0}$ et $\overline{1}$ dans $\mathbb{Z}/p\mathbb{Z}$. De même y^2-y a pour racines $\dot{0}$ et $\dot{1}$ dans $\mathbb{Z}/q\mathbb{Z}$. Dans B il existe donc quatre idempotents $(\overline{0},\dot{0})\,,\ (\overline{0},\dot{1})\,,\ (\overline{1},\dot{0})\,,\ (\overline{1},\dot{1})$. Dans A il existe donc 4 idempotents et 4 endomorphismes.

On a $589 = 19 \times 31$. Cherchons une relation de Bezout par l'algorithme d'Euclide.

$$31 = 19 + 12 \ , \quad 19 = 12 + 7 \ , \quad 12 = 7 + 5 \ , \quad 7 = 5 + 2 \ , \quad 5 = 2 \times 2 + 1 \, ,$$

d'où $1 = -13 \times 19 + 8 \times 31$. Les idempotents de $A = \mathbb{Z}/pq\mathbb{Z}$ associés aux idempotents de B sont les classes modulo 589 de :
$0 \ , \quad 8 \times 31 = 248 \quad , \quad -13 \times 19 = -247 \equiv 342 \quad , \quad 1 \, .$
Les 4 endomorphismes de A sont les applications $\overline{x} \mapsto \overline{k}\,\overline{x}$ correspondantes.

b) Puisque les anneaux A et B sont isomorphes, les groupes $A_* = (\mathbb{Z}/pq\mathbb{Z})_*$ et $B_* = (\mathbb{Z}/p\mathbb{Z})_* \times (\mathbb{Z}/q\mathbb{Z})_*$ sont isomorphes. Comme $K = \mathbb{Z}/p\mathbb{Z}$ et $K' = \mathbb{Z}/q\mathbb{Z}$ sont des corps (9-11, cor. 1), K_* et K'_* sont des groupes cycliques (10-7, cor. 1) d'ordres $p-1$ et $q-1$ pairs. Le produit $K_* \times K'_*$ n'est pas cyclique (3-4, prop.).

Pour $p = 19$ et $q = 31$ on a $K_* \simeq \mathbb{Z}/18\mathbb{Z} \simeq (\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/3^2\mathbb{Z})$ et $K'_* \simeq \mathbb{Z}/30\mathbb{Z} \simeq (\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/3\mathbb{Z}) \times (\mathbb{Z}/5\mathbb{Z})$ car les composantes primaires de ces groupes sont cycliques (3-3, prop.). La décomposition cyclique canonique de $K_* \times K'_*$ est donc

$$[(\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/3\mathbb{Z})]\,[(\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/3^2\mathbb{Z}) \times (\mathbb{Z}/5\mathbb{Z})] \ \simeq \ (\mathbb{Z}/6\mathbb{Z}) \times (\mathbb{Z}/90\mathbb{Z}) \, ,$$

car un produit de groupes cycliques dont les ordres sont deux à deux premiers entre eux, est cyclique. Les invariants de $K_* \times K'_*$ sont 6 et 90. (Voir aussi Ex. 3-11.)

Dans le groupe additif $(\mathbb{Z}/6\mathbb{Z}) \times (\mathbb{Z}/90\mathbb{Z})$, il existe des éléments d'ordre 90 comme $(\overline{0}, \dot{1})$. C'est le maximum de l'ordre $o(\overline{x}, \dot{y}) = \text{ppcm}(o(\overline{x}), o(\dot{y}))$ d'un élément car $o(\overline{x}) \,|\, 6$ et $o(\dot{y}) \,|\, 90$. Pour déterminer explicitement un tel élément dans $K_* \times K'_*$, cherchons des générateurs des groupes cycliques K_*, K'_*. On a $2 \wedge 19 = 1$ donc $\overline{2} \in K_*$. L'ordre $o(\overline{2})$ divise $[K_* : 1] = 18$ (th. de Lagrange). Donc $o(\overline{2})$ est l'un des diviseurs $1, 2, 3, 6, 9, 18$ de 18. On a : $\overline{2}^2 = \overline{4}$, $\overline{2}^3 = \overline{8}$, $\overline{2}^6 = \overline{7}$, $\overline{2}^9 = -\overline{1}$, donc $o(\overline{2}) = 18$. Cela prouve que $\overline{2}$ engendre le groupe cyclique K_*.

De même, $\dot{2} \in K'_*$ et $o(\dot{2})$ divise $[K'_* : 1] = 30$. On a $\dot{2}^2 = \dot{4}$, $\dot{2}^3 = \dot{8}$, $\dot{2}^5 = 1$. Ici $o(\dot{2}) = 5$. C'est parfait : dans $K_* \times K'_*$ l'ordre de $(\overline{2}, \dot{2})$ est $\text{ppcm}(18, 5) = 90$. L'élément de $\mathbb{Z}/589\,\mathbb{Z}$ correspondant à $(\overline{2}, \dot{2})$ est la classe de x où $x = -13 \times 19 \times 2 + 8 \times 31 \times 2 = 2$. Il a pour ordre 90 dans $\mathbb{Z}/589\mathbb{Z}$.

Ex 11 - 13

Les nombres $6, 5, 7$ sont deux à deux premiers entre eux. D'après le th. chinois, ce système a une solution, unique modulo $6 \times 5 \times 7 = 210$. Pour obtenir une solution n_0 déterminons une relation de Bezout liant $5 \times 7 = 35$, $6 \times 7 = 42$ et $6 \times 5 = 30$. La division de 42 par 35 donne $42 = 35 + 7$ et 7 est le pgcd de 42 et 35. Cherchons une relation de Bezout entre 30 et 7. On a $30 = 4 \times 7 + 2$, $7 = 3 \times 2 + 1$ d'où $1 = 7 - 3(30 - 4 \times 7) = 13 \times 7 - 3 \times 30$, puis $1 = -13 \times 35 + 13 \times 42 - 3 \times 30$.

Alors $n_0 = -(13 \times 35)a + (13 \times 42)b - (3 \times 30)c$ est tel que

$$n_0 \equiv a \ (\text{mod}\, 6) \quad , \quad n_0 \equiv b \ (\text{mod}\, 5) \quad , \quad n_0 \equiv c \ (\text{mod}\, 7) \, .$$

Avec $a = 3$, $b = 2$, $c = 6$ on obtient $n_0 = -813$ unique solution modulo 210. Les solutions du système sont donc $n = 27 + k\,210$ où $k \in \mathbb{Z}$. (Si on s'aperçoit a priori que $n_0 = 27$ est solution, on obtient cette réponse sans calcul.)

Quatrième partie

Théorie des nombres

Chapitre 12

Arithmétique

12.1 Congruences, anneau $\mathbb{Z}/n\mathbb{Z}$

Récapitulons ce que nous connaissons sur l'anneau $\mathbb{Z}$. Il est euclidien et donc principal. Les idéaux sont les parties de la forme $n\mathbb{Z}$, où $n \in \mathbb{N}$. Les idéaux maximaux, qui sont aussi les idéaux premiers autres que $\{0\}$, sont les parties $p\mathbb{Z}$, où p appartient à l'ensemble $\mathcal{P}$ des nombres premiers. Le groupe des unités de $\mathbb{Z}$ est $\{1, -1\}$.

Deux entiers $x \in \mathbb{Z}$ et $y \in \mathbb{Z}$ sont dits congrus modulo n, si

$$\exists k \in \mathbb{Z} \quad y = x + kn\,.$$

Cette relation notée $x \equiv y \ (\mathrm{mod}\, n\,)$ est la relation d'équivalence associée à l'idéal $n\mathbb{Z}$. D'après 9-7, elle est compatible avec les opérations de $\mathbb{Z}$:

$$\begin{array}{lllll} x \equiv x' & \text{et} & y \equiv y' & \Rightarrow & x + y \equiv x' + y'\,, \\ x \equiv x' & \text{et} & y \equiv y' & \Rightarrow & x\,y \equiv x'\,y'\,, \end{array}$$

L'ensemble quotient $\mathbb{Z}/n\mathbb{Z} = \{\overline{0}, \ldots, \overline{n-1}\}$ est un anneau si on le munit des opérations

$$(1) \qquad \overline{x} + \overline{y} = \overline{x+y} \qquad , \qquad \overline{x}\,\overline{y} = \overline{xy} \qquad \text{où} \qquad \overline{x}\,,\, \overline{y} \in \mathbb{Z}/n\mathbb{Z},$$

et $\overline{1}$ est unité. D'après 11-8, lemme, le groupe des unités de cet anneau $\mathbb{Z}/n\mathbb{Z}$ est $\{\overline{x} \in \mathbb{Z}/n\mathbb{Z} \mid 0 \leqslant x \leqslant n-1 \text{ et } x \wedge n = 1\}$. Son cardinal est $\varphi(n)$, où φ est la fonction d'Euler. Comme application, rappelons les critères de divisibilité classiques.

Proposition.

Considérons $n \in \mathbb{N}$ et son écriture décimale $\alpha_k \cdots \alpha_0$.
Modulo 2 et modulo 5, n est congru à son chiffre des unités α_0.
Modulo 3 et module 9, n est congru à la somme $\alpha_0 + \cdots + \alpha_k$.
Modulo 11, il est congru à la somme alternée $\alpha_0 - \alpha_1 + \alpha_2 + \cdots + (-1)^k \alpha_k$.
Modulo 7, il est congru à $\alpha_0 + 3\alpha_1 + 2\alpha_2 - \alpha_3 - 3\alpha_4 - 2\alpha_5 + \alpha_6 + \cdots$
Modulo 13, il est congru à $\alpha_0 - 3\alpha_1 - 4\alpha_2 - \alpha_3 + 3\alpha_4 + 4\alpha_5 + \alpha_5 + \cdots$

Démonstration. Modulo 2 et modulo 5, on a $10 \equiv 0$, $10^2 \equiv 0, \ldots$.
Modulo 3 et modulo 9, on a $10 \equiv 1$, $10^2 \equiv 1, \ldots$. et donc $n \equiv \alpha_0 + \cdots + \alpha_k$.
Modulo11, on a $10 \equiv -1$, $10^2 \equiv 1, ..., 10^k \equiv (-1)^k, \ldots$ d'où la troisième assertion.
Modulo7, on a $10 \equiv 3$, $10^2 \equiv 3^2 \equiv 2$, $10^3 \equiv 2 \times 10 \equiv -1, \ldots$
Modulo13, on a $10 \equiv -3$, $10^2 \equiv (-3)^2 \equiv -4$, $10^3 \equiv (-3) \times (-4) \equiv -1, \ldots$ ∎

Remarque. Rappelons que ces critères de divisibilité donnent un moyen de détecter des erreurs dans des calculs comportant des additions, des multiplications ou des divisions.

Si on veut faire la preuve par 9 pour le produit $ab = c$, on considère la somme a_1 des chiffres de l'expression décimale de a et de même les sommes b_1 et c_1 pour b et c. On doit avoir $a_1 b_1 \equiv c_1$. Si cette condition nécessaire n'est pas remplie, il existe obligatoirement une erreur dans le calcul. Cette condition n'est évidemment pas suffisante. Si elle est vérifiée, on ne peut être certain que l'opération soit juste.

Pour une division $a = bq + r$, les nombres a_1 , b_1 , q_1 , r_1 associés à a , b , q , r devront vérifier $a_1 \equiv b_1 q_1 + r_1$.

Exercice 1. a) Déterminer les facteurs premiers de $n = 135\,135$.

b) Pour quelles valeurs de k, le nombre $m = 1 \cdots 1$ dont l'écriture décimale comporte k fois le chiffre 1 est-il divisible par 7 ? Par 13 ?

Solution a) n est divisible par 5, par 9 car $5+3+1+5+3+1 = 18$ l'est. Il est divisible par 7, par 11, par 13, comme tout nombre d'écriture $\alpha\beta\gamma\alpha\beta\gamma$. Le quotient de n par $5 \times 7 \times 9 \times 11 \times 13 = 45045$ est visiblement 3 donc $n = 3^2 \times 5 \times 7 \times 11 \times 13$.

b) Si $k \equiv 0 \pmod 6$, les critères de divisibilité par 7 et par 13 sont vérifiés. Sinon, il ne l'est pas. Donc m est divisible par 7 ou par 13 si et seulement si k est multiple de 6 et alors m est divisible par 7, 13 et aussi par 11 et 3. On a $111111 = 7 \times 13 \times 3 \times 11 \times 37$.

Exercice 2. a) Soient $a \in \mathbb{N}$, $b \in \mathbb{Z}$. Résoudre $ax \equiv b \pmod n$ où $n \geqslant 2$

b) Soient $a \in \mathbb{N}^*$, $b \in \mathbb{Z}$, $c \in \mathbb{Z}$. Résoudre $ax + by = c$.

c) Calculer effectivement les solutions de $522\,x + 2214\,y = 36$.

Solution a) Dans $\mathbb{Z}/n\mathbb{Z}$, l'équation se traduit par $\overline{a}\,\overline{x} = \overline{b}$.

Si $\overline{a}$ est inversible, c'est-à-dire si $a \wedge n = 1$, on a dans $\mathbb{Z}/n\mathbb{Z}$ une solution $\overline{x} = (\overline{a})^{-1}\overline{b}$, unique. Si $x_0 \in \mathbb{Z}$ est tel que $\overline{x}_0 = (\overline{a})^{-1}\overline{b}$, alors les solutions sont $x = x_0 + kn$, où $k \in \mathbb{Z}$. Pour trouver un inverse de a modulo n, on peut chercher une relation de Bezout $au + nv = 1$ et alors $(\overline{a})^{-1} = \overline{u}$. Pour des petites valeurs de n, on peut utiliser le th. de Fermat-Euler (12-2) qui dit que $a^{\varphi(n)} \equiv 1$, de sorte que $(\overline{a})^{-1} = \overline{a}^{\,\varphi(n)-1}$.

Si $\overline{a}$ n'est pas inversible, l'équation a des solutions s'il existe $x \in \mathbb{Z}$, $k \in \mathbb{Z}$ tels que $ax + kn = b$, c'est-à-dire si $b \in \mathbb{Z}a + \mathbb{Z}n = d\mathbb{Z}$ où d est le pgcd de a et n. Donc le problème a des solutions si et seulement si $d|b$. Si cette condition est vérifiée, alors $a = da_1$, $n = dn_1$, $b = db_1$. On cherche alors x et k tels que $a_1 x + kn_1 = b_1$ avec $a_1 \wedge n_1 = 1$, situation étudiée précédemment...

b) Si $b = -1$, 0 ou 1, la résolution est immédiate. Quitte à changer les signes on peut supposer $b \geqslant 2$. Résoudre l'équation revient à résoudre $ax \equiv c \pmod b$, étudiée en a).

c) On a $522 \wedge 2214 = 18$ et $522 \times 17 - 2214 \times 4 = 18$ (11-4, ex. 1). Puisque $b = 36 \in 18\mathbb{Z}$, l'équation a des solutions. En divisant par 18, elle équivaut à $29x + 123y = 2$ et on a $29 \times 17 - 123 \times 4 = 1$ donc 17 est l'inverse de 29 module 123. On a donc

$29x \equiv 2 \pmod{123} \;\Leftrightarrow\; x \equiv 2 \times 17 = 34 \pmod{123} \;\Leftrightarrow\; \exists k \in \mathbb{Z},\ x = 34 + 123k$.

On reporte cette valeur dans $29x + 123y = 2$. On obtient $y = -8 - 29k$, d'où l'ensemble des solutions $\{(34 + 123k, -8 - 29k)\ ;\ k \in \mathbb{Z}\}$.

12.2 Théorèmes de Fermat-Euler et de Wilson

Proposition. (Fermat)

Soit $p \in \mathbb{N}$ premier. Pour tout $x \in \mathbb{Z}$ on a $x^p \equiv x \pmod p$.

Démonstration. $K = \mathbb{Z}/p\mathbb{Z}$ est un corps. Le groupe $K_* = \{\overline{1}, \ldots, \overline{p-1}\}$ de ses unités est d'ordre $p-1$. Le th. de Lagrange montre que $\overline{x}^{p-1} = \overline{1}$ pour tout $\overline{x} \in K_*$. On a donc $\overline{x}^p = \overline{x}$ pour tout $\overline{x} \in K$, y compris pour $\overline{x} = \overline{0}$. ∎

Corollaire. (Wilson)

Pour que $p > 2$ soit un nombre premier, i1 faut et il suffit que

$$(p-1)\,! \equiv -1 \pmod{p}\,.$$

Démonstration. Supposons p premier. Si $p = 2$, alors on a $(p-1)\,! = 1 \equiv -1 \pmod{2}$. Supposons $p \geqslant 3$. D'après le th. de Format, le polynôme $X^{p-1} - \overline{1}$ admet pour racines $\overline{1}, \ldots, \overline{p-1}$ dans le corps $K = \mathbb{Z}/p\mathbb{Z}$. Il se factorise donc sous la forme :

$$X^{p-1} - \overline{1} = (X - \overline{1})(X - \overline{2})(X - \overline{(p-l)})\,.$$

L'égalité des termes constants donne :

$$-\overline{1} = (-1)^{p-1}\overline{1} \times \overline{2} \times \cdots \times \overline{(p-l)} \quad \text{d'où} \quad -1 \equiv (p-1)\,! \pmod{p}\,.$$

Réciproquement si on a $(p-1)\,! \equiv -1 \pmod{p}$, aucun entier k tel que $1 < k < p$ ne peut diviser p, sinon étant diviseur de $(p-1)\,!$ il diviserait 1. Donc p est premier. ∎

Proposition 2. (Fermat-Euler)

Soit $n \geqslant 2$ entier. Pour tout $k \in \mathbb{Z}$, premier avec n, on a $k^{\varphi(n)} \equiv 1 \pmod{n}$.

Démonstration. Cette généralisation du th. de Fermat, due à Euler, se démontre de la même façon. Le groupe $(\mathbb{Z}/n\mathbb{Z})._*$ est d'ordre $\varphi(n)$. D'après le th. de Lagrange, pour tout k inversible, c'est-à-dire tel que $k \wedge n = 1$, on a $\overline{k}^{\varphi(n)} = \overline{1}$. ∎

Exercice 1. Quel est le chiffre des unités de $N = 27^{1995}$.

Solution. Nous voulons connaître le reste de la division par 10 de ce nombre. On a $27 \equiv 7 \pmod{10}$ et donc $N \equiv 7^{1995} \pmod{10}$. On a $\varphi(10) = \varphi(2)\varphi(5) = 4$. Comme $7 \wedge 10 = 1$, le th. de Fermat-Euler donne $7^4 \equiv 1 \pmod{10}$. Par division $1995 = 4q + 3$. On a donc $N \equiv 7^{4q+3} = [(7^4)^q]7^3 \equiv 7^3 \equiv 49 \times 7 \equiv 3$. Le chiffre des unités de N est 3.

Exercice 2. a) Soit K un corps fini commutatif. Montrer que le produit des éléments de K_* est -1 (généralisation du th. de Wilson).

b) Soit $p = 2k+1$ un nombre premier congru à 3 $(\bmod 4)$. Montrer que le produit N des nombres $x^2 + y^2$, où $0 \leqslant x \leqslant 2k$, $1 \leqslant y \leqslant k$ est congru à 1 $(\bmod p)$.

Solution. a) Sur le corps K, le polynôme $X^2 - 1$ a deux racines évidentes 1 et -1 (avec $-1 = 1$ si et seulement si caract$(K) = 2$). Sur un corps un polynôme de degré 2 a au plus 2 racines donc 1 et -1 sont les seuls éléments de K_* tels que $x^{-1} = x$. Si on regroupe les autres éléments de K_* par couples $\{x, x^{-1}\}$ inverses, on voit que le produit de ces éléments est 1. Le produit de tous les éléments de K_* est donc -1.

b) L'expression, produit d'entiers sommes de deux carrés, nous oriente vers l'anneau $A = \mathbb{Z} + i\mathbb{Z}$ des entiers de Gauss. D'après 11-6, cor. 1, si $p \equiv 3 \pmod{4}$, alors p est

irréductible dans A, le quotient $K = A/pA$ est un corps possédant p^2 éléments, classes de $x+iy$, où $0 \leqslant x \leqslant p-1 = 2k$ et $0 \leqslant y \leqslant p-1 = 2k$ ou encore $-k \leqslant y \leqslant k$. D'après a), le produit de toutes les classes non nulles est -1. Pour $y = 0$, on obtient pour produit la classe de $1 \times \cdots \times (p-1)$. Dans les autres termes, où $y \neq 0$ en regroupant les termes conjugués, on trouve $\prod(x^2+y^2) = N$. On a donc $N(p-1)\,! = -1 + (\alpha + i\beta)p$, où $(\alpha + i\beta) \in A$. On a nécessairement, $\beta = 0$. D'après le th. de Wilson, $(p-1)\,! \equiv -1 \pmod p$ donc $N \equiv 1 \pmod p$.

Notons que si $p \equiv 1 \pmod 4$, on a $N \equiv 0 \pmod p$ car $p = a^2 + b^2$ avec $0 < a. < b$ et donc $a < \sqrt{p} < \frac{p-1}{2} = k$. Le produit N contient donc $a^2 + b^2 = p$.

Exercice 3. Soient $p \geqslant 3$ premier, $x_1, \ldots, x_{p-1} \in \mathbb{Z}$ non divisibles par p. Notons Ω l'ensemble $\{-1, 1\}^{p-1}$ des $\omega = (\varepsilon_1, \ldots, \varepsilon_{p-1})$ où $\varepsilon_i = \pm 1$ pour tout i.

a) Démontrer la formule de C. Pop :

$$(1) \quad \sum_{\omega \in \Omega} \varepsilon_1 \cdots \varepsilon_{p-1}(\varepsilon_1 x_1 + \cdots + \varepsilon_{p-1}x_{p-1})^{p-1} = (p-1)\,!\, 2^{p-1} x_1 \cdots x_{p-1}\,.$$

b) Montrer que l'un des nombres $\varepsilon_1 x_1 + \cdots + \varepsilon_{p-1}x_{p-1}$ est divisible par p.

Solution. a) $\varepsilon_1 \cdots \varepsilon_{p-1}(\varepsilon_1 x_1 + \cdots + \varepsilon_{p-1}x_{p-1})^{p-1}$

$$= \sum_{i_1 + \cdots + i_{p-1} = p-1} \varepsilon_1 \cdots \varepsilon_{p-1} \frac{(p-1)\,!}{i_1\,! \cdots i_{p-1}\,!}\, \varepsilon_1^{i_1} \cdots + \varepsilon_{p-1}^{i_{p-1}} x_1^{i_1} \cdots x_{p-1}^{i_{p-1}}\,.$$

En regroupant au premier membre de (1) tous les termes contenant $x_1^{i_1} \cdots x_{p-1}^{i_{p-1}}$, celui-ci est multiplié par $\sum_{w \in \Omega} \varepsilon_1^{i_1+1} \cdots + \varepsilon_{p-1}^{i_{p-1}+1}$. Quand on somme ce terme par rapport à ε_1, les autres ε_i étant fixés, on obtient zéro si $i_1 + 1$ est impair. De même ensuite pour les sommations par rapport à $\varepsilon_2, \ldots, \varepsilon_{p-1}$. Les seuls termes restant sont ceux pour lesquels $i_k + 1$ est pair, soit i_k impair, pour tout $k = 1, \ldots, p-1$. Comme $i_1 + \cdots + i_{p-1} = p-1$, nécessairement, $i_1 = \cdots = i_{p-1} = 1$. Pour le terme correspondant on a :

$$\sum_{\omega \in \Omega} \varepsilon_1^{i_1+1} \cdots + \varepsilon_{p-1}^{i_{p-1}+1} = \sum_{\omega \in \Omega} 1 = \operatorname{card}(\Omega) = 2^{p-1} \quad , \quad \frac{(p-1)\,!}{1\,! \cdots 1\,!} = (p-1)\,!$$

et $x_1^{i_1} \cdots x_{p-1}^{i_{p-1}} = x_1 \cdots x_{p-1}$, d'où la formule.

b) Raisonnons par l'absurde. Supposons qu'aucun des nombres $\varepsilon_1 x_1 + \cdots + \varepsilon_{p-1}x_{p-1}$ n'est divisible par p. On a $(\varepsilon_1 x_1 + \cdots + \varepsilon_{p-1}x_{p-1})^{p-1} \equiv 1 \pmod p$ d'après le th. de Fermat. Le premier membre de la formule est congru à $\sum_{\omega \in \Omega} \varepsilon_1 \cdots \varepsilon_{p-1} = 0$. Au second membre, on a $2^{p-1} \equiv 1$ (th. de Fermat), $(p-1)\,! \equiv -1$ (th. de Wilson) et $x_1 \cdots x_{p-1} \not\equiv 0$ car $\mathbb{Z}/p\mathbb{Z}$ est un corps. C'est absurde. Donc p divise l'un des termes.

Application à la cryptographie. En 1975, W. Diffie et M. E. Hellman, professeurs à Stanford University démontraient l'existence de codages qui demanderaient des centaines d'années de calcul sur ordinateurs pour être déchiffrés par un intercepteur. En 1977, R. L. Rivest, A. Shamir, L. Adleman du MIT eurent l'idée de réaliser effectivement un tel codage, dit RSA, en s'appuyant sur le fait que pour calculer les facteurs premiers p, q, d'un nombre $N = pq$ donné (où p, q sont premiers inconnus) il faut des dizaines ou des centaines d'années de calcul sur ordinateur si p, q ont environ 100 chiffres dans leur expression décimale.

Supposons qu'un réseau E de personnes veuille communiquer secrètement. Le chef du réseau choisit deux ou trois nombres premiers $p_1 \ldots p_r$, distincts, très grands (plus de 100 chiffres par exemple) et calcule $N = p_1 \cdots p_r$ et $\varphi(N)$. Pour chaque membre A du réseau, il choisit $e_A \in \mathbb{Z}$ premier avec $\varphi(N)$ et il détermine $d_A \in \mathbb{N}$ tel que $e_A d_A \equiv 1$

modulo $\varphi(N)$ (par exemple en calculant par l'algorithme d'Euclide une relation de Bezout entre e_A et $\varphi(N)$). Il garde secret $\varphi(N)$ et publie dans un annuaire transmis aux membres du réseau, N et la liste des codes expéditeurs e_A des divers membres (clés publiques). Par contre, chacun conserve, connu de lui seul, son code confidentiel d_A.

Voici comment fonctionnera le réseau de communication. Si A veut expédier un message M à B, il remplace les caractères de M par les nombres qui les codent, par exemple $a \leftarrow 1, b \leftarrow 2, \ldots$ Pour des textes longs, on les découpe en suites de chiffres de longueurs inférieures à 100. Cette suite M est un nombre premier avec N.

L'expéditeur A calcule le reste X modulo N de M^{e_B}. Il le transmet à B. Quand B le reçoit, il calcule le reste modulo N de $X^{d_B} \equiv M^{e_B d_B}$. C'est le message M, pour la raison suivante : puisque $e_B d_B \equiv 1 \pmod{\varphi(N)}$, il existe $k \in \mathbb{Z}$ tel que $e_B d_B = 1 + k\varphi(N)$ et on a $M^{e_B d_B} = M[M^{\varphi(N)}]^k \equiv M$ d'après le th. de Fermat-Euler.

Notons que si A veut signer son message, l'authentifier, il lui suffit de chiffrer son nom. Si Y_A est le nombre obtenu, il transmet le reste modulo N de $Y_A^{d_A} = Z$. Le receveur calculera le reste de Z^{e_A} modulo N. Ce sera la signature Y_A.

C'est sur ce principe que fonctionnent les cartes bancaires et leurs codes Le chef de réseau est la banque. Le code secret de la carte d_A est connu du seul titulaire. Par la procédure que nous venons de décrire, la banque vérifie que l'identité de la personne est bien conforme à celle qui est lue sur la carte bancaire.

L'utilisation d'un codage RSA suppose que l'on sache déterminer des nombres premiers grands. Pour ce faire une idée sur la primalité d'un grand nombre impair n, on pourra le diviser par les entiers impairs jusqu'à une valeur assez petite pour que le volume des calculs soit raisonnable. Si n n'est divisible par aucun de ces nombres, on examinera si $2^{n-1}, 3^{n-1}$ sont divisibles par n (sur un ordinateur, vérifier si $a^{n-1} - 1$ est divisible par n n'est pas difficile, même quand n est très grand). Si c'est le cas, sans avoir une certitude, il sera assez probable que n est premier. On pourra alors entreprendre une vérification systématique de la divisibilité par les entiers premiers inférieurs à $\sqrt{n}$.

12.3 Résidus quadratiques

Définition.

Soit p un nombre premier. On dit que $k \in \mathbb{Z}$ est un résidu quadratique modulo p s'il existe $x \in \mathbb{Z}$ tel que $k \equiv x^2 \pmod{p}$.

Cela signifie que $\overline{k}$ est un carré dans le corps $\mathbb{Z}/p\mathbb{Z}$. La résolution d'équations de congruences du second degré

$$ak^2 + bk + c \equiv 0 \pmod{p}.$$

où $a, b, c \in \mathbb{Z}$ sont donnés, équivaut à résoudre, sur le corps $K = \mathbb{Z}/p\mathbb{Z}$, l'équation

$$\overline{a}X^2 + \overline{b}X + \overline{c} = \overline{0}.$$

Supposons $p \neq 2$. Si $\overline{a} \neq \overline{0}$, le trinôme prend la forme canonique

$$\overline{a}\left(\left(X - \frac{\overline{b}}{2\overline{a}}\right)^2 - \frac{\overline{b}^2}{4\overline{a}^2} + \frac{\overline{c}}{\overline{a}}\right) = \overline{a}\left(\left(X - \frac{\overline{b}}{2\overline{a}}\right)^2 - \frac{\overline{b}^2 - 4\overline{ac}}{4\overline{a}^2}\right).$$

Le trinôme aura des racines si $\Delta = \overline{b}^2 - 4\overline{ac}$ est un carré a^2. Un corps étant intègre, $(X - \alpha)(X + \alpha)$ a alors deux racines α et $-\alpha$ dans $\mathbb{Z}/p\mathbb{Z}$. L'équation de congruence a deux classes de solutions modulo p. Il est utile de caractériser les carrés dans $\mathbb{Z}/p\mathbb{Z}$.

Proposition. (Euler)

Soit $p > 2$ un nombre premier. Considérons $\overline{x} \in \mathbb{Z}/p\mathbb{Z}$ distinct de $\overline{0}$.

(i) *$\overline{x}$ est un carré si et seulement si $x^{\frac{p-1}{2}} \equiv 1 \pmod p$.*

(ii) *Si $\overline{x}$ n'est pas un carré on a $x^{\frac{p-1}{2}} \equiv -1 \pmod p$.*

Démonstration. Puisque $K = \mathbb{Z}/p\mathbb{Z}$ est un corps, le groupe K_* est cyclique (10-7, cor.1). Son ordre $p-1$ pair est divisible par 2. D'après 3-3, prop., il existe dans K_* un unique sous-groupe d'ordre $m = \frac{p-1}{2}$ à savoir :

$$\{\overline{x} \in K_* \mid \exists\, \overline{y} \in K_* \quad \overline{y}^2 = \overline{x}\} = \{\overline{x} \in K_* \mid \overline{x}^{\frac{p-1}{2}} = \overline{1}\}.$$

ce qui prouve l'assertion (i).

(ii) De même, K_* possède un unique sous-groupe d'ordre 2, qui est $\{\overline{1}, -\overline{1}\}$ donc

$$\{\overline{1}, -\overline{1}\} = \{\overline{x} \in K_* \mid \overline{x}^2 = \overline{1}\} = \{\overline{x} \in K_* \mid \exists \overline{y} \in K_* \quad \overline{y}^{\frac{p-1}{2}} = \overline{x}\}.$$

ce qui montre que $\overline{y}^{\frac{p-1}{2}}$ est égal à $\overline{1}$ ou $-\overline{1}$ pour tout $\overline{y} \in K_*$. Compte tenu de (i), $\overline{y}^{\frac{p-1}{2}} = -\overline{1}$ si et seulement si $\overline{y}$ n'est pas un carré. ∎

Définition.

Soient p un nombre premier impair et $a \in \mathbb{N}$. On appelle symbole de Legendre le nombre $\left(\frac{a}{p}\right)$ égal à 0 si p divise a, égal sinon à 1 ou -1 selon que a est un résidu quadratique modulo p ou non.

Exercice 1. Soit p premier.
a) Si p est de la forme $3k+1$, montrer que les cubes de $(\mathbb{Z}/p\mathbb{Z})_*$ sont caractérisés par la condition $\overline{x}^k = \overline{1}$. Généraliser.
b) Si $m \wedge (p-1) = 1$, combien $\overline{y} \in (\mathbb{Z}/p\mathbb{Z})$ a-t-il de racines $m^{\text{èmes}}$ dans $(\mathbb{Z}/p\mathbb{Z})_*$?

Solution. a) Si $p = 3k+1$ est premier, k divise l'ordre du groupe cyclique $(\mathbb{Z}/p\mathbb{Z})_*$. Il existe donc dans ce groupe un unique sous-groupe H d'ordre k, soit :

$$H = \{\overline{x} \in (\mathbb{Z}/p\mathbb{Z})_* \mid \exists\, \overline{y} \in (\mathbb{Z}/p\mathbb{Z})_* \quad \overline{y}^3 = \overline{x}\} = \{\overline{x} \in (\mathbb{Z}/p\mathbb{Z})_* \mid \overline{x}^{\frac{p-1}{3}} = \overline{1}\}.$$

Généralisons. Si $p = ak+1$ est premier, les éléments $\overline{x} \in (\mathbb{Z}/p\mathbb{Z})_*$ qui sont des puissances $a^{\text{èmes}}$ sont ceux qui vérifient $\overline{x}^k = \overline{1}$. Plus généralement, si K est un corps fini commutatif, dont le cardinal est de la forme $ak+1$, la même caractérisation existe.

b) Si $m \wedge (p-1) = 1$, $\overline{x} \mapsto \overline{x}^m$ est un automorphisme du groupe cyclique $(\mathbb{Z}/p\mathbb{Z})_*$ (3-2, cor.2). Tout $\overline{y} \in (\mathbb{Z}/p\mathbb{Z})_*$ a une unique racine $m^{\text{ème}}$ dans $(\mathbb{Z}/pz)_*$. Si $\overline{y} = \overline{0}$, c'est encore vrai car un corps est intègre.

Exercice 2. Pour quels $p > 2$ premiers, -1 est-il un résidu quadratique ? Soit $n \in \mathbb{N}$. Montrer que tout facteur premier impair de n^2+1 est de la forme $4k+1$.

Solution. $(-\overline{1})^{\frac{p-1}{2}} = \overline{1} \quad \Leftrightarrow \quad \exists k \in \mathbb{Z} \quad \frac{p-1}{2} = 2k \quad \Leftrightarrow \quad \exists k \in \mathbb{Z} \quad p = 4k+1.$

Ainsi, $X^2 + \overline{1}$ est irréductible dans $(\mathbb{Z}/p\mathbb{Z})[X]$ si et seulement si p est de la forme $4k+3$. Si $p = 2$ ou si p est de la forme $4k+1$, alors $X^2+\overline{1}$ est produit de deux facteurs de degré un. Cela recoupe ce que nous avons vu dans l'anneau des entiers de Gauss : on a alors $p = a^2 + b^2$, avec $a \neq 0$ et $b \neq 0$ car p est premier. Dans $\mathbb{Z}/p\mathbb{Z}$, on a $\left(\overline{a}(\overline{b})^{-1}\right)^2 = -\overline{1}$. (Voir aussi 10-7, ex.)

p est facteur premier de n^2+1, si $\overline{n}^2 = -\overline{1}$ dans $\mathbb{Z}/p\mathbb{Z}$, soit si $p \equiv 1 \pmod 4$.

12.4 Nombres premiers

Il existe un algorithme (le crible d'Eratosthène) pour déterminer dans $\mathbb{N}$ la suite des nombres premiers inférieurs à un nombre donné N. Il consiste à rayer dans la liste $1, \ldots, N$ les multiples de 2, puis de 3 et ainsi de suite. Quand on rencontre un entier qui n'est pas encore rayé, il est premier. On supprime ses multiples de la liste et alors apparaît, non rayé, le nombre premier suivant.

Exercice 1. Vérifier que 401 est un nombre premier.

Solution. Inutile d'écrire les 401 premiers entiers et d'appliquer le crible d'Eratosthène : si $n > 2$ est composé, il existe $a \leqslant b$ tels que $n = ab$, d'où $a \leqslant \sqrt{n}$. Il suffit d'examiner si les nombres premiers $p \leqslant E(\sqrt{n})$) divisent n. Pour n = 401, il suffit de considérer les nombres premiers $p < 20$. Pour 2, 3, 5, 7, 11, 13 les critères donnés en 12-1 échouent. Or 17, 19 ne divisent pas 401 car $401 = 2 \times 20 + 1$ est congru à $2 + 1 = 3$ modulo 19 et à $2 \times 3 + 1 = 7$ modulo 17. Donc 401 est premier.

Théorème 1. (Euclide)

L'ensemble $\mathcal{P}$ des nombres premiers est infini.

Démonstration. Supposons $\mathcal{P}$ fini, d'éléments $p_0, \ldots, p_k$. D'après 11-4 ou 11-5, $N = (p_0 p_1 \cdots p_k) + 1$ possède un facteur premier p. Or p ne peut être dans la liste $p_0, \ldots, p_k$ sinon divisant N et $(p_0 p_1 \cdots p_k)$, il diviserait leur différence 1. C'est absurde. ∎

Exercice 2. En adaptant le raisonnement d'Euclide montrer qu'il existe une infinité de nombres premiers de la forme $3k + 2$.

Solution. Raisonnons par l'absurde. A part 3, aucun nombre de la forme $3k$ n'est premier. Tout nombre premier $p > 3$ est donc congru à 1 ou à 2 modulo 3. Supposons qu'il n'existe qu'une famille finie $\{p1, \ldots, p_k\}$ de nombres premiers de la forme $3k + 2$. Posons $N = (p_1 \cdots p_k)^2 + 1$. Modulo 3 on a $(p_1 \cdots p_k)^2 \equiv 1$ et $N \equiv 2$. Donc 3 ne divise pas N. Si la décomposition en facteurs premiers $N = q_1 \cdots q_m$ ne comprenait que des facteurs de la forme $3k + 1$, on aurait $N \equiv 1$. Donc, au moins un des facteurs premiers q_i de N est de la forme $3k + 2$. Ce nombre q_i est distinct de $p_1, \ldots, pk$ car ces nombres ne divisent pas N. L'hypothèse faite est donc absurde.

Théorème 2. (Euler)

La série $\sum \frac{1}{p}$ des inverses des nombres premiers est divergente.

Démonstration. Raisonnons par l'absurde. Notons $p_1 < \cdots < p_m < \cdots$ la suite infinie des nombres premiers. Supposons que la série $\sum_{m=1}^{\infty} \frac{1}{p_m}$ converge. Il existerait alors $k \in \mathbb{N}^*$ tel que $\sum_{m=k+1}^{\infty} \frac{1}{p_m} < \frac{1}{2}$. Pour tout $x \in N^*$, partageons $\{n \in \mathbb{N}^* \mid n \leqslant x\}$ en deux classes :
- l'ensemble A_x des n dont tous les facteurs premiers appartiennent à $\{p_1, \ldots, p_k\}$,
- l'ensemble B_x des n qui possèdent au moins un facteur premier p_m avec $m \geqslant k + 1$.

Soit $n \in B_x$, tel que p_{k+1} divise n. On a $p_{k+1} \leqslant n$. Puisque $n \leqslant x$, il existe au plus $\frac{x}{p_{k+1}}$ éléments de ce type dans B_x. De même, il existe au plus $\frac{x}{p_{k+2}}$ éléments de B_x divisibles par p_{k+2}, etc. On a donc :

$$\text{card}\,(B_x) \leqslant \frac{x}{p_{k+1}} + \frac{x}{p_{k+2}} + \cdots < \frac{x}{2}\,.$$

Les éléments de A_x, sont des entiers $n \leqslant x$ ayant une décomposition en facteurs premiers de la forme $n = p_1^{a_1} \cdots p_k^{a_k}$. Si on fait apparaître le plus grand carré possible, on obtient $n = m^2 p_1^{\alpha_1} \cdots p_k^{\alpha_k}$ où $\alpha_i = 0$ ou 1 pour $i = 1, \ldots, k$. Pour construire un élément n de A_x, on doit donc donner m avec $m^2 \leqslant n \leqslant x$, d'où $m \leqslant \sqrt{x}$, et la suite $\alpha_1, \ldots, \alpha_k$ dans $\{0, 1\}$, ce qui laisse 2^k possibilités. Finalement, pour tout $x \in \mathbb{N}$ on obtient,

$$x = \text{card}\,(A_x) + \text{card}\,(B_x) \leqslant \frac{x}{2} + \sqrt{x}\,2^k \quad \text{d'où} \quad \sqrt{x} \leqslant 2^{k+1}\,.$$

C'est absurde car la fonction $x \mapsto \sqrt{x}$ n'est pas bornée sur $\mathbb{N}$. ∎

12.5 Nombres de Mersenne, nombres de Fermat

En 1640, Fermat avait affirmé, tout en précisant qu'il ne pouvait pas le prouver, que tous les nombres F_k, de la forme $2^{2^k} + 1$ devaient être premiers. C'est bien le cas pour $k = 1, 2, 3, 4$. Au siècle suivant, Euler montra que $F_5 = 2^{2^5} + 1$ n'est pas premier. Actuellement, on ignore s'il existe d'autres nombres de Fermat premiers en dehors de F_1, F_2, F_3, F_4 (mais pour $5 \leqslant k \leqslant 20$ l'utilisation de l'ordinateur a permis de vérifier qu'ils ne sont pas premiers).

Pour construire de grands nombres premiers, Mersenne, contemporain de Fermat, avait suggéré de considérer les nombres $M_r = 2^r - 1$ avec r appartenant à l'ensemble $\mathcal{P}$ des nombres premiers. On ne peut espérer que M_r soit toujours premier puisque $M_{11} = 2047 = 23 \times 87$ mais Mersenne avait montré que M_r est premier pour $r = 2, 3, 5, 7, 13, 17, 19, 31, 127$, oubliant certaines valeurs de r inférieures à 127, à savoir 61, 89, 109. Généralisons la notion de nombre de Mersenne.

Proposition.

Soit $r \in \mathcal{P}$.

(i) *Tous les facteurs premiers de M_r sont de la forme $kr + 1$ où $k \in \mathbb{N}$.*

(ii) *Plus généralement, considérons $x, y \in \mathbb{Z}$ distincts. Tout facteur premier de $y^r - x^r$ est soit un facteur premier de $y - x$, soit de la forme $kr + 1$ où $k \in \mathbb{N}$.*

(iii) *Pour tout $x \in \mathbb{Z}$, tout facteur premier de $(x+1)^r - x^r$ est de la forme $kr + 1$. Inversement, pour tout $p \in \mathcal{P}$ de la forme $kr + 1$, il existe $x \in \mathbb{Z}$ tel que p soit un facteur premier de $(x+1)^r - x^r$.*

Démonstration. Soit p un facteur premier de $2^r - 1$. Dans $\mathbb{Z}/p\mathbb{Z}$ on a $\overline{2}^r = \overline{1}$. Il en résulte que l'ordre de $\overline{2} \in (\mathbb{Z}/p\mathbb{Z})_*$ divise r. Comme r est premier, $\overline{2}$ est d'ordre r. D'après le th. de Lagrange, cet ordre divise l'ordre $p - 1$ du groupe $(\mathbb{Z}/p\mathbb{Z})_*$.

(ii) Considérons $x, y \in \mathbb{Z}$ et un facteur premier p de $y^r - x^r$. Dans $\mathbb{Z}/p\mathbb{Z}$ on a $\overline{y}^r = \overline{x}^r$. Ecartons le cas où $\overline{y} = \overline{x}$, c'est-à-dire où p divise $y - x$. On ne peut avoir $\overline{x} = \overline{0}$ car $\mathbb{Z}/p\mathbb{Z}$ étant un corps, on aurait également $\overline{y} = \overline{0}$. De même, $\overline{y} \neq \overline{0}$. Dans le groupe $(\mathbb{Z}/p\mathbb{Z})_*$ on a $\left(\overline{y}(\overline{x})^{-1}\right)^r = \overline{1}$, avec $\overline{y}(\overline{x})^{-1} \neq \overline{1}$. Comme en (i), on voit que l'ordre de $\overline{y}(\overline{x})^{-1}$ est r. Donc r divise l'ordre $p - 1$ du groupe $(\mathbb{Z}/pz)_*$ d'après le th. de Lagrange.

(iii) D'après (ii), tout facteur premier de $(x+1)^r - x^r$ est de la forme $kr + 1$. Comme $\mathbb{Z}/p\mathbb{Z}$ est un corps, $(\mathbb{Z}/pz)_*$ est un groupe cyclique d'ordre $p - 1$. Puisque r divise

$p-1$ il existe dans $(\mathbb{Z}/p\mathbb{Z})_*$ un unique sous-groupe H d'ordre r. D'après 3-3, prop., H est cyclique. Soit $h \in H$ d'ordre r et posons $\overline{x} = (\overline{h} - \overline{1})^{-1}$. Alors $\overline{h} = (\overline{x}+\overline{1})\overline{x}^{-1}$ est d'ordre r. Tout $x \in \mathbb{Z}$ représentant de $\overline{x}$ sera tel que p divise $(x+1)^r - x^r$. ∎

Exercice 1. Soient $r \in \mathcal{P}$, $r' \in \mathcal{P}$ distincts. Montrer que pour tout $x \in \mathbb{Z}$, les facteurs premiers de $(x+1)^r - x^r$ et de $(x+1)^{r'} - x^{r'}$ sont deux familles disjointes. En particulier, les nombres de Mersenne M_r et $M_{r'}$ sont premiers entre eux.

Solution. S'il existait $p \in \mathcal{P}$ tel que $(\overline{x}+\overline{1})^r = \overline{x}^r$ et $(\overline{x}+\overline{1})^{r'} = \overline{x}^{r'}$ dans $\mathbb{Z}/p\mathbb{Z}$, en utilisant la relation de Bezout $ru + r'v = 1$, on obtiendrait $(\overline{x}+\overline{1})^{ru} = \overline{x}^{ru}$ et $(\overline{x}+\overline{1})^{r'v} = \overline{x}^{r'v}$ d'où, en multipliant membre à membre, $\overline{x}+\overline{1} = \overline{x}$ ce qui est absurde.

Exercice 2. Soit $r \in \mathcal{P}$. Montrer que l'ensemble E des nombres premiers de la forme $kr+1$, où $k \in \mathbb{N}$, est infini.

Solution. D'après la proposition, E est non vide. Supposons E fini, d'éléments $p_1, \ldots, p_k$. Posons $x = p_1 \cdots p_k$ et $n = (x+1)^r - x^r$. Tout facteur premier q de n est de la forme $kr+1$ et donc élément de E. Or, q est distinct de $p_1, \ldots, p_k$, qui ne sont pas des diviseurs de n. C'est absurde.

Exercice 3. (Test de Lucas-Lehmer) Considérons $u = 2+\sqrt{3}$, $v = 2-\sqrt{3}$. Pour tout $n \in \mathbb{N}$ posons $s_n = u^{2^n} + v^{2^n}$.

a) Montrer que (s_n) est une suite d'entiers et que $s_{n+1} = s_n^2 - 2$.

b) Montrer que si le nombre de Mersenne M_p divise s_{p-2} alors M_p est premier.

Solution. a) On a $u^m + v^m = \sum_{k=0}^{m} C_m^k 2^{m-k}[(\sqrt{3})^k + (-1)^k + (\sqrt{3})^k]$ pour tout $m \in \mathbb{N}$. Pour k impair, le crochet est nul et pour k pair c'est un entier donc s_n, est un entier. Comme $uv = 1$ on a $s_n^2 = u^{2^{n+1}} + v^{2^{n+1}} + 2 = s_{n+1} + 2$.

b) Raisonnons par l'absurde. Si M_p, n'est pas premier, il existe $q \in \mathcal{P}$ qui divise M_p avec $q \leqslant \sqrt{M_p}$, soit $q^2 \leqslant 2^p - 1$. Par hypothèse, M_p divise s_{p-2}. Il existe donc $k \in \mathbb{N}$ tel que $s_{p_2} = u^{2^{p-2}} + v^{2^{p-2}} = qk$, d'où en multipliant par $u^{2^{p-2}}$,

$$u^{2^{p-1}} + 1 = qku^{2^{p-2}}. \tag{1}$$

Les deux membres appartiennent à l'anneau $A = \mathbb{Z}\sqrt{3}$ Considérons l'idéal qA et l'anneau quotient $B = A/qA$. Soit α la classe de $\sqrt{3}$ dans B. On a $\alpha \neq 0$. Les éléments de B sont $\overline{x} + \overline{y}\alpha$ où $\overline{x}$, $\overline{y}$ sont dans l'ensemble des classes $\overline{0}, \ldots, \overline{q-1}$. Donc B possède q^2 éléments. D'après (1), $\overline{u}^{2^{p-1}} = -\overline{1}$ donc $\overline{u} \in B_*$ est d'ordre 2^p. Le th. de Lagrange montre que $2^p | [B_* : 1] \leqslant q^2 - 1 \leqslant 2^p - 2$, absurde. Donc M_p est premier. (La réciproque est vraie : si M_p est premier, on montre que $M_p | s_{p-2}$.)

Remarque. Depuis Mersenne, les nombres de Mersenne ont fourni les plus grands nombres premiers connus. Actuellement, avec la puissance des ordinateurs, on peut appliquer le critère de Lucas (1878) à M_r jusqu'à de très grandes valeurs de r. En nov. 97, le 36^e nombre de Mersenne premier a été découvert. C'était le plus grand nombre premier connu à cette date. Mais on ne sait pas si l'ensemble des $r \in \mathcal{P}$ pour lesquels M_r est premier, est infini. On ne sait pas davantage si son complémentaire est infini.

12.6 Un pas vers le théorème de Dirichlet

Proposition. (Cas particulier du th. de Dirichlet)

Considérons un entier $a \geqslant 2$ et le polynôme cyclotomique $\Phi_a(X)$.

(i) *Pour tout $n \in \mathbb{Z} \setminus \{-1, 0, 1\}$ les facteurs premiers de $\Phi_a(n)$ sont soit des facteurs premiers de a, soit de la forme $ka + 1$, où $k \in \mathbb{N}$.*

(ii) *Il existe une infinité de nombres premiers de la forme $ka + 1$.*

(iii) *Pour tout nombre premier p de la forme $ka + 1$, il existe $n \in \mathbb{Z}$ tel que p soit facteur premier de $\Phi_a(n)$.*

Démonstration. D'après 10-6, prop., on a $\Phi_a(n) \in \mathbb{Z}$ car $\Phi_a(X) \in \mathbb{Z}[X]$ et $\Phi_a(n) \geqslant 2$. Soit p un facteur premier de $\Phi_a(n) = n^{\varphi(a)} + \cdots + 1$. Dans $\mathbb{Z}/p\mathbb{Z}$ on a $\Phi_a(\overline{n}) = \overline{0}$ donc $\overline{n}$ est racine de $X^a - \overline{1}$. Si la caractéristique p du corps $\mathbb{Z}/p\mathbb{Z}$ ne divise pas a, alors $\overline{n}$ engendre un sous-groupe cyclique d'ordre $a$de $(\mathbb{Z}/p\mathbb{Z})_*$ (10-7, prop. D'après le th. de Lagrange, a divise $[(\mathbb{Z}/p\mathbb{Z})_* : l] = p - 1$ donc p est de la forme $ka + 1$.

(ii) Soit $F = \{q_1, \ldots, q_m\}$ l'ensemble des facteurs premiers de a. Supposons que l'ensemble E des nombres premiers de la forme $ka + 1$ soit fini, d'éléments $p_1, \ldots, p_s$. Considérons $n = (q_1 \cdots q_m)p_1 \cdots p_s$. D'après 10-6, prop., on a $\Phi_a(n) \geqslant 2$ et $\Phi_a(n) \equiv 1$ modulo p_i pour tout i et modulo q_J pour tout j (car $\Phi_a(0) = 1$). Soit q un facteur premier de $\Phi_a(n)$. On a $\Phi_a(n) \equiv 0 \pmod{q}$. On a donc $q \notin E$, $q \notin F$. D'après (i), $q \in E$. C'est absurde.

(iii) Considérons le corps $K = \mathbb{Z}/p\mathbb{Z}$. L'ordre $p - 1$ du groupe cyclique K_* est divisible par a. Il existe donc un unique sous-groupe H de K_* d'ordre a et H est cyclique. Soit $n \in \mathbb{Z}$ tel que$\overline{n}$ soit un générateur de H. D'après 10-7, prop., on a $\Phi_a(\overline{n}) = \overline{0}$ ce qui signifie que p divise $\Phi_a(n)$. ∎

Remarque. Plus généralement, DIRICHLET a montré en 1837, en utilisant les fonctions d'une variable complexe, c'est-à-dire l'analyse complexe, le théorème suivant :

Considérons deux entiers $a > 1$ et $b > 0$ deux entiers premiers entre eux. Il existe une infinité de nombres premiers de la forme $ka + b$ où $k \in \mathbb{Z}$.

Les méthodes d'analyse complexe ont permis de résoudre d'autres problèmes difficiles, notamment le suivant. Notons $\pi(x)$ le cardinal de l'ensemble des nombres premiers majorés par $x \in \mathbb{N}$. Gauss et Legendre avaient conjecturé (fin du 18$^{\text{e}}$ siècle) que $\pi(x) \sim \frac{x}{\ln x}$ quand x tend vers $+\infty$. Les travaux de TCHEBYCHEV (1851), de RIEMANN (1859) puis de HADAMARD et DE LA VALLEE POUSSIN ont démontré complètement ce résultat. Il en résulte que $p_k \sim k \ln k$ où p_k désigne le $k^{\text{ième}}$ nombre premier.

Corollaire.

Soit $n \in \mathbb{Z}$ pair. Tout facteur premier de $n^{2^k} + 1$ est de la forme $m2^{k+1} + 1$. Cela s'applique notamment aux nombres de Fermat $F_k = 2^{2^k} + 1$.

Démonstration. Posons $a = 2^{k+1}$ et $\zeta = \exp(i\frac{2\pi}{a})$. Les racines $a^{\text{ième}}$ primitives de l'unité sont de la forme ζ^α, où $\alpha \in \{0, \ldots, a-1\}$ est premier avec 2^{k+1}, c'est-à-dire non divisible par 2. Leur ensemble Λ_a est donc le complémentaire dans $\mathbb{U}_a$ de $\{1, \zeta^2, \zeta^4, \zeta^6, \ldots\} = \mathbb{U}_{\frac{a}{2}}$, d'où l'expression du polynôme cyclotomique $\Phi_{2^{k+1}}(X)$ (voir également 10-6, ex. 2) :

$$\Phi_{2^{k+1}}(X) = \frac{X^a - 1}{X^{a/2} - 1} = X^{a/2} + 1 = X^{2^k} + 1.$$

Ainsi, $F_k = 2^{2^k} + 1 = \Phi_{2^{k+1}}(2)$. D'après la proposition, les facteurs premiers de $\Phi_{2^{k+1}}(n)$ sont soit de la forme $m2^{k+1} + 1$, soit diviseurs de 2^{k+1}, c'est-à-dire égaux à 2. Comme $\Phi_{2^{k+1}}(n)$ est impair quand n est pair, ce dernier cas ne se présente pas. ∎

Exercice 1. Montrer que le nombre F_5 n'est pas premier (dû à Euler).

Solution. Pour $k = 5$, on a $F_5 = 2^{32} + 1 = 4\,294\,967\,297$. D'après le corollaire, pour voir que F_5 n'est pas premier, il suffit d'examiner si les nombres premiers de la forme $m2^6 + 1 = 64m + 1$, inférieurs à $\sqrt{F_5}$, divisent F_5. Modulo 3 on a $64 \equiv 1$. Donc pour $m \equiv 2 \pmod 3$ on a $64m + 1$ divisible par 3, et de ce fait non premier. On a $64 \equiv -1 \pmod 5$ donc pour $m \equiv 1 \pmod 5$, $64m + 1$ est divisible par 5 et de ce fait non premier. Pour $m = 3, 4, 7, 9$ le nombre $64m + 1$ est premier mais ne divise pas F_5. Mais pour $m = 10$, le nombre $10 \times 64 + 1 = 641$ est premier et il divise $F_5 = 641 \times 6\,700\,417$. Donc, contrairement à ce que pensait Fermat, F_5 n'est pas premier.

Exercice 2. Montrer que pour tout $k > 0$, il existe une infinité de nombres premiers dont l'écriture décimale contient k zéros consécutifs.

Solution. D'après la proposition, il existe une infinité de nombres premiers de la forme $m10^{k+1} + 1$ de la forme voulue.

12.7 Equations diophantiennes

Proposition 1.

Pour que $(x, y, z) \in \mathbb{N}^3$ soit solution de l'équation de Diophante

$$x^2 + y^2 = z^2 \,, \tag{1}$$

il faut et il suffit qu'il existe $d \in \mathbb{N}$ et $u, v \in \mathbb{N}_*$ premiers entre eux, tels que (x, y, z) ou (y, x, z), soit égal à $\big(d(u^2 - v^2)\,,\, 2duv\,,\, d(u^2 + v^2)\big)$.

Démonstration. La condition est suffisante car $[d(u^2 - v^2)]^2 + [2duv]^2 = [d(u^2 + v^2)]^2$. Montrons qu'elle est nécessaire. Ecartons les solutions où l'une des variables est nulle, qui sont de la forme indiquée. Si x, y, z vérifient (1), en les divisant par leur pgcd on obtient une autre solution. On peut donc se contenter de chercher les solutions dites *premières* où x, y, z sont premiers dans leur ensemble. Les autres solutions s'obtiendront en les multipliant par un entier $d \in \mathbb{N}^*$.

Soit (x, y, z) une solution première. Alors (x, y, z) sont deux à deux premiers entre eux car un nombre premier qui divise deux des nombres divise l'autre d'après (1). En particulier, il est impossible que deux de ces nombres soient pairs. D'autre part, x et y ne peuvent être impairs tous les deux, sinon on aurait $x^2 \equiv 1 \pmod 4$, $y^2 \equiv 1 \pmod 4$ d'où $z^2 = x^2 + y^2 \equiv 2 \pmod 4$ et alors 2 diviserait z et on obtiendrait $z^2 \equiv 0 \pmod 4$, absurde. En résumé, pour une solution première, on a x impair y pair z impair ou bien x pair y impair z impair. Quitte à changer de notation, nous supposerons x impair et y pair.

Soient (x, y, z) premiers dans leur ensemble. Posons $X = \frac{x}{z}$, $Y = \frac{y}{z}$. Ce couple de rationnels est écrit sous forme réduite, ce qui signifie que les fractions qui expriment

initialement X et Y ont été simplifiées, puis réduites au plus petit dénominateur commun qui est le ppcm des deux dénominateurs. Cette forme réduite est unique.

On a $x^2+y^2=z^2$ si et seulement si $X^2+Y^2=1$. Nous cherchons donc des points de coordonnées rationnelles sur le cercle trigonométrique, plus précisément sur le quart de cercle $X=\frac{x}{z}>0$, $Y=\frac{y}{z}>0$, avec ici x impair. Or ce quart de cercle admet le paramétrage rationnel, où $t\in]0,1[$,

$$X=\cos\theta=\frac{1-t^2}{1+t^2} \quad , \quad Y=\sin\theta=\frac{2t}{1+t^2}\ .$$

Si $t\in\mathbb{Q}$ on a $X,Y\in\mathbb{Q}$. Réciproquement, si $X,Y\in\mathbb{Q}$, alors $t^2=\frac{1-X}{1+X}\in\mathbb{Q}$ et donc $t=\frac{1}{2}(1+t^2)Y\in\mathbb{Q}$. Ainsi, pour connaître les solutions premières (x,y,z) de (1), il suffit de choisir $t\in\mathbb{Q}$ et alors x,y,z seront déterminés par le fait que $X=\frac{x}{z}$, $Y=\frac{y}{z}$ avec xy,z premiers dans leur ensemble et x impair. Pour cela, on choisit $v\in\mathbb{N}$, $u\in\mathbb{N}^*$ premiers entre eux et $t=\frac{v}{u}$. On a

$$X=\frac{1-t^2}{1+t^2}=\frac{u^2-v^2}{u^2+v^2} \quad , \quad Y=\frac{2t}{1+t^2}=\frac{2uv}{u^2+v^2}\ .$$

Vérifions que u^2-v^2 , $2uv$, u^2+v^2 sont premiers dans leur ensemble. Ils seront alors égaux à x,y,z par unicité de la forme réduite de X et Y. Soit p un diviseur premier des trois nombres. Alors p divise $(u^2+v^2)+(u^2-v^2)=2u^2$ et $(u^2+v^2)-(u^2-v^2)=2v^2$. Si on suppose $p\neq 2$, on obtient $p|u$ et $p|v$. C'est exclu car $u\wedge v=1$. Donc $p=2$. Le fait que 2 divise u^2+v^2 nécessite que u et v soient de même parité. On ne peut avoir u et v pairs puisque $u\wedge v=1$. On a donc $u=2k+1$, $v=2m+1$ et donc $u^2-v^2=4k+4k^2-4m-4m^2$, $2uv=2(1+2k+2m+4km)$, $u^2+v^2=2+4k+4k^2+4m+4m^2$. On peut simplifier par 2. On obtient des nombres premiers dans leur ensemble qui seront donc égaux à x,y,z par unicité de la forme réduite de X et Y. On obtient x pair ce qui est exclu. Le facteur 2 est à rejeter et les trois nombres considérés sont effectivement premiers dans leur ensemble, égaux à x,y,z. Pour toute solution première (x,y,z), avec x impair, y pair, on a z impair et il existe donc $u\in\mathbb{N}^*, v\in\mathbb{N}^*$, uniques, avec $u\wedge v=1$ tels que $x=u^2-v^2$, $y=2uv$, $z=u^2+v^2$. ∎

Définition.

On appelle équation diophantienne, une équation $p(X,Y,Z)=0$ où les inconnues X,Y,Z sont des entiers et où p est un polynôme de plusieurs variables, à coefficients entiers.

Remarques. Ce vocabulaire doit son mom à DIOPHANTE, mathématicien qui vivait à Alexandrie aux environs de l'an 300. Il a laissé un traité qui résout l'équation (1) et certaines autres. Mais ce type d'équation a une longue histoire qui remonte jusqu'aux égyptiens, babyloniens et grecs. Pythagore en aurait déjà donné certaines solutions $x=2n+1$, $y=2n^2+2n$, $z=y+1$.

La méthode géométrique que nous avons employée pour résoudre (1) est applicable à d'autres équations $p(X,Y,Z)=0$. Il suffit que $p\in\mathbb{Z}[X]$ soit un polynôme homogène tel que la courbe plane d'équation $p(x,y,1)=0$ possède un bon paramétrage rationnel. C'est le cas par exemple des courbes algébriques de degré 3 admettant un point double. En les coupant par des droites de pente variable t, issues du point double, on obtient dans l'équation aux abscisses, une racine double due au point double et une troisième racine fonction rationnelle de t. Par exemple les cubiques classiques : cissoïde, strophoïde, folium de Descartes, etc. sont de ce type.

Proposition 2. (Fermat)

Les équations diophantiennes $x^4 + y^4 = z^2$ *et* $x^4 + y^4 = z^4$ *n'ont pas de solution non triviale.*

Démonstration. Il suffit bien sûr de démontrer que la première de ces équations n'a pas de solution telle que $xyz \neq 0$. La démonstration est une illustration de la méthode de *descente infinie* de Fermat. Raisonnons par l'absurde. Supposons que l'ensemble E des $(x, y, z) \in (\mathbb{N}^*)^3$ telles que $x^4 + y^4 = z^2$ soit non vide. Considérons une solution pour laquelle $z \in \mathbb{N}^*$ soit minimum. On va arriver à une contradiction en construisant une autre solution pour laquelle z soit encore plus petit.

Notons que x, y, z sont premiers dans leur ensemble (sinon, $d = \text{pgcd}(x, y, z) > 1$ et $\frac{x}{d}$, $\frac{y}{d}$, $\frac{z}{d^2}$ constituent une solution non triviale avec $\frac{z}{d^2} < z$. D'après la proposition 1, il existe des entiers $0 < v < u$. avec $u \wedge v = 1$ tels que

$$x^2 = 2uv \quad , \quad y^2 = u^2 - v^2 \quad , \quad z = u^2 + v^2 \, .$$

(Si y était pair et x impair, on échangerait les notations). Alors, u est impair. En effet si u était pair, alors v serait impair car $u \wedge v = 1$ et on aurait $y^2 \equiv -1 \pmod 4$, ce qui est impossible car modulo 4 un carré y^2 est congru à 0 si y est pair et à 1 si y est impair. Ainsi, u est impair et v est pair. Et on a :

$$v^2 + y^2 = u^2,$$

avec u, v, y premiers dans leur ensemble car $u \wedge v = 1$. D'après la proposition, il existe des entiers r, s tels que $r \wedge s = 1$ et :

$$v = 2rs \quad , \quad y = r^2 - s^2 \quad , \quad u = r^2 + s^2 \, .$$

On a $x^2 = 2uv = 4rs(s^2 + r^2)$. Puisque $r \wedge s = 1$, on a $r \wedge (s^2 + r^2) = 1$, $s \wedge (s^2 + r^2) = 1$. Donc nécessairement, r , s , $s^2 + r^2$ sont tous des carrés : il existe α, β, γ entiers tels que $r = \alpha^2$, $s = \beta^2$, $s^2 + r^2 = \gamma^2$, d'où $\alpha^4 + \beta^4 = \gamma^2$. On a obtenu une solution, avec $0 < \gamma < z$. En effet on a $\alpha \neq 0$ (sinon $x = 0$), $\beta \neq 0$ de même. Et $\gamma^2 = s^2 + r^2 = u < u^2 + v^2 = z$. D'où la contradiction annoncée. ∎

Remarque. Fermat indiquait dans la marge du traité de Diophante, qu'il savait prouver que pour tout $n \geqslant 3$ l'équation diophantienne $x^n + y^n = z^n$ n'avait pas de solution non triviale. Jusqu'en 1995, personne n'a pu le prouver, malgré des recherches intenses. La démonstration enfin donnée par Wiles en 1995, utilise des outils classiques introduits au siècle dernier (théorie des fonctions elliptiques) et des théories récentes et difficiles.

Exercice 1. Soit p un nombre premier. Si on a $p \equiv 3 \pmod 4$, montrer que l'équation diophantienne $x^2 + y^2 = pz^2$ n'a pas de solution non triviale.
En est-il de même si $p = 2$ ou si $p \equiv 1 \pmod 4$?

Solution. Si (x, y, z) est solution, on aura $\overline{x}^2 + \overline{y}^2 = \overline{0}$ dans $\mathbb{Z}/p\mathbb{Z}$. Si on avait $\overline{x} \neq \overline{0}$ et $\overline{y} \neq \overline{0}$, alors $-\overline{1} = (\overline{x})^{-2}\overline{y}^2$ serait un carré. D'après 12-3, ex. 2, cela est exclu. Donc, par exemple $\overline{x} = \overline{0}$ et donc $x = px_1$. En reportant dans l'équation, on voit que p divise y donc $y = py_1$ et on obtient $p(x_1^2 + y_1^2) = z^2$. On en déduit que $z = pz_1$, d'où $x_1^2 + y_1^2 = pz_1^2$. Ainsi (x_1, y_1, z_1) est une solution dont tous les termes sont strictement inférieurs à ceux de (x, y, z). On peut appliquer le principe de descente infinie de Fermat. On voit que cette équation ne peut avoir de solution non triviale.

Si $p = 2$ ou si $p \equiv 1 \pmod 4$, il existe $a, b \in \mathbb{N}$ tels que $p = a^2 + b^2$ (11-6, cor. 2). En posant $x = aX + bY$, $y = -bX + aY$, on obtient $X^2 + Y^2 = z^2$ qui admet une infinité de solutions. L'équation étudiée a une infinité de solutions...

Exercice 2. Montrer que l'équation $x^3 + y^3 = xyz$ a beaucoup de solutions en nombres entiers (alors qu'au premier coup d'oeil on pourrait la croire voisine de $x^3 + y^3 = z^3$ qui n'a pas de solution non triviale d'après le th. de Fermat-Wiles).

Solution. On peut se contenter de chercher les solutions avec (x, y, z) premiers dans leur ensemble et avec $z > 0$. (Pour $z = 0$ les solutions sont $y = -x \in \mathbb{Z}$.) Posons $X = \frac{x}{z}$, $Y = \frac{y}{z}$. Alors $M(X, Y)$ est un point de coordonnées rationnelles sur la courbe C de $\mathbb{R}^2$ d'équation $X^3 + Y^3 = XY$ (Folium de Descartes). Réciproquement, tout point $M(X, Y)$ à coordonnées rationnelles de C, autre que l'origine, fournit une solution du type indiqué en exprimant les rationnels $X = \frac{x}{z}$, $Y = \frac{y}{z}$ comme fractions réduites et ramenées au plus petit dénominateur commun. En recoupant C avec les droites d'équation $Y = tX$, on obtient le paramétrage rationnel $X = \frac{t}{t^3+1}$, $Y = \frac{t^2}{t^3+1}$ des points autres que l'origine. Pour $t \in \mathbb{Q}$, on a $X \in \mathbb{Q}$ et $Y \in \mathbb{Q}$. Réciproquement, si $X \in \mathbb{Q}$ et $Y \in \mathbb{Q}$ on a $t = \frac{Y}{X} \in \mathbb{Q}$ (on a $X \neq 0$ en dehors de l'origine). Pour tout $t = \frac{u}{v} \in \mathbb{Q}$, avec $u \in \mathbb{Z}^*$, $v \in N^*$, $u \wedge v = 1$, on obtient $x = uv^2$, $y = u^2v$, $z = u^3 + v^3$ premiers dans leur ensemble (solutions auxquelles il faut rajouter $\{(x, -x :, 0) ; x \in \mathbb{Z}\}$)

Commentaires historiques et problèmes

L'étude des nombres fut, avec la géométrie, au centre des préoccupations de l'école grecque ($5^{\text{ème}}$ siècle avant JC). Certains problèmes datant de cette époque ne furent résolus qu'au $19^{\text{ème}}$ siècle (quadrature du cercle, transcendance de $\pi \ldots$). D'autres restent toujours sans réponse. Voici quelques problèmes célèbres.

- Existe-t-il une infinité de couples de nombres premiers "jumeaux", c'est-à-dire de la forme $(p, p + 2)$*, comme 3 et 5, 5 et 7, 11 et 13, ?*
- Existe-t-il une infinité de nombres premiers de la forme $n^2 + 1$ *?*
- Pour tout $b > 0$*, existe-t-il un nombre premier de la forme* $a^2 + b$ *? - Tout nombre pair* $n > 2$*, est-il somme de deux nombres premiers ? - La relation* $a^x - b^y = 1$ *admet-elle d'autres possibilités que* $3^2 - 2^3 = 1$ *?*

Certains problèmes, restés longtemps hermétiques reçurent une réponse naturelle quand l'algèbre en se développant apporta des méthodes appropriées. On peut même dire que de nombreux développements importants de l'algèbre sont nés pour créer des outils adaptés à l'étude de problèmes de théorie des nombres.

Par exemple, E. GALOIS (1811-1832), avant de mourir à 21 ans dans un duel, confia à un ami intime un manuscrit introduisant les notions de groupe, de corps de nombres, d'extensions de corps (voir ch. 13) et démontrant, grâce à ces outils, une des plus célèbres conjectures de son époque : l'impossibilité de donner les solutions à l'aide de formules avec radicaux (comme les formules de Cardan pour le degré trois), pour les équation polynomiales à une inconnue de degré supérieur ou égal à cinq.

On doit à K. F. GAUSS (1777-1855), de très nombreuses découvertes. Par exemple, en introduisant l'anneau $\mathbb{Z} + i\mathbb{Z}$ des entiers de Gauss (premier exemple étudié d'anneaux "d'entiers algébriques"), il a caractérisé comme nous l'avons vu au ch. 11 les nombres premiers qui sont somme de deux carrés.

L. EULER utilisa le premier l'analyse pour étudier les nombres premiers (voir 12-4, prop. 2). Au $19^{\text{ème}}$ siècle, sous l'impulsion de G. DIRICHLET, P. TCHEBYCHEV, B. RIEMANN, les fonctions d'une variable complexe se révélèrent un outil puissant.

Exercices du chapitre 12

Ex 12 - 1

Soient $p \neq q$ deux nombres premiers impairs et $a \in \mathbb{N}$. Montrer que $X^2 - a^2$ admet quatre racines dans l'anneau $\mathbb{Z}/pq\mathbb{Z}$.

Exemple : résoudre $n^2 \equiv 4 \pmod{35}$.

Ex 12 - 2

Soit $f \in \mathbb{Z}[X]$. On considère la suite (u_n) définie par la relation de récurrence $u_{n+1} = f(u_n) + u_{n-1}$ et la donnée de u_0 et u_1 dans $\mathbb{Z}$. Montrer que pour tout entier $k \geqslant 2$, la suite des restes modulo k des nombres u_n est périodique.

Exemple : pour tout $r \in \mathbb{N}^*$, montrer que la suite de Fibonacci définie par :

$$u_{n+1} = u_n + u_{n-1}\,,\ u_0 = 1\,,\ u_1 = 0\,,$$

contient une infinité de termes dont l'expression décimale finit par r zéros.

Ex 12 - 3

Soit $p \in \mathbb{N}$ premier. Soient $x_1, \ldots, x_p$ des nombres entiers non divisibles par p. Pour toute partie non vide $A = \{i_1, \ldots, i_k\}$ de $E = \{1, \ldots, p\}$, on pose $n_A = x_{i_1} + \cdots + x_{i_k}$. Montrer que l'un des nombres n_A est divisible par p.

Par exemple, soient $a \in \mathbb{N}$ et $b \in \mathbb{N}$ non divisibles par p. Montrer que parmi les nombres $ua + vb$, où $u \in \mathbb{N}, v \in \mathbb{N}$ sont tels que $0 < u + v \leqslant p$, l'un d'eux au moins est divisible par p.

Ex 12 - 4

Soit p un nombre premier. En examinant les racines de $P(X) = X^p - X$ dans le corps $F_p = \mathbb{Z}/p\mathbb{Z}$ montrer que $P(X + \overline{1}) = P(X)$. Retrouver ainsi que $C_p^k \equiv 0 \pmod{p}$ pour $k = 1, \ldots, p-1$.

Ex 12 - 5

a) Soit K un corps commutatif fini, de caractéristique p, de cardinal q.
Montrer que $x^q - x = 0$ pour tout $x \in K$, (généralisation du th. de Fermat). Généraliser le th. de Wilson.
Montrer que le sous-corps premier de K est $\{x \in K \mid x^p - x = 0\}$.

b) Si $p = 2$ montrer que tout $x \in K$ est un carré. Si $p \neq 2$, on a $q = 2s + 1$ impair.
Soit $x \in K_*$. Montrer que $x^s = 1$ si x est un carré et que $x^s = -1$ sinon.

Ex 12 - 6

Soit $n \in \mathbb{N}$ tel que $n \geqslant 2$. S'il existe $a \in \mathbb{Z}$ tel que $a^{n-1} \equiv 1 \pmod{n}$ et $a^k \not\equiv 1 \pmod{n}$ pour $1 \leqslant k \leqslant n-1$, montrer que n est premier (réciproque du th. de Fermat).

Ex 12 - 7

Déterminer le reste $a \in \mathbb{N}$ de la division de $n = 1994^{1999}$ par 25 et le reste $b \in \mathbb{N}$ de la division de n par 9. En utilisant le th. chinois, en déduire le reste $r \in \mathbb{N}$ de la division de n par 225.

Ex 12 - 8

Soient $m \in \mathbb{N}^*$, $n \in \mathbb{N}^*$. Montrer que 56 786 730 divise $N = mn(m^{60} - n^{60})$.

Ex 12 - 9

Soit $p = 2m + 1$ un nombre premier impair. Montrer que

$$(-1)^m (m\,!)^2 \equiv -1 \pmod{p}.$$

Si de plus $p \equiv 3 \pmod{4}$, montrer que $m\,! \equiv \pm 1 \pmod{p}$. Réciproquement, si un entier impair $p = 2m + 1$ est tel que $(m\,!)^2 \equiv \pm 1 \pmod{p}$, montrer que p est premier.

Ex 12 - 10

Montrer que l'équation en nombres entiers $n^2 - 23m = 329$ n'a pas de solution. Pour tout entier $a \in \mathbb{Z}$, montrer que $n^3 - 23m = a$ admet des solutions.

Ex 12 - 11

Soient $p = 2m+1$ un nombre premier impair et $F_p = \mathbb{Z}/p\mathbb{Z}$.

a) Pour $k = 2, \ldots, m$, montrer que $-\overline{1}$ ou $\overline{k}$ ou $-\overline{k}$ est un carré dans F_p.

b) On suppose $p \equiv 3 \pmod 4$
(i) Montrer que l'un des éléments $\overline{k}$ ou $-\overline{k}$ est un carré et un seul.
(ii) En déduire que $m\,! \equiv \pm 1 \pmod p$ et que $(m\,!)^2 \equiv 1 \pmod p$.

Ex 12 - 12

Montrer que la classe de 58 dans l'anneau $\mathbb{Z}/77\,\mathbb{Z}$ est un carré et déterminer les éléments dont il est le carré.

Ex 12 - 13

Déterminer les entiers k tels que

$$39k^2 + 3k - 77 \equiv 0 \pmod{385}.$$

Ex 12 - 14

Soit $p \neq 2$ un nombre premier.

a) Soient $a, b, c \in F_p = \mathbb{Z}/p\mathbb{Z}$ non nuls. Montrer que $ax^2 + by^2 = c$ admet des solutions $(x, y) \in (F_p)^2$ (considérer les cardinaux de $A = \{ax^2\,;\ x \in F_p\}$ et de $B = \{c - by^2\,;\ y \in F_p\}$).
Montrer que dans F_p tout élément est somme de deux carrés.

b) Résoudre $5x^2 + 3y^2 \equiv 11 \pmod{13}$, puis $x^2 + xy + 8y^2 \equiv 10 \pmod{13}$.

Ex 12 - 15

Notons G l'anneau des entiers de Gauss. Soit $A \in \mathcal{M}_2(G)$ hermitienne, définie positive. On identifie un élément $x = (x_1, x_2) \in G^2$ et la matrice ligne $(x_1\ x_2)$. On note x^* la matrice ${}^t\overline{x}$ transposée de la conjuguée de x. On pose

$$m(A) = \inf\{xAx^*\,;\ x \in G^2 \setminus \{0\}\}.$$

a) Justifier l'existence de $m(A)$ et montrer qu'il existe $z_0 = (z_1, z_2) \in G^2 \setminus \{0\}$ tel que $m(A) = z_0 A z_0^*$.
Montrer que $z_1 \wedge z_2 = 1$ dans G.

b) Pour tout $U \in \mathrm{GL}(2, G)$, montrer que $m(UAU^*) = m(A)$ et que $\det(UAU^*) = \det(A)$.

c) Montrer qu'il existe $U_0 \in \mathrm{GL}(2, G)$ dont z_0 soit le premier vecteur ligne. Montrer que $B = U_0 A U_0^* = (b_{ij})$ est telle que $b_{11} = m(A) = m(B)$.

d) Montrer qu'il existe $q \in G$ tel que $|\, b_{12} - b_{11}q \,| < \frac{1}{\sqrt{2}}\, b_{11}$. En déduire

qu'il existe $C = \begin{pmatrix} a & r \\ \overline{r} & c \end{pmatrix} \in \mathcal{M}_2(G)$,

telle que $m(A) = a \leqslant \sqrt{2}\, d^{1/2}$, où $d = \det(C)$, et $\sqrt{2}\,|r| \leqslant a \leqslant c$.
Si $d = 1$, montrer qu'il existe $U \in \mathrm{GL}(2, G)$ telle que $A = U^* U$.

e) Soit $p \in \mathbb{N}$ premier impair. Montrer qu'il existe $x \in \mathbb{Z}, y \in \mathbb{Z}, m \in \mathbb{N}^*$,

tels que $A = \begin{pmatrix} p & x+iy \\ x-iy & m \end{pmatrix}$ soit,

hermitienne, définie positive, avec $\det(A) = 1$. En déduire que p est somme de quatre carrés (th. de Lagrange).

Ex 12 - 16

a) Soient $p = 2m+1$ un nombre premier impair et $\overline{u} \in F_p = \mathbb{Z}/p\mathbb{Z}$. En étudiant le polynôme unitaire $a(X) \in F_p[X]$ dont les racines sont les $\overline{c} - \overline{u}$, où $\overline{c}$ décrit l'ensemble C des carrés de $(F_p)_*$, calculer $\rho = \prod_{\overline{c} \in C} (\overline{u} - \overline{c})$.

b) Retrouver ainsi la caractérisation d'Euler des carrés de $(F_p)_*$.
Montrer que ρ vaut $\overline{0}$ ou $-\overline{2}$.

c) Si $p \equiv 3 \pmod 4$, en déduire que

$$\prod_{x=1}^{m} \prod_{y=1}^{2m} = (\overline{x}^2 + \overline{y}^2) = \overline{1}.$$

Ex 12 - 17

En adaptant le raisonnement d'Euclide, montrer qu'il existe une infinité de nombres premiers de la forme $4k+3$ ou de la forme $6k+5$.

Ex 12 - 18

a) Pour tout $n \in \mathbb{Z}$, montrer que tout facteur premier de $N = n^2 - n + 1$ est égal à 3 ou de la forme $6k+1$.
Etudier de même les facteurs premiers de $N' = n^4 + 1$ et de $N'' = n^6 + n^3 + 1$.

b) Résoudre $n^4 + 1 \equiv 0 \pmod{17}$.

Ex 12 - 19

Montrer que pour tout $k \in \mathbb{N}$, il existe une infinité de nombres premiers de la forme $m2^{k+1} + 1$.

Ex 12 - 20

Soit $m \in \mathbb{N}^*$ impair. On note $\Phi_n(X)$ le polynôme cyclotomique d'indice $n \in \mathbb{N}^*$. Montrer que les nombres $\Phi_{2^{k+1}}(m)$, où $k \in \mathbb{N}$, sont deux à deux premiers entre eux.
En déduire que les nombres de Fermat F_k sont deux à deux premiers entre eux, d'où une autre démonstation du fait qu'il existe une infinité de nombres premiers.

Ex 12 - 21

Soit p un nombre premier. Pour $k \in \mathbb{N}$, posons $n_k = k^2 + k + p$. Si n_k est premier pour $k = 0, \ldots, E(\sqrt{\frac{p}{3}})$, montrer que n_k est premier pour $k = 0, \ldots, p-2$.
Application : $p = 11$, 17, 41.

Ex 12 - 22

Landry a montré en 1880 que le nombre de Fermat F_6 n'est pas premier. Pour vérifier cela, montrer qu'il n'est pas nécessaire de tester la divisibilité de F_6 par tout entier inférieur à $(F_6)^{1/2}$.

Indications

Ex 12 - 1

Resoudre l'équation dans $\mathbb{Z}/p\mathbb{Z}$ et $\mathbb{Z}/q\mathbb{Z}$, puis utiliser le th. chinois.

Ex 12 - 2

Montrer que dans $(\mathbb{Z}/k\mathbb{Z})^2$ la suite $(\overline{u}_n, \overline{u}_{n+1})$ a une répétition.

Ex 12 - 3

Montrer que tout élément de $\mathbb{Z}/p\mathbb{Z}$ est classe d'un nombre n_A.

Ex 12 - 4

D'après le th. de Fermat,
$X^p - X = \prod (X - \overline{k})$, où $\overline{k}$ décrit $\mathbb{Z}/p\mathbb{Z}$.

Ex 12 - 5

a) Appliquer le th. de Lagrange au groupe K_*. Utiliser le th. de Fermat.

b) Dans le groupe cyclique K_*, raisonner comme en 12-3, prop. pour $\mathbb{Z}/p\mathbb{Z}$.

Ex 12 - 6

Montrer que
$\langle a \rangle = (\mathbb{Z}/n\mathbb{Z}) \setminus \{0\} \subset (\mathbb{Z}/n\mathbb{Z})_*$.

Ex 12 - 7

Appliquer le th. de Fermat-Euler dans $\mathbb{Z}/25\mathbb{Z}$ et $\mathbb{Z}/9\mathbb{Z}$ et utiliser le th. chinois.

Ex 12 - 8

Utiliser le th. de Fermat pour $p = 61, 31, 13, \ldots$

Ex 12 - 9

Reprendre la démonstration du th. de Wilson.

Ex 12 - 10

$\overline{329}$ n'est pas un carré de $\mathbb{Z}/23\mathbb{Z}$ d'après le critère d'Euler. Vérifier que $\overline{n} \mapsto \overline{n}^3$ est un automorphisme du groupe $(\mathbb{Z}/23\mathbb{Z})_*$.

Ex 12 - 11

Utiliser la caractérisation d'Euler des carrés de $(F_p)_*$.

Ex 12 - 12

Par le th. chinois, on se ramène à la recherche des racines carrées de $\overline{2}$ dans $\mathbb{Z}/7\mathbb{Z}$ et de $\overline{3}$ dans $\mathbb{Z}/11\mathbb{Z}$.

Ex 12 - 13

Dans $\mathbb{Z}/385\mathbb{Z}$, mettre le trinôme sous forme canonique. Utiliser le th. chinois.

Ex 12 - 14

a) Les parties A et B de cardinal $\frac{p+1}{2}$ ne peuvent être disjointes dans F_p.

b) Dans $\mathbb{Z}/13\mathbb{Z}$, exprimer A et B pour $a = \overline{5}$, $b = \overline{3}$, $c = \overline{11}$.
Utiliser la méthode de Gauss pour exprimer la forme quadratique comme combinaison de carrés de formes linéaires indépendantes.

Ex 12 - 15

Suivre pas à pas les questions (partie d'épreuve de l'agrégation 1989).

Ex 12 - 16

a) Utiliser le th. de Fermat pour factoriser $a(X)$.

b) $\overline{u}$ est un carré si $\rho = \overline{0}$.

c) Mettre en facteur $\overline{x}^2$.

Ex 12 - 17

Reprendre la démonstration du th. 1 du paragraphe 12-4.

Ex 12 - 18

Il suffit d'appliquer 12-6, prop.

Ex 12 - 19

Utiliser 12-6, cor. et prop.

Ex 12 - 20

Si un nombre premier p divisait $\Phi_{2^{k+1}}(m)$ et $\Phi_{2^{n+1}}(m)$ avec $k \leqslant n$, alors $\overline{m}$ serait dans $\mathbb{Z}/p\mathbb{Z}$ une racine multiple pour $X^n - 1$. On peut utiliser 10-7, prop.

Ex 12 - 21

Raisonner par l'absurde : s'il existe $k \in [0, p-2]$ tel que $n_k = ab$ avec $1 < a \leqslant b$, montrer que $(k-a)^2 + (k-a) + p = a(a + b - 2k - 1)$, avec $a + b - 2k - 1 > 1$.

Ex 12 - 22

Il suffit de considérer les diviseurs de la forme $k2^7 + 1 = 128k + 1$ (12-6, cor.).

Solutions des exercices du chapitre 12

Ex 12 - 1

Soit $x \in \mathbb{Z}$. Notons $\widehat{x}, \overline{x}, \dot{x}$ les classes de x dans $\mathbb{Z}/pq\mathbb{Z}$, $F_p = \mathbb{Z}/p\mathbb{Z}$, $F_q = \mathbb{Z}/q\mathbb{Z}$. D'après le th. chinois, l'application $\widehat{x} \mapsto (\overline{x}, \dot{x})$ de $\mathbb{Z}/pq\mathbb{Z}$ dans $F_p \times F_q$ est bien définie et c'est un isomorphisme. Donc

$$\widehat{x}^2 = \widehat{a}^2 \quad \Leftrightarrow \quad (\overline{x}^2, \dot{x}^2) = (\overline{a}^2, \dot{a}^2) \quad \Leftrightarrow \quad \overline{x}^2 = \overline{a}^2 \quad \text{et} \quad \dot{x}^2 = \dot{a}^2 .$$

Comme F_p est un corps, le polynôme $X^2 - \overline{a}^2$ admet au plus deux solutions. Comme $\overline{a}, -\overline{a} = \overline{p-a}$ sont racines, avec $\overline{a} \neq -\overline{a}$ car p est impair, $X^2 - \overline{a}^2$ a exactement deux racines distinctes dans F_p. De même, $X^2 - \dot{a}^2$ a exactement deux racines distinctes $\dot{a}, -\dot{a}$ dans F_q. Dans $F_p \times F_q$ on a quatre solutions $(\overline{a}, \dot{a})$, $(\overline{a}, -\dot{a})$, $(-\overline{a}, \dot{a})$, $(-\overline{a}, -\dot{a})$. Ainsi $\widehat{x}^2 = \widehat{a}^2$ a exactement quatre solutions dans $\mathbb{Z}/pq\mathbb{Z}$.

Avec $p = 5$ et $q = 7$ on a $3 \times 5 - 2 \times 7 = 1$. Dans $\mathbb{Z}/5\mathbb{Z}$ (resp. $\mathbb{Z}/7\mathbb{Z}$) les racines de $X^2 - \overline{4}$ sont $\overline{2}, \overline{3}$ (resp. $\overline{2}, \overline{5}$). En utilisant le th. chinois, les racines de $X^2 - 4$ dans l'anneau $\mathbb{Z}/35\mathbb{Z}$ sont les quatre classes (deux à deux opposées) des entiers :

$$\begin{array}{ll} 3 \times 5 \times 2 - 2 \times 7 \times 2 = 2 , & 3 \times 5 \times 5 - 2 \times 7 \times 2 = 12 , \\ 3 \times 5 \times 2 - 2 \times 7 \times 3 = -12 , & 3 \times 5 - 2 \times 7 \times 3 = -2 . \end{array}$$

Dans $(\mathbb{Z}/35\mathbb{Z})[X]$, le polynôme $X^2 - \overline{4}$ admet deux factorisations (voir Ex. 10-5) :

$$X^2 - \overline{4} \;=\; (X - \overline{2})(X + \overline{2}) \;=\; (X - \overline{12})(X + \overline{12}) .$$

Ex 12 - 2

Appliquons le principe des tiroirs : "si on range $q+1$ objets dans q tiroirs, alors nécessairement deux de ces objets iront dans le même tiroir".

Ici, les tiroirs seront les $q = k^2$ couples de classes $(\overline{x}, \overline{y}) \in (\mathbb{Z}/k\mathbb{Z})^2$ et les $q+1$ objets seront $(u_0, u_1), \ldots, (u_q, u_{q+1})$. Il existe donc des entiers m et N tels que

$$0 \leqslant m < m + N \leqslant q \text{ et tels que } (\overline{u}_m, \overline{u}_{m+1}) = (\overline{u}_{m+N}, \overline{u}_{m+N+1}) .$$

Puisque la suite $(\overline{u}_n)$ vérifie la relation de récurrence, $\overline{u}_{n+2} = f(\overline{u}_{n+1}) + \overline{u}_n$ on obtient $\overline{u}_{m+2} = \overline{u}_{m+N+2}, \ldots, \overline{u}_{m+N-1} = \overline{u}_{m+2N-1}$. La suite des couples de classes a la période N à partir de $\overline{u}_m$. Comme $\overline{u}_{n-1} = \overline{u}_{n+1} - f(\overline{u}_n)$ on a également $\overline{u}_{m-1} = \overline{u}_{m+N-1}$, etc. La périodicité se vérifie en "descendant", jusqu'à l'indice zéro.

Appliquons cela à la suite de Fibonacci, avec $k = 10^r$. La suite $(\overline{u}_n)$ de $\mathbb{Z}/k\mathbb{Z}$ a une période $N > 0$. La suite $\overline{u}_0 = \overline{0}, \overline{u}_N, \overline{u}_{2N}, \ldots$ est donc constante dans $\mathbb{Z}/k\mathbb{Z}$ donc $k = 10^r$ divise $u_0, u_N, u_{2N}, \ldots$. (Voir aussi Ex. 9-3.)

Ex 12 - 3

Faisons l'hypothèse (H) : pour toute partie A de E, distincte de E, le nombre n_A n'est pas divisible par p. Montrons que n_E est alors divisible par p, ce qui établira le résultat. D'après (H), dans le corps $\mathbb{Z}/p\mathbb{Z}$ les classes des entiers $k_1 = x_1$, $k_2 = x_1 + x_2, \ldots, k_{p-1} = x_1 + \cdots + x_{p-1}$ sont non nulles. Elles sont deux à deux distinctes car s'il existait $i < j$ tels que $\overline{k}_i = \overline{k}_j$, par soustraction on aurait $\overline{x}_{i+1} + \cdots + \overline{x}_j = \overline{0}$, ce qui est contraire à (H). L'ensemble de ces $p-1$ classes est donc égal à $(\mathbb{Z}/p\mathbb{Z})_*$. Alors, la classe de $x_1 + \cdots + x_p$ dans $\mathbb{Z}/p\mathbb{Z}$, distincte des précédentes, est $\overline{0}$.

En particulier, prenons $x_1 = \cdots = x_k = a$, $x_{k+1} = \cdots = x_p = b$, avec $0 < k < p$. Les nombres n_A sont les nombres $ua + vb$, avec $0 < u + v \leqslant p$, $0 \leqslant u \leqslant k$ et $0 \leqslant v \leqslant p - k$. Si p ne divise ni a, ni b, l'un des nombres $ua + vb$ est divisible par p.

Ex 12 - 4

D'après le th. de Fermat, tout $x \in \mathbb{Z}/p\mathbb{Z} = F_p$ est racine de $P(X) = X^p - X$. Comme $P(X)$ admet au plus p racines dans le corps F_p, ses racines sont les p éléments de F_p et $P(X) = X^p - X = X(X - \overline{1})(X - \overline{2}) \cdots (X - \overline{p-1})$. Les racines de $P(X + \overline{1})$ se déduisent de celles de $P(X)$ par l'application $\lambda \mapsto \lambda - \overline{1}$ qui est une bijection de F_p sur F_p. La factorisation du polynôme $(X+1)^p - (X+1)$ est donc la même que celle de $P(X)$. Ces polynômes sont égaux. Comme $(X+1)^p = X^p + C_p^1 X^{p-1} + \cdots + C_p^{p-1} X + 1$, l'égalité $P(X+1) = P(X)$ donne $C_p^1 = \overline{0}, \ldots, C_p^{p-1} = \overline{0}$ (démontré en 9-1).

Ex 12 - 5

a) Le groupe K_* est d'ordre $q - 1$. D'après le th. de Lagrange, on a $x^{q-1} = 1$ pour tout $x \in K_*$ et donc $x^q - x = 0$ pour tout $x \in K$. Dans $K[X]$, le polynôme $P(X) = X^{q-1} - 1$ de degré $q - 1$, admet les $q - 1$ éléments de K_* pour racines distinctes. Il est égal à $\prod_{x \in K_*} (X - x)$. Pour $X = 0$, on obtient $(-1)^{q-1} \prod_{x \in K_*} x = -1$ généralisant le th. de Wilson.

Le sous-corps premier K_0 de K est isomorphe à $F_p = \mathbb{Z}/p\mathbb{Z}$ (voir 9-12). On a donc $x^p - x = 0$ pour tout $x \in K_0$. Comme un polynôme de $K[X]$ de degré p a au plus p racines, les p éléments de K_0 sont les seules racines de $X^p - X$ dans K.

b) Si $p = 2$, il existe $m \in \mathbb{N}^*$ tel que $q = 2^m$ (9-12, cor.). Tout $x \in K$ est un carré car $x = x^{2^m} = (x^{2^{m-1}})^2$. Si q est impair, l'ordre $q - 1 = 2s$ de K_* est divisible par s et par 2. D'après 10-7, cor. 1, K_* est un groupe cyclique. D'après 3-3, prop., il existe un unique sous-groupe d'ordre s qui est

$$\{x \in K_* \ \ \exists y \in K_* \quad x = y^2\} = \{x \in K_* \mid x^s = 1\}.$$

D'après le th. de Lagrange, $(x^s)^2 = x^{2s} = 1$ pour tout $x \in K_*$. Donc x^s est l'une des deux racines 1 ou -1 de $X^2 - 1$. Nous venons de voir que $x \in K_*$ est un carré si et seulement si $x^s = 1$. Donc x n'est pas un carré si et seulement si $x^s = -1$.

Ex 12 - 6

Le groupe G des éléments inversibles de l'anneau $\mathbb{Z}/n\mathbb{Z}$ contient $\overline{a}$ car $\overline{a}\,\overline{a}^{n-2} = \overline{1}$. On a $\langle \overline{a} \rangle \subset G \subset (\mathbb{Z}/n\mathbb{Z}) \setminus \{0\}$. Le sous-groupe $\langle \overline{a} \rangle$ de G est d'ordre $n - 1$ d'après l'hypothèse donc ces trois ensembles sont égaux. Ainsi tout élément non nul de $\mathbb{Z}/n\mathbb{Z}$ est inversible, ce qui prouve que $\mathbb{Z}/n\mathbb{Z}$ est un corps et que n est premier.

Notons que l'existence de a tel que $a^{n-1} \equiv 1 \pmod{n}$ ne suffit pas pour que n soit premier. Par exemple $n = 3 \times 11 \times 17 = 561$ est tel que $\varphi(n)$ divise $n - 1$. D'après le th. de Fermat-Euler, pour tout a premier avec n, on a $a^{n-1} \equiv 1 \pmod{n}$.

Ex 12 - 7

Comme $1994 \equiv 4 \pmod 5$, n'est pas divisible par 5, il est premier avec $25 = 5^2$. Le th. de Fermat-Euler s'applique. On a $\varphi(25) = \varphi(5^2) = 5(5-1) = 20$ d'où $1 \equiv (-6)^{20} \pmod{25}$. Puisque $1994 = 2000 - 6 \equiv -6 \pmod{25}$, dans $\mathbb{Z}/25\mathbb{Z}$ on a :

$\overline{n} = (-\overline{6})^{1999} = [(-\overline{6})^{20}]^{100}(-\overline{6})^{-1} = (-\overline{6})^{-1} = \overline{4}$. (On a $(-\overline{6}) \times \overline{4} = -\overline{24} = \overline{1}$.)

De même $1994 \equiv 1+9+9+4 \equiv 5 \pmod 9$ est premier avec 9 et $\varphi(9) = 3(3-1) = 6$. Dans $\mathbb{Z}/9\mathbb{Z}$, le th. de Fermat-Euler donne : $\overline{n} = (\overline{5})^{1999} = [(\overline{5})^6]^{333}\overline{5} = \overline{5}$.

Ainsi n est congru à 4 modulo 25 et à 5 modulo 9. Comme $25 \times 4 - 9 \times 11 = 1$, le th. chinois montre que $n \equiv 25 \times 4 \times 5 - 9 \times 11 \times 4 = 104 \pmod 2 25$ donc $r = 104$.

Ex 12 - 8

On a $N = (m^{61} - m)n - (n^{61} - n)m$ et 61 est premier. D'après le th. de Fermat, dans $\mathbb{Z}/61\,\mathbb{Z}$ on a $\overline{k}^{61} - \overline{k} = \overline{0}$ pour tout $k \in \mathbb{Z}$. Donc N est divisible par 61.

$N = (m^{60} - 1)mn - (n^{60} - 1)mn = (m^{30} - 1)m(m^{30} + 1)n - (n^{30} - 1)n(n^{30} + 1)m$.

Comme 31 est premier, on a $\overline{k}^{31} - \overline{k} = \overline{0}$ dans $\mathbb{Z}/31\,\mathbb{Z}$ pour tout $k \in \mathbb{Z}$. Donc 31 divise N. De même, on peut faire apparaître $m^d - 1$ et $n^d - 1$ dans N pour $d = 12, 10, 6, 4, 2, 1$. Ainsi N est divisible par $2 \times 3 \times 5 \times 7 \times 11 \times 13 \times 31 \times 61 = 56\,786\,730$.

Ex 12 - 9

La liste $\overline{0}, \overline{1}, \ldots, \overline{p-1}$ des éléments de $\mathbb{Z}/p\mathbb{Z}$ peut s'écrire $-\overline{m}, \ldots, -\overline{1}, \overline{0}, \overline{1}, \ldots, \overline{m}$.
La relation $(-1)^m(\overline{m\,!})^2 = -\overline{1}$ est donc le th. de Wilson.
Si $p \equiv 3 \pmod 4$, m est impair. On a alors $(\overline{m\,!})^2 = \overline{1}$ et donc $(\overline{m\,!}) = \pm\overline{1}$.
Si $(-1)^m(\overline{m\,!})^2 = \pm\overline{1}$, alors m est premier (voir la démonstration du th. de Wilson).

Ex 12 - 10

Il existe $n \in \mathbb{Z}$ et $m \in \mathbb{Z}$ tels que $n^2 - 23m = 329$, si et seulement s'il existe $\overline{n} \in K = \mathbb{Z}/23\mathbb{Z}$ tel que $\overline{n}^2 = \overline{329} = \overline{7}$. Pour cela, d'après le critère d'Euler, il faut et il suffit que $\overline{1} = \overline{7}^{\frac{p-1}{2}}$, où $p = 23$, soit $\overline{1} = \overline{7}^{11}$. On a $\overline{7}^2 = \overline{3}$, $\overline{7}^4 = \overline{9}, \ldots, \overline{7}^{11} = -\overline{1}$. Donc $\overline{7}$ n'est pas un carré. L'équation n'a pas de solution.

Puisque $3 \wedge 22 = 1$, $f : \overline{x} \mapsto \overline{x}^3$ est un automorphisme du groupe cyclique K_* (3-2, cor. 2). En posant $f(\overline{0}) = \overline{0}$, on obtient une application bijective de K sur K. Pour tout $\overline{a} \in K$, il existe $\overline{x} \in K$, unique, tel que $\overline{x}^3 = \overline{a}$. Pour tout $a \in \mathbb{Z}$, l'équation $n^3 - 23m = a$ a donc des solutions. Si on choisit n_0 tel que $\overline{n}_0^3 = \overline{a}$. Les solutions seront $(n_0 + 23k, m)$ où m est une fonction de k qui se déduit de la relation suivante dont les termes sont divisibles par 23,

$$23m = n^3 - a = (n_0^3 - a) + 3 \times 23 n_0^2 k + 3 \times 23^2 n_0 k^2 + 23^3 k^3 .$$

Ex 12 - 11

a) D'après la caractérisation d'Euler, si aucun des éléments $-\overline{1}, \overline{k}, -\overline{k}$ n'était un carré, on aurait $(-\overline{1})^m = -\overline{1}$, $(\overline{k})^m = -\overline{1}$, $(-\overline{k})^m = -\overline{1}$ et donc $\overline{k}^{2m} = [(-\overline{1})\overline{k}(-\overline{k})]^m = -\overline{1}$. C'est impossible car $\overline{k}^{2m} = \overline{k}^{p-1} = \overline{1}$ (th. de Fermat) et $\overline{1} \neq -\overline{1}$ (puisque $p \neq 2$).

b) (i) Supposons $p \equiv 3 \pmod 4$, c'est-à-dire m impair. Si $\overline{k}$ et $-\overline{k}$ ne sont pas des carrés, d'après la caractérisation d'Euler, on a $-\overline{1} = (\overline{k})^m$, $-\overline{1} = (-\overline{k})^m = -(\overline{k})^m$. C'est contradictoire. On a donc au moins un carré dans chaque couple $(\overline{k}, -\overline{k})$ pour $k = 1, \dots, m$. Comme on a m carrés dans $(F_p)_*$, il existe exactement un carré dans chaque couple. D'ailleurs, si $\overline{k}$ et $-\overline{k}$ étaient des carrés, alors $-\overline{1}$ serait un carré, ce qui n'est pas le cas si $p \equiv 3 \pmod 4$ (voir 10-7, ex. 1).

(ii) D'après (i), on trouve un carré dans chaque couple $(\overline{2}, -\overline{2}), \dots, (\overline{m}, -\overline{m})$. La liste des carrés de $(F_p)_*$ est donc $\overline{1}, \varepsilon_2\overline{2}, \dots, \varepsilon_m\overline{m}$ où $\varepsilon_i = \pm 1$ pour $2 \leqslant i \leqslant m$. Donc $\varepsilon_2 \cdots \varepsilon_m\, \overline{1} \times \overline{2} \times \cdots \times \overline{m}$ est égal au produit de tous les carrés de $(F_p)_*$. Or, pour tout carré x^2, on a $x^2 = -x(-x)$. Donc, en posant $\varepsilon = \varepsilon_2 \cdots \varepsilon_m (-1)^m$ on obtient $\varepsilon\overline{1} \times \cdots \times \overline{m} = (-\overline{m}) \times \cdots \times (-\overline{1}) \times \overline{1} \times \cdots \times \overline{m}$ qui vaut $-\overline{1}$ d'après le th. de Wilson. Ainsi $m! \equiv \pm 1 \pmod p$ et $(m!)^2 \equiv 1 \pmod p$.

Ex 12 - 12

D'après le th. chinois, $f : \overline{x} \mapsto (\overline{x}, \overline{x})$ est un isomorphisme d'anneaux de $\mathbb{Z}/77\mathbb{Z}$ sur $(\mathbb{Z}/7\mathbb{Z}) \times (\mathbb{Z}/11\mathbb{Z})$ et $f(\overline{58}) = (\overline{2}, \overline{3})$. Dans le corps $\mathbb{Z}/7\mathbb{Z}$, on a $\overline{2} = \overline{3}^2$ donc $\overline{3}, -\overline{3}$ sont racines de $X^2 - \overline{2}$. Ce sont les seules car un polynôme de degré 2 a au plus 2 racines sur un corps. Dans le corps $\mathbb{Z}/11\,\mathbb{Z}$, on a $\overline{3} = \overline{5}^2$ donc $\overline{5}, -\overline{5}$ sont les racines de $X^2 - \overline{3}$. On a la relation de Bezout $-3 \times 7 + 2 \times 11 = 1$, d'où les quatre racines carrées de 58 dans $\mathbb{Z}/77\,\mathbb{Z}$:

$$f^{-1}(\overline{3}, \overline{5}) = -3 \times 7 \times \overline{5} + 2 \times 11 \times \overline{3} = -\overline{39} = \overline{38} \quad ; \quad f^{-1}(-\overline{3}, -\overline{5}) = \overline{39}$$
$$f^{-1}(-\overline{3}, \overline{5}) = -3 \times 7 \times \overline{5} - 2 \times 11 \times \overline{3} = -\overline{171} = \overline{60} \quad ; \quad f^{-1}(\overline{3}, -\overline{5}) = -\overline{60} = \overline{17}.$$

Ex 12 - 13

$39 = 3 \times 13$ est premier avec $385 = 5 \times 7 \times 11$ donc $\overline{39}$ a un inverse $\overline{u}$ dans $\mathbb{Z}/385\mathbb{Z}$. Déterminons-le en cherchant une relation de Bezout par l'algorithme d'Euclide.

$385 = 39 \times 10 - 5$, $39 = 5 \times 8 - 1$ d'où $1 = -39 + 8 \times 5 = -39 + 8(39 \times 10 - 385) = 79 \times 39 - 8 \times 385$. Ainsi, $\overline{1} = \overline{39} \times \overline{79}$ et $\overline{79}$ est l'inverse de $\overline{39}$ dans $\mathbb{Z}/385\mathbb{Z}$.

$$\begin{aligned} \overline{39}\,\overline{k}^2 + \overline{3}\,\overline{k} - \overline{77} = \overline{0} &\Leftrightarrow \overline{k}^2 + \overline{79} \times \overline{3}\,\overline{k} - \overline{79} \times \overline{77} = \overline{0} \\ &\Leftrightarrow \overline{k}^2 - \overline{148}\,\overline{k} + \overline{77} = \overline{0}. \end{aligned}$$

Dans $\mathbb{Z}/5\mathbb{Z}$, $P(X) = X^2 - \overline{48}X + \overline{77} = X^2 - \overline{3}X + \overline{2}$ a pour racines $\overline{1}, \overline{2}$.
Dans $\mathbb{Z}/7\mathbb{Z}$, $P(X) = X^2 - \overline{48}X + \overline{77} = X^2 - \overline{6}X$ a pour racines $\overline{0}, \overline{6}$.
Dans $\mathbb{Z}/11\mathbb{Z}$, $P(X) = X^2 - \overline{48}X + \overline{77} = X^2 - \overline{4}X$ a pour racines $\overline{0}, \overline{4}$.

D'après le th. chinois, $\overline{x} \mapsto (\overline{x}^{(5)}, \overline{x}^{(7)}, \overline{x}^{(11)})$ est un isomorphisme de $A = \mathbb{Z}/385\mathbb{Z}$ sur l'anneau $(\mathbb{Z}/5\mathbb{Z}) \times (\mathbb{Z}/7\mathbb{Z}) \times (\mathbb{Z}/11\mathbb{Z})$. Ainsi, $\overline{x}$ est solution dans A de l'équation si et seulement si $\overline{x}^{(5)}, \overline{x}^{(7)}, \overline{x}^{(11)}$ en sont solution dans $\mathbb{Z}/5\mathbb{Z}$, $\mathbb{Z}/7\mathbb{Z}$, $\mathbb{Z}/11\mathbb{Z}$. Si on connaît x modulo 5, 7 et 11, le th. chinois permet de déterminer x.

Les nombres $M_1 = 7 \times 11$, $M_2 = 5 \times 11$, $M_3 = 5 \times 7$ sont premiers dans leur ensemble. Il existe donc u, v, w tels que $7 \times 11u + 5 \times 11v + 5 \times 7w = 1$.

Déterminons u_0, w tels que $11u_0 + 35w = 1$, par l'algorithme d'Euclide. On a $35 = 3 \times 11 + 2$, $11 = 5 \times 2 + 1$ d'où $1 = 11 - 5 \times 2 = 11 - 5(35 - 3 \times 11) = 16 \times 11 - 5 \times 35$.

Puisque $1 = 3 \times 7 - 4 \times 5$, on obtient :

$$1 = 16 \times 11 \times (1 = 3 \times 7 - 4 \times 5) - 5 \times 35 = 48 \times 77 - 64 \times 55 - 5 \times 35.$$

D'après le th. chinois,

$$\left.\begin{array}{rcl} x & \equiv & a\,(\mathrm{mod}\,5) \\ x & \equiv & b\,(\mathrm{mod}\,7) \\ x & \equiv & c\,(\mathrm{mod}\,11) \end{array}\right\} \quad \Leftrightarrow \quad x \equiv 48\times 77\,a - 64\times 55\,b - 5\times 35\,c\ (\mathrm{mod}\,385)\,.$$

D'où les huit solutions de l'équation $\overline{39}\,X^2 + \overline{3}\,X - \overline{77} = \overline{0}$ dans $\mathbb{Z}/385\mathbb{Z}$.

$$\begin{array}{lll} a=1,\ b=0,\ c=0, & x \equiv 48\times 77 \equiv 3\times 77 & \equiv 231\ (\mathrm{mod}\,385) \\ a=1,\ b=0,\ c=4, & x \equiv 48\times 77 - 5\times 35\times 4 \equiv 231 + 2\times 35 & \equiv 301\ (\mathrm{mod}\,385) \\ a=1,\ b=6,\ c=0, & x \equiv 48\times 77 - 64\times 55\times 6 \equiv 3\times 77 + 55 & \equiv 286\ (\mathrm{mod}\,385) \\ a=1,\ b=6,\ c=4, & x \equiv 286 - 5\times 35\times 4 \equiv 286 + 2\times 35 & \equiv 356\ (\mathrm{mod}\,385) \\ a=2,\ b=0,\ c=0, & x \equiv 48\times 77\times 2 & \equiv 77\ (\mathrm{mod}\,385) \\ a=2,\ b=0,\ c=4, & x \equiv 77 - 20\times 35 \equiv 77 + 2\times 35 & \equiv 147\ (\mathrm{mod}\,385) \\ a=2,\ b=6,\ c=0, & x \equiv 48\times 77\times 2 + 55 \equiv 77 + 55 & \equiv 132\ (\mathrm{mod}\,385) \\ a=2,\ b=6,\ c=4, & x \equiv 77 + 55 + 70 & \equiv 202\ (\mathrm{mod}\,385) \end{array}$$

Ex 12 - 14

a) On a $p = 2m+1$ impair. Le groupe $(F_p)_*$ est cyclique (10-7, cor. 1), d'ordre $2m$. D'après 12-3, prop., il existe $m = \frac{p-1}{2}$ carrés dans F_p. Comme 0 est un carré, l'ensemble C des carrés de F_p est de cardinal $m+1 = \frac{p+1}{2}$. Comme $a \neq 0$ est inversible dans F_p, l'application linéaire $f : x \mapsto ax$ est bijective de F_p sur F_p. Donc $A = f(C)$ a $\frac{p+1}{2}$ éléments. L'application affine $g : x \mapsto c - bx$ est bijective de F_p sur F_p donc $B = g(C)$ a $\frac{p+1}{2}$ éléments. Les parties A et B de F_p ne peuvent être disjointes, sinon dans F_p, de cardinal p, on trouverait une partie $A \cup B$ ayant $p+1$ éléments. Il existe donc $x \in F_p$ et $y \in F_p$ tels que $ax^2 = c - by^2$.

Avec $a = b = 1$, on voit que tout $c \in (F_p)_*$ est somme de deux carrés. Par ailleurs, $\overline{0} = \overline{0}^2 + \overline{0}^2$ donc tout élément de F_p est somme de deux carrés.

b) Dans F_{13}, nous voulons résoudre $\overline{5}\,\overline{x}^2 + \overline{3}\,\overline{y}^2 = \overline{11}$. Simplifions légèrement en multipliant par l'inverse $-\overline{5}$ de $\overline{5}$. On obtient l'équation équivalente $\overline{x}^2 - \overline{2}\overline{y}^2 = -\overline{3}$. Cherchons ses solutions selon la méthode utilisée en (a).

$\overline{x}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$	$\overline{6}$
$\overline{x}^2$	$\overline{0}$	$\overline{1}$	$\overline{4}$	$\overline{9}$	$\overline{3}$	$\overline{12}$	$\overline{10}$

$\overline{y}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$	$\overline{6}$
$\overline{2}\overline{y}^2 - \overline{3}$	$\overline{10}$	$\overline{12}$	$\overline{5}$	$\overline{2}$	$\overline{3}$	$\overline{8}$	$\overline{4}$

Les solutions sont donc $(\pm x, \pm y)$ avec :

$x = \overline{2}$, $y = \overline{6}$ ou $x = \overline{4}$, $y = \overline{4}$ ou $x = \overline{5}$, $y = \overline{1}$ ou $x = \overline{6}$, $y = \overline{0}$.

Dans F_{13}, étudions l'équation $\overline{x}^2 + \overline{x}\,\overline{y} + \overline{8}\,\overline{y}^2 = \overline{10}$. Décomposons la forme quadratique en somme de carrés de formes linéaires indépendantes (algorithme de Gauss) :

$$\overline{x}^2 + \overline{x}\,\overline{y} + \overline{8}\,\overline{y}^2 = \overline{x}^2 + \overline{14}\,\overline{x}\,\overline{y} + \overline{8}\,\overline{y}^2 = (\overline{x} + \overline{7}\,\overline{y})^2 - (\overline{49} - \overline{8})\,\overline{y}^2 = (\overline{x} + \overline{7}\,\overline{y})^2 - \overline{2}\,\overline{y}^2\,.$$

En posant $\overline{X} = \overline{x} + \overline{7}\,\overline{y}$, $\overline{Y} = \overline{y}$ on retrouve l'équation précédente, d'où les valeurs de $\overline{X}$ et $\overline{Y}$ et ensuite celles de $\overline{x} = \overline{X} - \overline{7}\,\overline{Y}$, $\overline{y} = \overline{Y}$ que nous n'écrirons pas.

Ex 12 - 15

a) Soit $x \in G$. On a $xAx^* \in G$ et $xAx^* \in \mathbb{R}_+^*$ car A est hermitienne, définie positive. Ainsi l'ensemble des xAx^* où $x \in G^2 \setminus \{0\}$ est une partie de $G \cap \mathbb{R}_+^* = \mathbb{N}^*$. Elle a donc un plus petit élément $z_0 A z_0^*$, où $z_0 = (z_1, z_2) \in G^2 \setminus \{0\}$.

Soit δ pgcd de z_1 et z_2 dans l'anneau principal G. Si on avait $|\delta| > 1$, on aurait $z_1 = \delta z_1'$, $z_2 = \delta z_2'$ avec $z' = (z_1', z_2') \in G^2 \setminus \{0\}$ tel que $z_0 A z_0^* = \delta\overline{\delta}\, z' A z'^* > z' A z'^*$. Cela contredirait la minimalité de $z_0 A z_0^*$. Donc $|\delta| = 1$ et δ est une unité de G (11-6, lemme). Ainsi z_1 et z_2 sont premiers entre eux.

b) Tout $U \in \mathrm{GL}(2, G)$ définit une bijection de G^2 surG^2 qui laisse fixe 0.
On a donc $\{zU\,;\, z \in G^2 \setminus \{0\}\} = G^2 \setminus \{0\}$ et
$m(UAU^*) = \inf\{(zU)A(zU)^*\,;\ z \in G^2 \setminus \{0\}\} = \inf\{zAz^*\,;\, z \in G^2 \setminus \{0\}\} = m(A)$.
De plus, U étant inversible, $\det(U)$ est une unité de G (9-1, prop.). On a donc $\det(U) = 1$ (11-6, lemme) et par ailleurs $\det(U^*) = \overline{\det(U)}$. On en déduit $\det(UAU^*) = \det(U)\det(A)\det(U^*) = \det(A)$.

c) Puisque z_1 et z_2 sont premiers entre eux, dans l'anneau principal G il existe u et v tels que $z_1 u + z_2 v = 1$ (th. de Bezout). Alors, la matrice $U_0 = \begin{pmatrix} z_1 & z_2 \\ -v & u \end{pmatrix}$ est un élément de $\mathrm{GL}(2, G)$ car $\det(U_0) = 1 \in G_*$ (9-1, prop.). On a $m(A) = z_0 A z_0^* = b_{11}$.

d) L'anneau G est euclidien et la norme $z \mapsto n(z) = z\overline{z}$ est un stathme (11-3, prop.). Plus précisément, puisque $b_{11} \neq 0$, il existe q et r dans G tels que $b_{12} = b_{11}q + r$ avec $n(r) \leqslant \frac{1}{2}\, n(b_{11})$ car la plus courte distance de $\frac{b_{12}}{b_{11}} \in \mathbb{C}$ à un élément q du réseau G est au plus $\frac{\sqrt{2}}{2}$ (valeur atteinte quand on est au centre d'une maille du réseau G).

Posons $T = \begin{pmatrix} 1 & -q \\ 0 & 1 \end{pmatrix}$. Alors $C = T^* B T = \begin{pmatrix} a & r \\ \overline{r} & c \end{pmatrix}$ est telle que

$a = b_{11} = m(A)$, $r = b_{12} - b_{11}q$, $|r| \leqslant \frac{1}{\sqrt{2}}\,|a|$, $c = (0,1)C\begin{pmatrix} 0 \\ 1 \end{pmatrix} \geqslant a = \inf(zCz^*)$.

On en déduit $d = \det(C) = ac - |r|^2 \geqslant a^2 - \frac{1}{2}a^2$, soit $a \leqslant \sqrt{2}\, d^{1/2}$.

Si $d = 1$, on a $a = m(A) \leqslant \sqrt{2}$ et $a \in \mathbb{N}^*$ donc $a = 1$. Comme $|r|^2 = n(r) \in \mathbb{N}$ vérifie $|r|^2 \leqslant \frac{1}{2}$, on voit que $r = 0$. Alors $1 = d = ac - |r|^2 = c$ donc $C = I_2$. Comme C était congruente sur l'anneau G à A, il existe $U \in \mathrm{GL}(2, G)$ telle que $A = U^* U$.

e) D'après l'exercice précédent, il existe $x \in \mathbb{Z}$, $y \in \mathbb{Z}$ tels que $\overline{x}^2 + \overline{y}^2 = -\overline{1}$ dans $\mathbb{Z}/p\mathbb{Z}$. Il existe alors $m \in \mathbb{Z}$ tel que $pm = x^2 + y^2 + 1$ et on a $m > 0$.

La matrice $A = \begin{pmatrix} p & x + iy \\ x - iy & m \end{pmatrix}$ est hermitienne. Elle est donc diagonalisable dans une base orthonormée de $\mathbb{C}^2$, avec des valeurs propres λ et μ réelles. On a $\lambda + \mu = \mathrm{tr}(A) = p + m > 0$, $\lambda\mu = \det(A) = 1 > 0$ et donc $\lambda > 0$, $\mu > 0$. La matrice A est donc définie positive.

D'après d), il existe $U = \begin{pmatrix} x & z \\ y & t \end{pmatrix} \in \mathrm{GL}(2, G)$ telle que $A = U^* U$. En particulier, si $x = x_1 + ix_2$, $y = y_1 + iy_2$ on obtient $p = \overline{x}x + \overline{y}y = x_1^2 + x_2^2 + y_1^2 + y_2^2$.

Ex 12 - 16

a) On a $a(X) = \prod_{k=1}^{m}(X+\overline{u}-\overline{k}^2) = \prod_{k=1}^{m}(Y-\overline{k}^2)$ en posant $Y = X+\overline{u}$, d'où,

$$a(Y^2-\overline{u}) = \prod_{k=1}^{m}(Y^2-\overline{k}^2) = \prod_{k=1}^{m}(Y-\overline{k})(Y+\overline{k}) = \prod_{x\in K_*}(Y-\overline{x}) = Y^{p-1}-\overline{1}.$$

En effet, d'après le petit th. de Fermat, $Y^{p-1}-\overline{1}$ est le polynôme unitaire de degré $p-1$ ayant pour racines les éléments de $(F_p)_*$. On en déduit que $a(Y-\overline{u}) = Y^m-\overline{1}$ et donc que $a(X) = (X+\overline{u})^m-\overline{1}$. Pour $X=0$, en comparant les deux expressions de $a(X)$, il vient $\prod_{k=1}^{m}(\overline{u}-\overline{k}^2) = \overline{u}^{\,m}-\overline{1}$. Pour $\overline{u}=\overline{0}$ on retrouve le th. de Wilson.

b) Le corps F_p étant intègre, $\overline{u} \in (F_p)_*$ est un carré si et seulement si $\overline{u}^{\,m}-\overline{1} = \prod_{k=1}^{m}(\overline{u}-\overline{k}^2)$ est nul. On retrouve la condition $u^{\frac{p-1}{2}} \equiv 1 \pmod p$ d'Euler. On a $(\overline{u}^{\,m})^2 = \overline{u}^{\,p-1} = \overline{1}$ (th. de Fermat) et le polynôme $X^2-\overline{1}$ n'a que les deux racines $\overline{1}$ et $-\overline{1}$ dans F_p. Donc si $\overline{u}$ est un carré $\overline{u}^{\frac{p-1}{2}} = \overline{1}$ et on a $\prod_{k=1}^{m}(\overline{u}-\overline{k}^2) = \overline{0}$.

Si $\overline{u}$ n'est pas un carré, $\overline{u}^{\frac{p-1}{2}} = -\overline{1}$; dans ce cas, $\prod_{k=1}^{m}(\overline{u}-\overline{k}^2) = \overline{u}^{\,m}-\overline{1} = -\overline{2}$.

c) Comme $\overline{y} \mapsto \overline{x}^{-1}\overline{y}$ est une bijection de $(F_p)_*$ sur $(F_p)_*$, on a :

$$\zeta = \prod_{x=1}^{m}\prod_{y=1}^{2m}(\overline{x}^2+\overline{y}^2) = \prod_{x=1}^{m}\overline{x}^2\left(\prod_{y=1}^{2m}(\overline{1}+(\overline{x}^{-1}\overline{y})^2)\right) = \prod_{x=1}^{m}\overline{x}^2\left(\prod_{z=-m}^{m}m\,(\overline{1}+\overline{z}^2)\right).$$

D'après b), $\prod_{z=1}^{m}(\overline{1}+\overline{z}^2)$ vaut $\overline{0}$ si $-\overline{1}$ est un carré, c'est-à-dire si $p \equiv 1 \pmod 4$ et vaut $-\overline{2}$ si $p \equiv 3 \pmod 4$. Donc $\zeta = \overline{0}$ si $p \equiv 1 \pmod 4$. Si $p \equiv 3 \pmod 4$, on a

$$\zeta = \prod_{x=1}^{m}\overline{x}^2(-\overline{2})^2 = (\overline{2})^{2m}\left(\prod_{x=1}^{m}\overline{x}\right)^2.$$

On a $\overline{2}^{2m} = \overline{2}^{p-1} = \overline{1}$ (th. de Fermat) et $(\prod_{x=1}^{m}\overline{x})(\prod_{x=1}^{m}-\overline{x}) = -\overline{1}$ (th. de Wilson). Comme m est impair, $\prod_{x=1}^{m}\overline{x}^2 = \overline{1}$ et $\zeta = \overline{1}$ (valeur obtenue en 12-2, ex. 2.).

Ex 12 - 17

Soit $a \in \mathbb{N}^*$ tel que $\varphi(a) = 2$, soit donc $a = 2^2$, 3 ou 6. Soit $p \in \mathbb{N}$ premier qui ne divise pas a. On a donc $p \wedge a = 1$. Puisque $\varphi(a) = 2$ on a $p \equiv 1 \pmod a$ ou $p \equiv -1 \pmod a$. Supposons que l'ensemble Λ des nombres premiers congrus à -1 modulo a soit fini, d'éléments $p_1, \ldots, p_k$. Considérons alors $n = ap_1\cdots p_k - 1$ qui est congru à -1 modulo a. Si sa décomposition en facteurs premiers ne comportait que des nombres premiers congrus à 1 modulo a, on aurait $n \equiv 1$ (modulo a). Il existe donc au moins un facteur premier q de n congru à -1 modulo a. Or q ne peut appartenir à l'ensemble $\{p_1, \cdots, p_k\}$ sinon il diviserait $1 = ap_1\cdots p_k - n$. C'est absurde. L'ensemble des nombres premiers de la forme $ka-1$ est donc infini (pour $a = 3, 4, 6$).

Ex 12 - 18

a) $N = \Phi_6(-n)$, où $\Phi_a(X)$ est le polynôme cyclotomique d'indice a. D'après 12-6, prop., les facteurs premiers de $\Phi_6(-n)$ sont de la forme $6k+1$ ou facteurs

de $a = 6$ (égaux à 3 car N est impair). De même, puisque $\Phi_8(X) = X^4 + 1$ et $\Phi_9(X) = X^6 + X^3 + 1$, les facteurs premiers de N' (resp. N'') sont de la forme $8k+1$ ou égaux à 2 (resp. $9k+1$ ou égaux à 3).

b) Soit $p \in \mathbb{N}$ premier impair. D'après a), pour que $n^4 + 1 \equiv 0 \pmod p$ ait des solutions, il est nécessaire que p soit de la forme $8k+1$ (cette condition est vérifiée par 17). Ici, n est solution si et seulement si $\Phi_8(\overline{n}) = \overline{0}$, soit si $\overline{n}^4 = -1$ c'est-à-dire si $\overline{n}$ est d'ordre 8 dans le groupe cyclique $(\mathbb{Z}/17\mathbb{Z})_*$. On a $\overline{2}^4 = -\overline{1}$, $\overline{2}^8 = 1$ donc $o(\overline{2}) = 8$. Les générateurs de l'unique sous-groupe d'ordre 8 de $(\mathbb{Z}/17\mathbb{Z})_*$ sont donc $\overline{2}$, $\overline{2}^3 = \overline{8}$, $\overline{2}^5 = \overline{15}$, $\overline{2}^7 = \overline{9}$. Les solutions sont $n = 2$ ou 8 ou 15 ou $9 \pmod{17}$.

Ex 12 - 19

D'après 12-6, prop., pour tout $n \in \mathbb{Z}^*$, tous les diviseurs premiers de $\Phi_{2^{k+1}}(n) = n^{2^k} + 1$ sont de la forme $m2^{k+1} + 1$ et il existe une infinité de nombres premiers de cette forme.

Ex 12 - 20

S'il existait $k < n$ tels que $\Phi_{2^{k+1}}(m)$ et $\Phi_{2^{n+1}}(m)$ aient un facteur premier commun p alors $X^{2^{n+1}} - 1 = \Phi_{2^{n+1}}(X) \cdots \Phi_{2^{k+1}}(X) \cdots \Phi_1(X)$ aurait pour racine multiple $\overline{m}$ dans le corps $\mathbb{Z}/p\mathbb{Z}$. On aurait $p \mid 2^{n+1}$, soit $p = 2$. Comme $\Phi_{2^{n+1}}(m) = m^{2^n} + 1$ est impair, c'est impossible. Donc $\Phi_{2^{k+1}}(m)$ et $\Phi_{2^{n+1}}(m)$ sont premiers entre eux.

Ex 12 - 21

Raisonnons par l'absurde. Supposons qu'il existe k avec $0 \leqslant k \leqslant p-2$ et $1 < a \leqslant b$ tels que $k^2 + k + p = ab$. Soit k minimum dans $\mathbb{N}$ avec cette propriété. On a

(1) $\qquad (k-a)^2 + (k-a) + p = (a-k-1)^2 + (a-k-1) + p = a(a+b-2k-1)$,

avec $1 < a$ et $a + b - 2k - 1 > 1$. En effet, puisque $k < p - 1$, on a

$$2k + 2 = 2\sqrt{k^2 + 2k + 1} < 2\sqrt{k^2 + k + p} = 2\sqrt{ab} \leqslant a + b.$$

Compte tenu de (1), puisque k est minimum, on a $k - a < 0$, soit $a - k - 1 \geqslant 0$, et $k \leqslant a - k - 1$, soit $2k + 1 \leqslant a$. On en déduit

$(2k+1)^2 \leqslant a^2 \leqslant ab = k^2 + k + p$, d'où $3k^2 + 3k + 1 \leqslant p$ soit $(k + \frac{1}{2})^2 \leqslant \frac{p}{3} - \frac{1}{12}$.

Ainsi on a $k \leqslant -\frac{1}{2} + \sqrt{\frac{p}{3} - \frac{1}{12}} < \sqrt{\frac{p}{3}}$. Puisque $k^2 + k + p$ est premier pour $k = 0, \ldots, E(\sqrt{\frac{p}{3}})$ c'est contradictoire. Donc pour $0 \leqslant k \leqslant p-2$ le nombre n_k est premier.

Si $p = 11$, on a $E(\sqrt{\frac{11}{3}}) = 1$. Comme $n_0 = 11$, $n_1 = 13$ sont premiers, n_k est premier pour $0 \leqslant k \leqslant 9$.

Si $p = 17$, on a $E(\sqrt{\frac{17}{3}}) = 2$. Comme $n_0 = 17$, $n_1 = 19$, $n_2 = 23$ sont premiers, n_k est premier pour $0 \leqslant k \leqslant 15$.

Si $p = 41$, on a $E(\sqrt{\frac{41}{3}}) = 3$. Comme $n_0 = 41$, $n_1 = 43$, $n_2 = 47$, $n_3 = 53$ sont premiers, n_k est premier pour $0 \leqslant k \leqslant 39$. Par exemple, $n_{39} = 1601$ est premier.

Ex 12 - 22

D'après 12-6, cor., tout diviseur de $F_6 = 2^{2^6} + 1$ est de la forme $m2^7 + 1 = m128 + 1$. Il suffit de tester la divisibilité de F_6 pour ces valeurs. Le calcul numérique aboutit à $F_6 = 274\,177 \times 67\,280\,421\,310\,721$, avec $274\,177 = 128 \times 2\,142 + 1$.

Chapitre 13

Nombres algébriques

13.1 Eléments algébriques d'une algèbre

Définitions.

Soient K un corps commutatif, A une algèbre unifère sur K. Un élément $\alpha \in A$ est dit algébrique sur K, s'il existe un polynôme non nul $f \in K[X]$ tel que $f(\alpha) = 0$. Le degré du polynôme minimal f_α de α sera appelé le degré de α.

Nous avons vu en 11-2, cor. que si $\alpha \in A$, alors $J_\alpha = \{f \in K[X] \mid f(\alpha) = 0\}$ est un idéal de l'anneau principal $K[X]$. Si $J_\alpha \neq \{0\}$, (c'est-à-dire si α est algébrique, le polynôme minimal f_α de α est le générateur unitaire de l'idéal J_α. Nous noterons $K(\alpha)$ la sous-algèbre de A engendrée par α et 1.

Soit E un espace vectoriel de dimension finie sur un corps (commutatif) K et soit $u \in \mathcal{L}(E)$. Le polynôme minimal f_u de u joue un rôle important dans l'étude de l'endomorphisme u. Par exemple, u est triangulable si et seulement si f_u est scindé, u est diagonalisable si et seulement si f_u est scindé avec racines simples.

On peut voir $\mathbb{R}$ ou $\mathbb{C}$, comme des algèbres sur leur sous-corps premier $\mathbb{Q}$. Conformément à la définition, un nombre réel ou complexe, est algébrique sur $\mathbb{Q}$ (on dit tout simplement algébrique), s'il est racine d'un polynôme $f \in \mathbb{Q}[X]$ non nul. En réduisant au même dénominateur les fractions que sont les coefficients de f, on voit qu'un nombre est algébrique si et seulement s'il est racine d'un polynôme non nul de $\mathbb{Z}[X]$. Par exemple, $\sqrt{2}$, $\sqrt[3]{2}$, $\frac{1}{\sqrt[3]{2}}$, $1+\sqrt{2}$ sont racines des polynômes X^2-2, X^3-2, $2X^3-1$, X^2-2X-1. Ils sont donc algébriques.

Proposition.

Soit A une algèbre unifère sur le corps K. Soit $\alpha \in A$ algébrique sur K.

(i) *On a $K(\alpha) = \{f(\alpha)\,;\, f \in K[X]\}$. C'est une algèbre isomorphe à $K[X]/J_\alpha$.*

(ii) *Tout élément de $K(\alpha)$ a une expression unique de la forme $a_0 1 + \cdots + a_{n_1}\alpha^{n-1}$ où $n = \mathrm{d}^\circ(f_\alpha)$ et où $a_0, \ldots, a_{n-1} \in K$. Autrement dit, $K(\alpha)$ est un espace vectoriel sur K de dimension $n = \mathrm{d}^\circ(f_\alpha)$. Il admet $(1, \alpha, ..., \alpha^{n-1})$ pour base.*

(iii) *Les conditions suivantes sont équivalentes : a) $K(\alpha)$ est intègre, b) $K(\alpha)$ est un corps, c) f_α est un polynôme irréductible.*

Démonstration. (i) Pour tout polynôme $f(X) = a_n X^n + \cdots + a_0$ de $K[X]$, on a $f(\alpha) = a_n\alpha^n + \cdots + a_0 1 \in K(\alpha) \subset A$. L'application $\varphi : f \mapsto f(\alpha)$ est un homomorphisme d'algèbres (homomorphisme d'anneaux linéaire), de $K[X]$ dans$A$. Son image

$\{f(\alpha)\,;\ \ f \in K[X]\}$ est une sous-algèbre commutative de $K(\alpha)$. Elle contient α, 1. Elle est donc égale à la sous-algèbre $K(\alpha)$ de A engendrée par 1 et α. Factorisons $\varphi : f \mapsto f(\alpha)$ à travers son noyau J_α. On obtient un homomorphisme d'anneaux injectif $\overline{\varphi} : K[X]/J_\alpha \to \mathrm{Im}\,(\varphi) = \{f(\alpha)\,;\ f \in K[X]\} = K(\alpha)$.

(ii) La division euclidienne de $f \in K[X]$ par f_α, donne $f(X) = q(X)f_\alpha(X) + r(X)$ avec $r(X) = a_0 + \cdots + a_{n-1}X^{n-1}$ de degré au plus $n-1$. On en déduit que $f(\alpha) = r(\alpha)$ est de la forme $a_0 1 + \cdots + a_{n-1}\alpha^{n-1}$ avec $a_0, ..., a_{n-1} \in K$.

Les éléments $1, \alpha, ..., \alpha^{n-1}$ de $K(\alpha)$ sont libres sur le corps K. En effet, si une combinaison linéaire non triviale $b_0 1 + \cdots + b_{n-1}\alpha^{n-1}$ était nulle, il existerait un polynôme non nul, de degré au plus $n-1$ annulant α, ce qui contredirait le fait que le générateur f_α, de l'idéal $\mathrm{Ker}\,(\varphi)$ soit le polynôme unitaire de plus bas degré annulant α.

(iii) L'anneau $K(a)$ est isomorphe à $K[X]/J_\alpha$, par $\overline{\varphi}$. L'équivalence des conditions a), b), c) se déduit donc de 11-8, prop. ∎

Corollaire 1

L'élément α de l'algèbre A est algébrique sur K, si et seulement si $K(\alpha)$ est un sous-espace vectoriel de A de dimension finie sur K. Et dans ce cas, la dimension de $K(\alpha)$ sur K est le degré $\mathrm{d}^\circ(f_\alpha)$ de α.

Démonstration. D'après la proposition, si α est algébrique, alors $K(\alpha)$ est de dimension finie sur K, égale à $\mathrm{d}^\circ(f_\alpha)$. Réciproquement, si $K(\alpha)$ est de dimension finie n, alors les $n+1$ éléments $1, \alpha, \ldots, \alpha^n$ de $K(\alpha)$ sont liés. Il existe $a_0, \ldots, a_n \in K$, non tous nuls, tels que $a_0 1 + a_1\alpha + \cdots + a_n\alpha^n = 0$ et α est algébrique sur K. ∎

Corollaire 2

Supposons que l'algèbre A soit un anneau intègre. Soit $\alpha \in A$ algébrique sur K et soit $f \in K[X]$ unitaire tel que $f(\alpha) = 0$. Pour que f soit le polynôme minimal de α il faut et il suffit que f soit irréductible.

Démonstration. La condition est nécessaire d'après la proposition. Réciproquement, s'il existe $f \in K[X]$ unitaire, et donc non nul, tel que $f(\alpha) = 0$, alors α est algébrique et f est multiple du polynôme minimal f_α. Si f est irréductible, cela oblige $f = f_\alpha$. ∎

Corollaire 3

Supposons que l'algèbre A soit de dimension finie N sur le corps K. Alors, tout élément α de A est algébrique sur K, de degré au plus N.

Démonstration. On a $K(\alpha) \subset A$ donc $K(\alpha)$ est un sous-espace vectoriel de A de dimension finie majorée par N, d'où le résultat d'après le cor.1. ∎

13.2 Une application à l'algèbre linéaire

Proposition.

Soient E un espace vectoriel de dimension finie n sur le corps K et $u \in \mathcal{L}(E)$. Supposons que $\{0\}$ et E soient les seuls sous-espaces vectoriels de E stables par u. Alors le polynôme minimal f_u de u est irréductible de degré $\dim(E)$.

Démonstration. Nous avons prouvé et utilisé cet énoncé en 8-2. Donnons une autre démonstration et d'autres applications classiques de ce résultat. L'algèbre $\mathcal{L}(E)$ est

de dimension finie n^2. Tout $u \in \mathcal{L}(E)$ est donc algébrique d'après 13-1, cor.3. Avec l'hypothèse faite, vérifions que $K(u)$ est intègre. Considérons deux éléments $g(u)$ et $h(u)$ de $K(u)$, où $g, h \in K\{X\}$. Supposons que $g(u)h(u) = 0$ et $h(u) \neq 0$. On a $\mathrm{Im}\,(h(u)) \neq \{0\}$ et $\mathrm{Im}\,(h(u)) \subset \mathrm{Ker}\,(g(u))$ donc $\mathrm{Ker}\,(g(u)) \neq \{0\}$. Si on suppose $g(u) \neq 0$ alors $\mathrm{Ker}\,(g(u)) \neq E$. Or $\mathrm{Ker}\,(g(u))$ est un sous-espace stable par u car u et $g(u)$ commutent. Cela contredit l'hypothèse faite sur E. On a donc $g(u) = 0$ ou $h(u) = 0$ et K est intègre.

D'après la prop. 13-1-(iii), le polynôme minimal de u est irréductible et $K(u)$ est un corps. Comme en 8-2, lemme 2, on voit ensuite que $\dim(E) = \mathrm{d}^\circ(f_u)$. ∎

Corollaire 1.

Considérons un espace vectoriel euclidien E et $u \in \mathcal{L}(E)$.

(i) *Supposons u symétrique. Il existe une base orthonormée de E qui diagonalise u.*

(ii) *Supposons u antisymétrique. Il existe une base orthonormée de E dans laquelle la matrice de u est bloc-diagonale, avec un bloc nul correspondant au noyau de u et des blocs de format 2 antisymétriques.*

(iii) *Supposons que u commute avec son adjoint u^*. Il existe une base orthonormée de E dans laquelle la matrice de u est bloc-diagonale, avec des blocs de format 1 associés aux valeurs propres, des blocs de format 2 de la forme $\begin{pmatrix} \alpha & -\beta \\ \beta & \alpha \end{pmatrix}$.*

Démonstration. (i) Dans l'anneau $\mathbb{R}[X]$, les polynômes irréductibles sont de degré 1 ou 2. Choisissons un sous-espace vectoriel F invariant par u, distinct de $\{0\}$, de dimension minimum. Il est de dimension 1 ou 2 d'après la proposition.

Montrons qu'il est de dimension 1. Supposons que $\dim(F) = 2$ et que $u = u^*$. On a $(u(x)|y) = (x|u(y))$ pour tous $x, y \in E$ et donc pour tous $x, y \in F$. L'endomorphisme v induit par u sur le sous-espace stable F est donc symétrique. Dans une base orthonormée de F, la matrice de u est donc symétrique, soit $\begin{pmatrix} a & b \\ b & c \end{pmatrix}$.

Le polynôme caractéristique de cette matrice $X^2 - (a+c)X + (ac - b^2)$ a un discriminant $\Delta = (a+c)^2 - 4ac + 4b^2 = (a-c)^2 + 4b^2 \geqslant 0$. Ainsi v a une valeur propre. Il existe une droite vectorielle de F, engendrée par un vecteur propre non nul, invariante par u. Cela contredit le fait que F soit de dimension minimum. Donc F est de dimension un, formé de vecteurs propres.

Si $F \neq E$, son orthogonal $F^\perp$ est alors stable par u car u est symétrique. On peut appliquer à l'endomorphisme induit par u sur $F^\perp$, le raisonnement précédent. On obtient une autre droite de vecteurs propres. En itérant, on construit par récurrence une base orthonormée de E qui diagonalise u.

(ii) Supposons que $u^* = -u$. Comme en (i), choisissons F invariant de dimension minimum, égale à 1 ou 2. Si $F \neq E$, alors $F^\perp$ est stable par u. On peut choisir un deuxième sous-espace invariant dans $F^\perp$ de dimension 1 ou 2. En itérant, on décompose E comme somme directe orthogonale de droites stables par u (la valeur propre correspondante est nulle car $u* = -u$) et de sous-espaces stables par u minimaux de dimension deux. En choisissant des bases orthonormées de ces sous-espaces, on obtient le résultat.

(iii) Supposons que $u^*u = uu^*$. Posons $f = \frac{1}{2}(u + u^*)$, $g = \frac{1}{2}(u - u^*)$. L'endomorphisme f est symétrique. D'après (i), E est somme directe orthogonale des sous-espaces propres de f. Comme g commute avec f, il laisse stable tout sous-espace propre E_λ, de f. Ainsi, f et g laissent stable E_λ et induisent des endomorphismes $f_\lambda = \lambda\,\mathrm{Id}_{E_\lambda}$ et g_λ

de E_λ. Comme g est antisymétrique, g_λ est antisymétrique et (ii) lui est applicable. Il existe une base orthonormée de E_λ dans laquelle g_λ a une matrice bloc-diagonale, avec des blocs de format 1 correspondant à des vecteurs du noyau de g_λ, et des blocs de format 2 antisymétriques et donc de la forme $\begin{pmatrix} 0 & -\beta \\ \beta & 0 \end{pmatrix}$. La matrice de f_λ étant $\lambda \mathbb{1}$, on obtient le résultat annoncé pour $u = f + g$. ∎

Corollaire 2.

Considérons un espace vectoriel hermitien E et $u \in \mathcal{L}(E)$. Si u est normal, c'est-à-dire si $uu^* = u^*u$, il existe une base orthonormée de E qui diagonalise u et u^*.

Démonstration. Les polynômes irréductibles de $\mathbb{C}[X]$ sont de degré 1. En raisonnant comme dans le cor.1(i), on décompose E en somme directe orthogonale de sous-espaces vectoriels invariants par u de dimension 1, c'est-à-dire de sous-espaces propres. ∎

Exercice.. Soient E un espace vectoriel, $u \in \mathcal{L}(E))$ et F un sous-espace vectoriel de E stable par u. On note v l'endornorphisme $u_{|F}$ de F induit par u.
a) Montrer que le polynôme minimal f_v de v divise le polynôme minimal de u. En déduire que si u est diagonalisable, alors v est diagonalisable.
b) Supposons qu'il existe un supplémentaire F' de F stable par u. Calculer f_u en fonction de f_v et de $f_{v'}$, où $v' = u_{|F'}$.

Solution. **a)** Si $f_u(X) = a_0 + \cdots + a_n X^n$, on a $(a_0 \operatorname{Id}_E + \cdots + a_n u^n)(x) = 0$ pour tout $x \in$E et donc pour tout $x \in F$. Ainsi, $f_u(v) = 0$ et f_u un élément de l'idéal J_v. Il est donc multiple de f_v .

On sait que u est diagonalisable si et seulement s'il existe un polynôme scindé à racines simples qui annule u ou encore si f_u est scindé à racines simples. Dans ce cas, f_v qui divise f_u est scindé à racines simples et v est diagonalisable.
b) Soit $f(X) = b_0 + \cdots + b_m X^m$ un élément de $K[X]$. On a $f \in J_u$ si pour tout $x = y + y' \in E = F \oplus F'$, où $y \in F$ et $y \in F'$ on a
$0 = f(u)(x) = (b_0 \operatorname{Id}_E + \cdots + b_m u^m)(y + y') = f(u)(y) + f(u)(y')$, d'où

$$\begin{aligned} f \in J_u &\Leftrightarrow \forall y \in F\ f_u(y) = 0 \quad \text{et} \quad \forall y' \in F'\ f_u(y') = 0 \\ &\Leftrightarrow f(v) = 0 \quad \text{et} \quad f(v') = 0 \\ &\Leftrightarrow f \in J_v \cap J_{v'} \ . \end{aligned}$$

Le générateur f_u de $J_u = J_v \cap J_{v'}$ est le ppcm des générateurs f_v et $f_{v'}$ de J_v et $J_{v'}$.

13.3 Nombres transcendants

Définitions.

Soient K_1 un corps (commutatif) et K un sous-corps de K_1. Si $\alpha \in K_1$ n'est pas algébrique sur K, on dit que α est transcendant sur K. En particulier, si $\alpha \in \mathbb{C}$ n'est pas algébrique sur $\mathbb{Q}$, on dit que α est un nombre transcendant.

D'après 13-1, $\alpha \in K_1$ est algébrique sur K si $J_\alpha = \{fEK[X] | f(\alpha) = 0\} = \operatorname{Ker}(\varphi)$ est non nul ou de manière équivalente, si $[K(\alpha) : K] < +\infty$(13-1, cor. 1).

Donc $\alpha \in K_1$ est transcendant sur K si et seulement si l'homomorphisme d'anneaux $\varphi : f \mapsto f(\alpha)$ est injectif ou encore si la dimension $[K(\alpha) : K]$ de $K(\alpha)$ sur K est infinie. La propriété universelle du corps des fractions $K(X)$ de $K[X]$ fournit alors un homomorphisme φ' de $K(X)$ dans le corps $K(\alpha)$ prolongeant φ. Comme $K(X)$ est un corps, φ' est injectif et son image est un sous-corps de $K(\alpha)$ isomorphe à $K(X)$.

Ce sous-corps contient K et α. Il est donc égal à $K(\alpha)$. Si $\alpha \in K_1$ est transcendant sur K, alors $K(\alpha)$ est isomorphe au corps $K(X)$ des fractions rationnelles sur K. La réciproque est vraie car le corps $K(X)$ des fractions rationnelles sur K est un espace vectoriel de dimension infinie sur K puisqu'il contient $K[X]$.

Remarque. Rappelons que $\mathbb{Q}$ est dénombrable : il est en bijection avec le sous-ensemble de $\mathbb{Z} \times \mathbb{N}^*$ constitué des fractions $\frac{p}{q}$ réduites, où $p \wedge q = 1$. L'ensemble $\mathcal{P}_n$ des polynômes de $\mathbb{Q}[X]$ de degré majoré par n est en bijection avec $\mathbb{Q}^{n+1}$ et donc dénombrable. L'ensemble des polynômes $\mathbb{Q}[X] = \cup \mathcal{P}_n$, réunion dénombrable d'ensembles dénombrables est dénombrable. Tout $p \in \mathbb{Q}[X]$ n'a qu'un nombre fini de racines. L'ensemble $\mathcal{A}$ des nombres algébriques est donc une partie dénombrable de $\mathbb{C}$.

Or $\mathbb{C}$ n'est pas dénombrable. Son cardinal est $2^{\mathrm{card}(\mathbb{N})}$ distinct de card $(\mathbb{N})$ d'après un th. de Cantor. On en déduit que l'ensemble des nombres transcendants, complémentaire de $\mathcal{A}$ dans $\mathbb{C}$, est infini, non dénombrable, de cardinal $2^{\mathrm{card}(\mathbb{N})}$. La théorie des cardinaux de Cantor (élaborée vers 1880) montre donc qu'il existe "énormément" de nombres transcendants. Néanmoins, on connaît très peu de nombres transcendants, faute de caractérisations simples de ces nombres. LIOUVILLE exhiba des nombres transcendants pour la première fois en 1844, en mettant en évidence une propriété que doit vérifier tout nombre algébrique. HERMITE montra en 1873 que e est transcendant. En adaptant sa démonstration, LINDEMANN montra en 1882 que π est transcendant. Voici le résultat de Liouville.

Lemme.

Considérons un nombre algébrique $\alpha \in \mathbb{R}$, de degré $n > 1$. Il existe une constante $k > 0$, qui ne dépend que de α, telle que pour tout $p \in \mathbb{Z}$ et tout $q \in N^*$ vérifiant $0 < \left|\alpha - \frac{p}{q}\right| \leqslant 1$, on ait $\left|\alpha - \frac{p}{q}\right| > \frac{k}{q^n}$.

Démonstration. Soit $f(X) = a_0 + \cdots + a_n X^n \in \mathbb{Z}[X]$, irréductible dans $\mathbb{Q}[X]$ de degré n, qui annule α. La fonction f' est continue. Il existe donc une constante $m > 0$ qui majore $|f'(x)|$ sur l'intervalle compact $[\alpha - 1, \alpha + 1]$. Si $\frac{p}{q} \in [\alpha - 1, \alpha + 1]$, on a

$$\left|f(\frac{p}{q})\right| = \frac{|a_0 q^n + a_1 q^{n-1} p + \cdots + a_n p^n|}{q^n} \geqslant \frac{1}{q^n} .$$

En effet, le numérateur est entier. Il est non nul car aucun rationnel ne peut être racine de $f(X)$ sinon $f(X)$ aurait un facteur de degré un dans $\mathbb{Q}[X]$ et ne serait pas irréductible dans $\mathbb{Q}[X]$. D'après le th. des accroissements finis, il existe c entre $\frac{p}{q}$ et α tel que

$$f(\frac{p}{q}) = f(\frac{p}{q}) - f(\alpha) = (\frac{p}{q} - \alpha) f'(c) .$$

On en déduit $\left|\frac{p}{q} - \alpha\right| = \frac{|f(\frac{p}{q})|}{|f'(c)|} > \frac{1}{mq^n}$. Il suffit de poser $k = \frac{1}{m}$. ∎

Proposition. (Liouville)

Le nombre $\alpha = \frac{1}{10} + \frac{1}{10^{2!}} + \cdots + \frac{1}{10^{n!}} + \cdots$ est transcendant. Plus généralement, $\sum_{n=1}^{\infty} \frac{a_n}{10^{n!}}$ est transcendant pour toute suite bornée d'entiers (a_n).

Démonstration. Les rationnels $x_n = \frac{1}{10} + \frac{1}{10^{2!}} + \cdots + \frac{1}{10^{n!}} = \frac{p}{q}$, où $q = 10^{n!}$, vérifient $0 < \alpha - \frac{p}{q} < \frac{2}{10^{(n+1)!}}$ incompatible avec la condition du lemme. ∎

13.4 Le corps des nombres algébriques

Définitions.

Si un corps K est sous-corps d'un autre corps commutatif K_1, nous dirons que K_1 est une extension de K.

La dimension, notée $[K_1 : K]$, de l 'espace vectoriel K_1 sur K, est appelée le degré de K_1 sur K. Si $[K_1 : K] = 2$, on dit que K_1 est une extension quadratique de K.

Si $\alpha_1, \ldots, \alpha_k$ sont des éléments de K_1, nous noterons $K(\alpha_1, \ldots, \alpha_k)$ le plus petit sous-corps de K_1 qui contient K et les éléments $\alpha_1, \ldots, \alpha_k$; (notation cohérente avec la notation $K(\alpha_1)$ déjà introduite, compte tenu de la prop. 13-1, (ii)*).*

Proposition.

Considérons un corps K, une extension K_1 de K et une extension K_2 de K_1.

(i) *Supposons $[K_1 : K] = p$ et $[K_2 : K_1] = q$ finis. Soient $(x_1, \ldots, x_p)$ une base de K_1 sur K et $(y_1, \ldots, y_q)$ une base de K_2 sur K_1, alors les éléments $(x_i y_j)$, où $1 \leqslant i \leqslant p$ et $1 \leqslant j \leqslant q$, est une base de K_2 sur K.*

(ii) *On a $[K_2 : K] = [K_2 : K_1][K_1 : K]$, ces valeurs étant finies ou infinies.*

Démonstration. (i) Soit $(x_1, \ldots, x_p)$ une famille de K_1 libre sur K et $(y_1, \ldots, y_q)$ une famille de K_2 libre sur K_1. Pour $1 \leqslant i \leqslant p$ et $1 \leqslant j \leqslant q$, considérons $\lambda_{ij} \in K$. Supposons que $0 = \sum_{i,j} \lambda_{ij} x_i y_j = \sum_j (\sum_i \lambda_{ij} x_i) y_j$. Pour tout j on a $\sum_i \lambda_{ij} x_i = 0$ car (y_j) est une famille libre sur K_1. Comme (x_i) est libre sur K, on en déduit que $\lambda_{ij} = 0$ pour tout j, tout i. Ainsi la famille $(x_i y_j)$ est libre sur K.

Vérifions que $(x_i y_j)$ engendre K_2 sur K. Soit $x \in K_2$. Il existe $\mu_1, \ldots, \mu_q \in K_1$ tels que $x = \mu_1 y_1 + \ldots + \mu_q y_q$ car (y_j) est base de K_2 sur K_1. Puisque (x_i) est une base de K_1 sur K, pour $j = 1, \ldots, q$ il existe $\lambda_{1j}, \ldots, \lambda_{pj} \in K$ tels que $\mu_j = \lambda_{1j} x_1 + \cdots + \lambda_{pj} x_p$ Ainsi, $x = \sum_{i,j} \lambda_{ij} x_i y_j$ et $(x_i y_j)$ est une base de K_2 sur K.

(ii) D'après (i), si $p = [K_1 : K]$ et $q = [K_2 : K_1]$ sont finis, alors K_2 est de dimension pq sur K. Si $[K_1 : K] = +\infty$, il existe dans K_1 des familles libres de cardinal arbitrairement grand donc $[K_2 : K] = +\infty$. De même, si $[K_2 : K1] = +\infty$. ∎

Corollaire 1.

Soient K un corps et L une extension de K. Si $[L : K]$ est un nombre premier alors K et L sont les seuls sous-corps de L contenant K. En particulier, pour tout $\alpha \in L$ n'appartenant pas à K, on a $K(\alpha) = L$.

Corollaire 2.

Soient K un corps et L une extension de K. L'ensemble $\mathcal{A}$ des éléments de L algébriques sur K est un sous-corps de L.

Démonstration. Les éléments α, β de L sont algébriques sur K si et seulement si $[K(a) : K]$ et $[K(\beta) : K]$ sont finis. Le polynôme minimal f_β de β sur K est aussi un élément de $K(\alpha)[X]$. Ainsi β est algébrique sur $K(\alpha)$. Son polynôme minimal sur $K(\alpha)$ divise f_β car $f_\beta(\beta) = 0$ donc $[K(\alpha)(\beta) : K(a)] \leqslant \mathrm{d}^\circ(f_\beta) = [K(\beta) : K]$ et

$$[K(\alpha)(\beta) : K] = [K(\alpha)(\beta) : K(\alpha)][K(\alpha) : K] \leqslant [K(\beta) : K][K(\alpha) : K] < \infty\,.$$

Le corps $K(\alpha, \beta) = K(a)(\beta)$ contient $\alpha + \beta$, $\alpha\beta$ et $1/\alpha$ si $\alpha \neq 0$. Les sous-corps $K(\alpha + \beta)$, $K(\alpha\beta)$, $K(1/\alpha)$ de $K(\alpha, \beta)$ sont donc de dimension finie sur K. D'après 13-1, cor.1, $\alpha + \beta$, $\alpha\beta$ et $1/\alpha$ sont algébriques sur K de degré au plus $\mathrm{d}^\circ(\alpha) \times \mathrm{d}^\circ(\beta)$. ∎

Exercice 1. Montrer que $\alpha = \sqrt{2}+\sqrt{3}$ est algébrique sur $\mathbb{Q}$. Donner son polynôme minimal, une base de $\mathbb{Q}(\sqrt{2}+\sqrt{3})$ sur $\mathbb{Q}$.
Montrer que $\mathbb{Q}(\sqrt{2}) \cap \mathbb{Q}(\sqrt{3}) = \mathbb{Q}$.

Solution. Puisque $\sqrt{2}$ et $\sqrt{3}$ sont algébriques sur $\mathbb{Q}$, racines de $X^2-2 \in \mathbb{Q}[X]$ et $X^2-3 \in \mathbb{Q}[X]$, le corollaire 2 montre que $\alpha = \sqrt{2}+\sqrt{3}$ est algébrique sur $\mathbb{Q}$, de degré au plus $d^\circ(\sqrt{2}) \times d^\circ(\sqrt{3})$. On sait que $\sqrt{2} \notin \mathbb{Q}$ (voir 9-9, ex. 2, b)). On a donc $[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] > 1$. Le degré de $\sqrt{2}$ sur $\mathbb{Q}$, c'est-à-dire le degré de son polynôme minimal $f_{\sqrt{2}}$, vérifie donc $d^\circ(f_{\sqrt{2}}) \geqslant 2$. Par ailleurs $f_{\sqrt{2}}$ divise X^2-2 qui annule $\sqrt{2}$. Donc $d^\circ(f_{\sqrt{2}}) = 2$ et $f_{\sqrt{2}} = X^2-2$. De même $f_{\sqrt{3}} = X^2-3$. On a donc $d^\circ(\alpha) \leqslant 2 \times 2 = 4$.

Une base de l'extension quadratique $\mathbb{Q}(\sqrt{2})$ de $\mathbb{Q}$ est $(1, \sqrt{2})$ et $\mathbb{Q}(\sqrt{2})$ est l'ensemble des nombres $\alpha+\beta\sqrt{2}$ où $\alpha, \beta \in \mathbb{Q}$ (expression unique). De même, $\sqrt{3}$ est de degré 2 sur $\mathbb{Q}$ et $\mathbb{Q}(\sqrt{3}) = \{\lambda+\mu\sqrt{3}\,;\ \lambda, \mu \in \mathbb{Q}\}$.

Considérons maintenant X^2-2 comme un polynôme à coefficients dans $\mathbb{Q}(\sqrt{3})$. S'il était réductible dans $\mathbb{Q}(\sqrt{3})[X]$, il aurait une racine dans $\mathbb{Q}(\sqrt{3})$, autrement dit $\sqrt{2}$ ou $-\sqrt{2}$ serait élément de $\mathbb{Q}(\sqrt{3})$. Il existerait $a, b \in \mathbb{Q}$ tels que $\sqrt{2} = a+b\sqrt{3}$. On devrait avoir $b \neq 0$ sinon $\sqrt{2} = a \in \mathbb{Q}$ et $a \neq 0$ sinon $2 = 3b^2$ et 3 diviserait 2. De la relation $2 = a^2+3b^2+2ab\sqrt{3}$ on déduirait que $\sqrt{3} \in \mathbb{Q}$. C'est absurde. Ainsi X^2-2 est irréductible sur le corps $\mathbb{Q}(\sqrt{3})$ et $\sqrt{2}$ est algébrique de degré 2 sur $\mathbb{Q}(\sqrt{3})$. Donc $K = \left(\mathbb{Q}(\sqrt{3})\right)(\sqrt{2}) = \mathbb{Q}(\sqrt{3}, \sqrt{2})$ est de degré 2 sur $\mathbb{Q}(\sqrt{3})$ et

$$[K : \mathbb{Q}] = [K : \mathbb{Q}(\sqrt{3})][\mathbb{Q}(\sqrt{3}) : \mathbb{Q}] = 2 \times 2 = 4.$$

Le corps $\mathbb{Q}(\alpha)$ contient $\alpha = \sqrt{2}+\sqrt{3}$ et $\alpha^3 = 11\sqrt{2}+9\sqrt{3}$. En tirant $\sqrt{2}$ et $\sqrt{3}$ de ce système de Cramer on voit que $\mathbb{Q}(\alpha)$ contient $\sqrt{2}$ et $\sqrt{3}$ et contient donc le sous-corps $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ de $\mathbb{R}$. Réciproquement, $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ contient $\alpha = \sqrt{2}+\sqrt{3}$ et contient donc $\mathbb{Q}(\alpha)$. Ainsi,

$$\mathbb{Q}(\alpha) = \mathbb{Q}(\sqrt{2}, \sqrt{3}) = \left(\mathbb{Q}(\sqrt{3})\right)(\sqrt{2}) = K \quad \text{et} \quad [\mathbb{Q}(\alpha) : \mathbb{Q}] = 4.$$

On a $\alpha^2 = 5+2\sqrt{6}$, d'où $(\alpha^2-5)^2 = 24$. Ainsi $f(X) = X^4-10X^2+1$ a pour racine α. Le polynôme minimal f_α, de α divise f. Il a pour degré $[\mathbb{Q}(a) : \mathbb{Q}] = 4$ et il est unitaire. Donc $f = f_\alpha$, et f est irréductible. D'après 13-1, prop. (ii), $(1, \sqrt{2})$ est une base de $\mathbb{Q}(\sqrt{2})$ sur $\mathbb{Q}$ et $(1, \sqrt{3})$ est une base de $\left(\mathbb{Q}(\sqrt{2})\right)(\sqrt{3})$ sur $\mathbb{Q}(\sqrt{2})$. La proposition précédente montre que $(1, \sqrt{2}, \sqrt{3}, \sqrt{6})$ est une base de $\mathbb{Q}(\alpha)$ sur $\mathbb{Q}$. Une autre base est $(1, \alpha, \alpha^2, \alpha^3)$ d'après 13-1, prop.

D'après la proposition, la dimension sur $\mathbb{Q}$ du sous-corps $L = \mathbb{Q}(\sqrt{2}) \cap \mathbb{Q}(\sqrt{3})$ de $\mathbb{R}$ divise $[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2$. Si on avait $[L : 1] = 2$, on aurait $L = \mathbb{Q}(\sqrt{2})$ et pareillement $L = \mathbb{Q}(\sqrt{3})$. C'est impossible car $\sqrt{2} \notin \mathbb{Q}(\sqrt{3})$. Donc $[L : 1] = 1$ et $L = \mathbb{Q}$.

Exercice 2. Montrer que $f(X) = X^4-2X^2+9$ est irréductible dans $\mathbb{Q}[X]$.

Solution. Calculons dans $\mathbb{C}$ les racines de ce polynôme bicarré. Posons $Y = X^2$. On a $Y^2-2Y+9 = (Y-1)^2+8 = (Y-1)^2-(2i\sqrt{2})^2 = (Y-1-2i\sqrt{2})(Y-1+2i\sqrt{2})$, avec $1+2i\sqrt{2} = 2+2i\sqrt{2}-1 = (\sqrt{2}+i)^2 \quad , \quad X^2 = 1-2i\sqrt{2} = (\sqrt{2}-i)^2$.

Les racines de $f(X)$ sont $\alpha = \sqrt{2}+i$, $\sqrt{2}-i, -\sqrt{2}+i$ et $-\sqrt{2}-i$. En résolvant le système $\alpha = \sqrt{2}+i$, $\alpha^3 = -\sqrt{2}+5i$ on voit que i et $\sqrt{2}$ sont combinaisons linéaires sur $\mathbb{Q}$ de α et α^3. Donc $\mathbb{Q}(\alpha)$ contient i et $\sqrt{2}$. Ainsi $\mathbb{Q}(\alpha)$ contient $\mathbb{Q}(\sqrt{2})$ et $\mathbb{Q}(\sqrt{2})(i)$ qui est de degré 4 sur $\mathbb{Q}$. D'après la proposition, 4 divise $[\mathbb{Q}(a) : \mathbb{Q}] = d^\circ(f_\alpha)$. Le polynôme minimal f_α de α divise f car $f(\alpha) = 0$ donc $d^\circ(f_\alpha) \leqslant 4$. Ainsi, $d^\circ(f_\alpha) = [\mathbb{Q}(a) : \mathbb{Q}] = 4$. Comme f_α divise f, on a $f = f_\alpha$ qui est irréductible.

13.5 Constructions à la règle et au compas

Dans le plan affine euclidien $\mathcal{E}$ considérons une famille finie $\mathcal{F}_0 = \{M_1, \dots, M_d\}$ de points distincts avec $d \geqslant 2$. Considérons les droites D_{ij} de $\mathcal{E}$ qui passent par deux points distincts M_i , M_j de $\mathcal{F}_0$ et les cercles $C_{k\ell}$ centrés en l'un des points M_k et passant par un autre point M_ℓ de la famille. Soit $\mathcal{F}_1$ la famille des points de $\mathcal{E}$ qui sont intersection de deux de ces courbes (droites D_{ij} ou cercles $C_{k\ell}$). On a $\mathcal{F}_0 \subset \mathcal{F}_1$. On définit de même une famille $\mathcal{F}_2$ de points de $\mathcal{E}$ à partir de $\mathcal{F}_1$ et par récurrence des familles finies croissantes $\mathcal{F}_0 \subset \mathcal{F}_1 \subset \cdots \subset \mathcal{F}_m \subset \cdots$.

Définition.

Les points de $\cup_m \mathcal{F}_m$ sont dits constructibles à la règle et au compas à partir des points de $\mathcal{F}_0 = \{M_1, \dots, M_d\}$. En abrégé, nous dirons qu'ils sont constructibles.

Choisissons un repère orthonormé $R = (O, \overrightarrow{\imath}, \overrightarrow{\jmath})$ de $\mathcal{E}$, tel que $O \in \mathcal{F}_0$ et $A = O + \overrightarrow{\imath} \in \mathcal{F}_0$ (quitte a changer l'unité de longueur cela est possible). Soit K_0 le sous-corps de $\mathbb{R}$ engendré par les coordonnées $(x_1, y_1), \dots, (x - d, y_d)$ de ces points.

L'équation $(y_j - y_i)(X - x_i) - (x_j - x_i)(Y - y_i) = 0$ de la droite D_{ij} est de la forme $aX + bY + c = 0$ avec $a, b, c \in K_0$. Si deux telles droites sont sécantes, leur intersection est un point de $\mathcal{F}_1$ dont les coordonnées s'obtiennent en résolvant le système de Cramer de leurs deux équations. Les formules de Cramer montrent que ces coordonnées sont des éléments du corps K_0.

L'équation $(X - x_k)^2 + (Y - y_k)^2 - [(x_\ell - x_k)^2 + (y_\ell - y_k)^2] = 0$ du cercle $C_{k\ell}$ est de la forme $X^2 + Y^2 - 2uX - 2vY + w = 0$ où $u, v, w \in K_0$. Pour trouver les coordonnées des points d'intersection de la droite D_{ij} et du cercle $C_{k\ell}$ on peut tirer X (ou Y) de l'équation de la droite, le reporter dans l'équation du cercle. Cela conduit à une équation du second degré en Y (ou en X), à coefficients dans K_0. Toute racine α dans $\mathbb{C}$ de ce trinôme a pour polynôme minimal un diviseur de ce trinôme donc $[K_0(\alpha) : K_0] = 1$ ou 2. Ensuite l'autre coordonnée, déduite de α en utilisant l'équation $aX + bY + c = 0$ est encore un élément de $K_0(\alpha)$.

L'intersection de deux cercles $C_{k\ell}$, $C_{k'\ell'}$ de centres distincts, d'équations

$$X^2 + Y^2 - 2uX - 2vY + w = 0 \quad , \quad X^2 + Y^2 - 2u'X - 2v'Y + w' = 0,$$

est également l'intersection de $C_{k\ell}$ et de la droite, axe radical des deux cercles, d'équation $2(u - u')X + 2(v - v') - (w - w') = 0$ à coefficients dans K_0. Les coordonnées des points d'intersection de $C_{k\ell}$ et $C_{k'\ell'}$ sont donc, comme précédemment, algébriques sur K_0, de degré 2 sur K_0 si elles n'appartiennent pas à K_0. Ainsi, les coordonnées de tout point de $\mathcal{F}_1$ appartiennent à K_0 ou sont algébriques sur K_0 de degré 2.

Théorème. (Wantzel)

Pour que $M \in \mathcal{E}$, de coordonnées x, y soit constructible à partir des points $M_1, \dots, M_d$, il faut et il suffit qu'il existe $s \in \mathbb{N}$, des extensions $K_0 \subset K_1 \subset \cdots \subset K_s$ de K_0 dans $\mathbb{R}$ telles que $x, y \in K_s$ et $[K_i : K_{i-1}] = 2$ pour $i = 1, \dots, s$.

En particulier, pour que M soit constructible, il est nécessaire que les coordonnées (x, y) de M soient algébriques sur le corps K_0 engendré par les coordonnées de $M_1, \dots, M_d$, dans le repère R et que leurs degrés soient des puissances de 2 sur K_0.

Démonstration. Supposons M construit à partir de $M_1, \dots, M_d$, à l'aide de p constructions à la règle et au compas successives. La première construction a donné un point M_{d+1} dont les coordonnées appartiennent à un sous-corps K_1 de $\mathbb{R}$ qui est égal à K_0 ou de degré $[K_1 : K_0] = 2$ sur K_0. A la deuxième étape, on construit un point M_{d+2}

dont les coordonnées appartiennent à une extension K_2 de K_1 égale à K_1 ou de degré 2 sur K_1. On opère ainsi p fois. Les coordonnées du point M obtenu à la $p^{\text{ième}}$ étape appartiennent à une extension K_p du corps K_{p-1} précédent, telle que $[K_p : K_{p-1}] = 1$ ou 2. En ne considérant que les extensions successives telles que$[K_1 : K_{i-1}] = 2$, on voit (13-4, prop.) que la condition énoncée est nécessaire.

Montrons qu'elle est suffisante. D'abord, tout élément de K_0 est constructible à partir de $M_1, \ldots, M_d$. En effet, on détermine les abscisses et ordonnées x_i, y_i de $M_1, \ldots, M_d$ à la règle et au compas, par projection des points sur les axes et report. Ensuite tout élément de K_0 est obtenu par un nombre fini d'additions, produits, prises d'inverse à partir de ces coordonnées. Or, dans $\mathbb{R}$ ou $\mathbb{C}$, la somme $z + z'$, le produit zz', l'inverse $1/z$ si $z \neq 0$ se construisent à la règle et au compas (voir exercice ci-dessous).

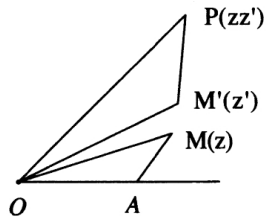
Considérons maintenant une extension K_1 de K_0 de degré 2. Soit α un élément de K_1 qui n'appartient pas à K_0. Comme $[K_1 : K_0] = 2$ est premier on a $[K_0(\alpha) : K_0] = 2$ donc le polynôme minimal de α est de degré deux, soit $X^2 - 2aX + b = (X - a)^2 - \delta$, où $a, b, \delta = a^2 - b$ sont éléments de K_0. Si $\delta = |\delta| e^{i\theta} \neq 0$, alors δ, $\overline{\delta}$, $|\delta|$, $e^{i\theta/2}$ se construisent à la règle et au compas. Les racines $\alpha = a + |\delta|^{1/2} e^{i\theta/2}$ et $\alpha' = a - |\delta|^{1/2} e^{i\theta/2}$ sont constructibles. Par récurrence, on voit que dans une suite d'extensions successives $K_0 \subset K_1 \subset \cdots \subset K_s$ où chacune est de degré 2 sur la précédente, tout point sera constructible. La condition est donc suffisante.

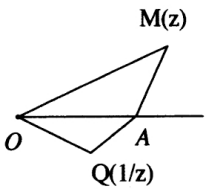
Les coordonnées (x, y) de M étant éléments de K_s, $[K(x) : K_0]$ et $[K(y) : K_0]$ divisent $[K_s : K_0] = [K_s : K_{s-1}] \times \cdots \times [K_1 : K_0] = 2^s$. Ce sont des puissances de 2. ∎

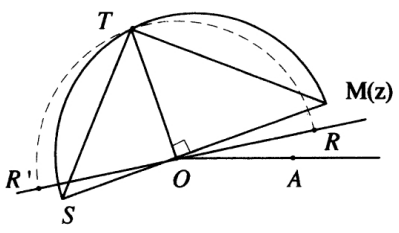
Remarque. Le fait que les coordonnées x et y de M soient algébriques, de degré puissances de 2 sur K_0, n'est pas suffisant pour que M soit constructible. Par exemple, il existe des extensions de $\mathbb{Q}$ de degré 4 ne contenant aucun sous-corps de degré 2.

Exercice. Montrer que l'ensemble K des éléments de $\mathbb{C}$ constructibles à partir de $M_1, \ldots, M_d$, est un sous-corps de $\mathbb{C}$ et que si $z \in K$, alors ses racines carrées sont éléments de K.

Solution. Notons A le point d'affixe 1. Soient $z \in K$ et $z' \in K$ et M, M' les points ayant ces affixes. Le point d'affixe $z + z'$ est le quatrième sommet du parallélogramme construit sur $\overrightarrow{OM}$ et $\overrightarrow{OM'}$. Il se construit au compas donc $z + z' \in K$. Le point P d'affixe zz' est tel que les triangles OAM et $OM'P$ soient semblables. Il se construit à la règle et au compas (report d'angle et d'une longueur proportionnelle à OM dans le rapport $\dfrac{OM'}{OA}$ connu). Le point Q d'affixe $1/z$, si $z \neq 0$, est tel que les triangles OQA et OAM soient semblables. Il est constructible. Si $z = 0$, sa racine carrée est zéro. Si $z \neq 0$, ses racines carrées s'obtiennent en traçant la bissectrice de $(\overrightarrow{Ox}, \overrightarrow{OM})$, ce qui se fait à la règle et au compas, et en portant à partir de O, de part et d'autre de O, des segments $[OR]$ et $[OR']$ de même longueur $\sqrt{|z|}$ que l'on peut par exemple déterminer comme hauteur $[TO]$ d'un triangle rectangle STM tel que $OS = 1$.







13.6 Quelques constructions à la règle et au compas

1 - Quadrature du cercle. Depuis l'antiquité, où la géométrie euclidienne s'était développée, on s'était beaucoup intéressé, pour les besoins des géomètres et des architectes, aux procédés de construction géométriques sur épures à l'aide des outils de ces professions : la règle et le compas. Les tracés des bissectrices d'un angle, de la médiatrice d'un segment, des médianes d'un triangle... faisaient partie de tout apprentissage de la géométrie. Prouver une telle construction était une étape obligée de toute étude de figure. Or certains problèmes devinrent rapidement célèbres car ils résistaient à toute tentative de ce genre. Ce n'est qu'à la fin du 19^e siècle que les progrès de l'algèbre apportèrent des éclaircissements sur ces questions (th. de Wantzel précédent).

Le plus célèbre de ces problèmes était celui de la quadrature du cercle. Le cercle est une figure essentielle et on pressentait que la nature du nombre π était impliquée. Etant donné un cercle C, on voulait construire, à la règle et au compas, un carré ayant la même surface. Considérons une demi-droite issue du centre O du cercle et le point A où elle rencontre C. La donnée de O et de A revient à donner le cercle C que l'on peut alors tracer au compas. Choisissons le centre O de C pour origine du plan. Quitte à changer l'unité de longueur, on peut supposer que $\overrightarrow{\imath} = \overrightarrow{OA}$ est unitaire. On considère le repère orthonormé direct $(O, \overrightarrow{\imath}, \overrightarrow{\jmath})$. Le sous-corps de $\mathbb{R}$ engendré par les coordonnées $(0,0)$ et $(0,1)$ des points O et A est $\mathbb{Q}$. Si on sait construire à la règle et au compas, à partir de O et A, un carré du plan d'aire égale à l'aire π du cercle C, on pourra ensuite le translater, en construisant des parallélogrammes et ramener un de ses sommets en O. Une rotation de centre O amènera ce sommet sur $[Ox)$. Toutes ces opérations s'effectuent à la règle et au compas. On voit donc que si la construction d'un tel carré était possible, alors le point de l'axe $(x'x)$ d'abscisse $c = \sqrt{\pi}$ serait constructible à la règle et au compas à partir de O et A.

Lindemann a montré en 1882 que π est transcendant. Donc $c = \sqrt{\pi}$ n'est pas algébrique sur $\mathbb{Q}$, (sinon $[\mathbb{Q}(c) : \mathbb{Q}]$ serait fini, le corps $\mathbb{Q}(c)$ contiendrait $c^2 = \pi$ qui serait algébrique). D'après le th. de Wantzel, la quadrature du cercle est impossible.

2 - Duplication du cube. On considère un cube $\Gamma = ABCDA'B'C'D'$. Quitte à modifier l'unité de longueur, on peut supposer que le repère $R = (A, \overrightarrow{AB}, \overrightarrow{AD}, \overrightarrow{AA'})$, constitué du sommet A et des arêtes issues de A, est orthonormé. On voudrait construire un cube Γ_1 de volume double du précédent, de sommets A et M avec $\overrightarrow{AM}$ et $\overrightarrow{AB}$ colinéaires et de même sens. Soit x l'abscisse de M dans le repère R. Les volumes de Γ et Γ_1 sont x^3 et 1. On doit avoir : $x^3 = 2$. Or $\sqrt[3]{2}$ est racine du polynôme $X^3 - 2$ et ce polynôme est irréductible sur $\mathbb{Q}$. En effet, si on avait $X^3 - 2 = (\alpha X + \beta)(\gamma X^2 + \delta X + \varepsilon)$ avec $\alpha, \beta, \gamma, \delta, \varepsilon \in \mathbb{Q}$ alors le polynôme $X^3 - 2$ aurait une racine $-\dfrac{\alpha}{\beta}$ dans $\mathbb{Q}$. Cette racine serait égale à l'unique racine réelle $\sqrt[3]{2}$ de $X^3 - 2$. Or le nombre $\sqrt[3]{2}$ n'est pas rationnel. Ainsi $X^3 - 2$ est irréductible. C'est donc le polynôme minimal de $\sqrt[3]{2}$, qui est donc algébrique de degré 3 sur $\mathbb{Q}$. Ce n'est pas une puissance de 2. Sa construction à la règle et au compas est impossible d'après le th. de Wantzel.

3 - Trisection d'un angle. On sait construire à la règle et au compas la bissectrice d'un angle de vecteurs. Peut-on construire de même, les demi-droites qui divisent cet angle en trois angles égaux ?

Considérons un repère orthonormé du plan ayant pour origine le sommet de l'angle, dont l'un des axes est un côté de l'angle et tel que la mesure α de l'angle soit comprise entre 0 et 2π. On veut construire θ tel que $3\theta = \alpha$. Cela revient à construire le point M

d'intersection du cercle trigonométrique avec la demi-droite d'angle polaire θ. Puisque $\cos 3\theta = 4\cos^3\theta - 3\cos\theta$,, on voit que $\cos\theta$ est racine de l'équation :

$$4X^3 - 3X - \cos\alpha = 0\,.$$

Par exemple, avec $\alpha = 2\pi/3$ ce polynôme a pour expression $8X^3 - 6X + 1$. Posons $Y = 2X$. Il devient $Y^3 - 3Y + 1$. En raisonnant comme dans l'exemple 2, on peut vérifier qu'il est irréductible sur $\mathbb{Q}$. On peut aussi poser $Y = Z - 1$. Il devient $Z^3 - 3Z^2 + 3$ irréductible d'après le critère d'Eisenstein (voir 14-5, rem. a)). L'abscisse $\cos\theta$ de M est algébrique de degré 3 sur $\mathbb{Q}$. On ne peut donc pas construire M à la règle et au compas.

4 - Polygones réguliers. Dans le plan euclidien $\mathcal{E}$ muni d'un repère orthonormé $(O, \overrightarrow{\imath}, \overrightarrow{\jmath})$ tout le monde sait construire à la règle et au compas :

- l'hexagone régulier et le triangle équilatéral qui ont pour centre O et pour sommet le point A de coordonnées $(1, 0)$, et par récurrence le polygone régulier ayant 3×2^n côtés, où $n \in \mathbb{N}^*$, en traçant les bissectrices des angles au centre du polygone ayant $3 \times 2^{n-1}$ côtés,

- le carré, puis l'octogone à 8 côtés, de centre O et de sommet A et par récurrence le polygone régulier ayant 2^n côtés, où $n \in \mathbb{N}^*$.

Pour tout $n \geqslant 2$, peut-on construire de même, le polygone régulier à n côtés ? Représentons ses sommets à l'aide de leurs affixes. Celles-ci sont les racines $n^{\text{ièmes}}$ de l'unité dans $\mathbb{C}$. Si on sait construire la racine primitive $\zeta = \exp(i\frac{2\pi}{n})$, les autres sommets s'en déduisent par des reports au compas sur le cercle trigonométrique. Or ζ est racine du polynôme cyclotomique $\Phi_n(X)$ qui a ses coefficients dans $\mathbb{Z}$. Dans la théorie de Galois, il est classique que $\Phi_n(X)$ est irréductible sur $\mathbb{Q}$ et donc polynôme minimal de ζ. Nous démontrerons ce résultat en 14-6.

Si $[\mathbb{Q}(\zeta) : \mathbb{Q}] = \mathrm{d}^\circ(\Phi_n)) = \varphi(n)$ n'est pas une puissance de 2, la construction à la règle et au compas de ζ est impossible. C'est le cas, pour $n = 7$, pour $n = 9\ldots$ Dans ce dernier cas, on retrouve l'impossibilité de la trisection de l'angle, puisqu'il faudrait diviser en trois, à la règle et au compas, l'angle de mesure $\frac{2\pi}{3}$ du triangle équilatéral.

Pour $n = 5$ on a $\varphi(5) = 2^2$. La condition nécessaire de la proposition est vérifiée. La construction est effectivement possible (Voir exercice qui suit)

Pour $n = 17$ on a $\varphi(17) = 2^4$. Une construction à la règle et au compas fut donnée en 1796 par Gauss, âgé alors de 19 ans. Quand on examine cette construction, on voit clairement des extensions successives de degré 2, conduisant à celle qui contient ζ. En 1801, Gauss a caractérisé les valeurs de $n \in \mathbb{N}^*$ pour lesquelles le polygone régulier $\mathcal{P}_n$ de centre O de sommet A est constructible.

Proposition. (Gauss)

Pour que $\mathcal{P}_n$ soit constructible il faut et il suffit que $n = 2^k p_1 \cdots p_s$, où $p_1, \ldots, p_s$ sont des nombres de Fermat premiers, distincts.

Démonstration. Montrons que la condition est nécessaire, en utilisant le fait, démontré en 14-6, que le polynôme cyclotomique $\Phi_n(X)$ est irréductible sur $\mathbb{Q}$ et donc polynôme minimal de $z = \exp(i\frac{2\pi}{n})$. Soit $n = p_1^{k_1} \cdots p_s^{k_s}$ la décomposition de n en facteurs premiers. Si z est constructible, alors $\mathrm{d}^\circ(\Phi_n) = \varphi(n) = p_1^{k_1-1}(p_1 - 1) \cdots p_s^{k_s-1}(p_s - 1)$ est une puissance de 2. Chacun des facteurs $p_1^{k_1-1}(p_1 - 1), \ldots, p_s^{k_s-1}(p_s - 1)$ est une puissance de 2. Si 2 est facteur premier de n, cette condition est réalisée pour le terme correspondant. Considérons un premier impair p. Pour que $p^{k-1}(p-1)$ soit puissance

de 2, il faut que $k = 1$ et que $p - 1 = 2m$. En mettant en facteur dans m la puissance de 2 maximum, on obtient $m = 2^r q$, d'où $p = (2^{2^r})^q + 1 = (2^{2^r} + 1) \sum_{k=0}^{q-1} (-1)^k (2^{2^r})^k$. Comme p est premier, on a nécessairement $q = 1$ et $p = 2^{2^r} + 1$. Donc p est un nombre de Fermat premier.

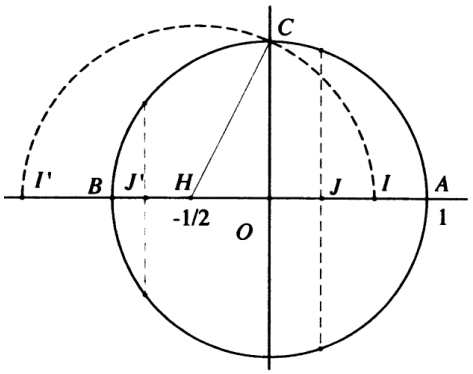
Pour limiter la longueur de l'exposé, nous admettons que la condition est suffisante. ■

Remarque. On ne connaît à ce jour que 5 nombres de Fermat $2^{2^r} + 1$ premiers, pour $r = 0, 1, 2, 3, 4$ (voir 12-5). Pour n impair, on ne connaît donc qu'un nombre fini de valeurs de n impaires pour lesquelles $\mathcal{P}_n$ est constructible.

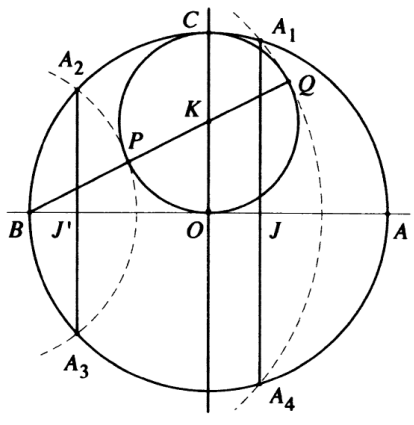
Exercice.. Dans le plan complexe, d'origine O, soit A le point d'affixe 1. Montrer que le pentagone régulier P de centre O, de sommet A est constructible à partir de O et A et donner une construction.

Solution. Puisque $5 = 2^2 + 1$ est le nombre premier de Fermat F_1, le th. de Gauss montre que P est constructible. Les affixes des sommets autres que A sont $\zeta, \zeta^2, \zeta^3, \zeta^4$, où $\zeta = \exp(i\frac{2\pi}{5})$. Ce sont les racines du polynôme cyclotomique $\Phi_4(X) = X^4 + X^3 + X^2 + X + 1$. On a donc :
$0 = \zeta^2 + \zeta + 1 + \zeta^{-1} + \zeta^{-2} = (\zeta^2 + \zeta^{-2}) + (\zeta + \zeta^{-1}) + 1 = 2\cos\frac{4\pi}{5} + 2\cos\frac{2\pi}{5} + 1 = 2(2(\cos\frac{2\pi}{5})^2 - 1) + 2\cos\frac{2\pi}{5} + 1$.
Ainsi, $\cos\frac{2\pi}{5}$ est racine de $4X^2 + 2X - 1$. Comme ζ^2 est une autre racine primitive de l'unité, racine de $\Phi_4(X)$, de même $\cos\frac{4\pi}{5}$ est racine de ce polynôme, d'où les valeurs $\cos\frac{2\pi}{5} = \frac{-1+\sqrt{5}}{4} > 0$ et $\cos\frac{4\pi}{5} = \frac{-1-\sqrt{5}}{4} < 0$.

Pour construire P, on trace le cercle de centre O et de rayon OA. On déterminer le milieu H de $[B0]$, d'affixe $-\frac{1}{2}$. Le cercle de centre H de rayon $HC = \sqrt{(\frac{1}{2})^2 + 1^2} = \frac{\sqrt{5}}{2}$ recoupe $(x'x)$ en des points I et I'. On construit les milieux J et J' de $[OI]$ et $[OI']$. Les perpendiculaires en J et J' à $(x'x)$ coupent le cercle trigonométrique aux sommets du pentagone distincts de A.



Signalons une autre construction. On trace le cercle de diamètre $[OC]$. Son centre K est le milieu de $[OC]$. La droite (BK) recoupe ce cercle en P et Q. Les cercles de centre B de rayons BP et BQ recoupent le cercle trigonométrique aux sommets du pentagone autres que A. En effet, $\{A1, A4\}$ est l'intersection des cercles d'équations,
$(x+1)^2 + y^2 = BQ^2 = \left(\frac{1+\sqrt{5}}{2}\right)^2$ et $x^2 + y^2 = 1$. Par différence, on obtient l'équation d'une droite qui passe par A et par B. C'est l'*axe radical* des deux cercles, d'équation $x = -\frac{1}{4} + \frac{\sqrt{5}}{4}$. De même, A_2 et A_3 ont pour abscisse $x = -\frac{1}{4} - \frac{\sqrt{5}}{4}$. On a bien obtenu les sommets du pentagone.



Exercices du chapitre 13

Ex 13 - 1

Soit E un espace vectoriel de dimension finie sur le corps K.

a) Soit $u \in \mathcal{L}(E)$. Montrer que les conditions suivantes sont équivalentes.
(i) u est diagonalisable.
(ii) Le polynôme minimal de u est scindé simple.
(iii) Il existe $p \in K[X]$ scindé simple annulant u.

b) Soient $u, v \in \mathcal{L}(E)$ diagonalisables qui commutent. Montrer qu'il existe une base de E qui diagonalise u et v.

c) Si $K = \mathbb{C}$, montrer que les endomorphismes diagonalisables sont partout denses dans $\mathcal{L}(E)$. Si $K = \mathbb{R}$, montrer que cette propriété n'est pas vérifiée.

Ex 13 - 2

Soit $a \in \mathbb{Q}[X]$ irréductible. Montrer que dans $\mathbb{C}[X]$ c'est un polynôme simple. Généraliser à d'autres corps.

Ex 13 - 3

Soient K un corps commutatif et $p \in K[X]$ irréductible tel que p' ne soit pas nul. Montrer que $f \in K[X]$ admet p comme facteur irréductible avec multiplicité si et seulement si p divise f et f'.

Ex 13 - 4

Soit K un corps commutatif. Montrer qu'il existe dans $K[X]$ une infinité de polynômes irréductibles.

Ex 13 - 5

Dans le plan euclidien, on considère le réseau R des points de coordonnées entières. Montrer qu'il n'existe pas de triangle équilatéral, plus généralement de polygone régulier non carré, dont les sommets appartiennent à R. Généraliser à d'autres réseaux.

Ex 13 - 6

Montrer que les nombres réels
$a_1 = \sqrt{2}$, $a_2 = \sqrt{1+a_1}$, $a_3 = \sqrt{1+a_2}$
sont algébriques. En utilisant le critère d'Eisenstein (voir 14-5), déterminer leur polynôme minimal. Pour $i = 1,2,3$ donner une base de $\mathbb{Q}(a_i)$ sur $\mathbb{Q}$.

Dans le plan affine euclidien muni d'un repère orthonormé, montrer que les points A_i de coordonnées $(a_i, 0)$ sont constructibles à la règle et au compas à partir des points $O(0,0), A(1,0)$. Qu'en est-il pour le point $B(1+\sqrt[3]{2}, 0)$?

Ex 13 - 7

Soit A un anneau commutatif unifère et J son radical de Jacobson (intersection des idéaux maximaux de A).

a) Pour tout $x \in J$, montrer que $1-x$ est inversible dans A.

b) Si $A = K[X]$, où K est un corps commutatif, montrer que $J = \{0\}$.
Si $p \in K[X]$ est non nul, montrer qu'il existe une extension L de K et $\alpha \in L$ algébrique sur K tel que $p(\alpha) \neq 0$.

Ex 13 - 8

Soient K un corps, L une extension de K de degré m et $a \in K[X]$ unitaire irréductible de degré n. Si $m \wedge n = 1$, montrer que a est irréductible sur L.

Exemple 1. Montrer que $X^3 - 2$ est irréductible sur $\mathbb{Q}(i)$. En déduire que $X^6 + 4$ est irréductible sur $\mathbb{Q}$.

Exemple 2. Déterminer dans $\mathbb{C}$ le corps de décomposition du polynôme $X^5 - 7$.

Indications

Ex 13 - 1

a) Utiliser le lemme des noyaux.

b) Les sous-espaces propres de u sont stables par v. Les restrictions de v sont diagonalisables d'après a).

c) Si $K = \mathbb{C}$, dans une base convenable, u a une matrice A triangulaire. Approcher A par une suite (A_k) où A_k est triangulaire diagonalisable.

Sur $\mathbb{R}$, montrer par exemple qu'une matrice de rotation A n'est pas limite de matrices diagonalisables (considérer la trace de A et celle de A^2).

Ex 13 - 2

Si $\alpha \in \mathbb{C}$ était racine multiple de $a(X)$, elle annulerait $a'(X)$ dont le degré est inférieur à celui de $a(X)$.

Ex 13 - 3

Si $f = ph$ et si p divise f', d'après le lemme de Gauss, il doit diviser h.

Ex 13 - 4

On peut reprendre la démonstration d'Euclide montrant qu'il existe une infinité de nombres premiers.

Ex 13 - 5

S'il existait un tel polygone, $z = e^{2i\pi/n}$ appartiendrait au corps $\mathbb{Q}(i)$. Or le polynôme minimal de z est le polynôme cyclotomique $\Phi_n(X)$ de degré $\varphi(n)$.

Ex 13 - 6

a_1, a_2, a_3 sont racines des polynômes $X^2 - 2, X^4 - 2X^2 - 1, X^8 - 4X^6 + 4X^4 - 2$. Le critère d'Eisenstein montre qu'ils sont irréductibles (pour le deuxième, poser $X = Y + 1$). Ce sont les polynômes minimaux de a_1, a_2, a_3.

Ex 13 - 7

a) Si $1 - x$ n'était pas inversible, l'idéal $(1 - x)A$ de A serait contenu dans un idéal maximal M et on aurait $1 \in M$.

b) Si $a \in K[X]$ n'est pas nul, il n'appartient pas à J sinon $Xa(X)$ appartiendrait à J et $1 - Xa(X)$ serait inversible.

Ex 13 - 8

Dans $L[X]$, si $p(X)$ est un facteur irréductible de $a(X)$, $M = L[X]/(p)$ est une extension de L. La classe x de X dans M est racine de $p(X)$ et de $a(X)$.

Solutions des exercices du chapitre 13

Ex 13 - 1

a) (i) $\Rightarrow$ (iii) Supposons u diagonalisable. Soient $\lambda_1, \ldots, \lambda_k$ ses valeurs propres, et soient $E_1, \ldots, E_k$ ses sous-espaces propres. Alors $(u - \lambda_i \operatorname{Id})(x) = 0$ pour tout $x \in E_i$ et cela pour tout i. Le polynôme scindé simple $p(X) = (X - \lambda_1) \cdots (X - \lambda_k)$ est donc tel que $p(u)(x) = 0$ pour tout $x \in E = E_1 \oplus \cdots \oplus E_k$.

(iii) $\Rightarrow$ (ii) Si un polynôme $p(X)$ scindé simple annule u, alors le polynôme minimal de u divise $p(X)$. Il est donc scindé simple, produit de facteurs de degré un de $p(X)$.

(ii) $\Rightarrow$ (i) Si un polynôme scindé simple $p(X) = (X - \alpha_1) \cdots (X - \alpha_m)$ annule u, alors on a $E = \operatorname{Ker}(p(u)) = \operatorname{Ker}(u - \alpha_1 \operatorname{Id}_E) \oplus \cdots \oplus \operatorname{Ker}(u - \alpha_m \operatorname{Id}_E)$, (lemme des noyaux, voir 8-2, lemme 2). Donc u est diagonalisable.

b) Comme v commute avec u, les sous-espaces propres $E_1 = \operatorname{Ker}(u - \lambda_1 \operatorname{Id}_E), \ldots, E_k = \operatorname{Ker}(u - \lambda_k \operatorname{Id}_E)$ de u sont stables par v. Donc v induit sur $E_1, \ldots, E_k$ des endomorphismes $v_1, \ldots, v_k$. Le polynôme minimal $p(X)$ de v est scindé simple car v est diagonalisable. Alors $p(X)$ annule $v_1, \ldots, v_k$ qui sont donc diagonalisables d'après a), (iii). Il existe des bases $\mathcal{B}_1, \ldots, \mathcal{B}_k$ de $E_1, \ldots, E_k$ faites de vecteurs propres pour $v_1, \ldots, v_k$ et donc propres pour v. Ils sont propres également pour u. Alors $\mathcal{B} = \mathcal{B}_1 \cup \cdots \cup \mathcal{B}_k$ est une base de E. Elle diagonalise v et u.

c) Supposons que $K = \mathbb{C}$. Soit $u \in \mathcal{L}(E)$. Le polynôme caractéristique de u est scindé car $\mathbb{C}$ est algébriquement clos. Il existe donc une base $\mathcal{B} = (e_1, \ldots, e_n)$ de E dans laquelle le matrice A de u est triangulaire supérieure. Les valeurs $\lambda_1, \ldots, \lambda_n$ de la diagonale X de A sont les racines de $\det(\lambda I_n - A)$, c'est-à-dire les valeurs propres de u. Si certaines racines sont multiples, en notant d le plus petit des nombres $|\lambda_i - \lambda_j|$ non nuls, où $i \neq j$, la suite $X_k = (\lambda_1 + \frac{d}{nk}, \lambda_2 + 2\frac{d}{nk}, \ldots, \lambda_n + n\frac{d}{nk})$ converge dans $\mathbb{C}^n$ vers $X = (\lambda_1, \ldots, \lambda_n)$ lorsque $k \to \infty$ et pour $k > 1$ les coordonnées de X_k sont deux à deux distinctes. Les matrices A_k obtenues en remplaçant la diagonale X de A par X_k (sans modifier les autres coefficients) converge vers A et A_k est diagonalisable puisqu'elle a n valeurs propres distinctes.

Si $K = \mathbb{R}$, les matrices diagonalisables ne sont pas denses dans $\mathcal{M}_n(\mathbb{R})$. Par exemple, considérons $A = \begin{pmatrix} \cos(\pi/3) & -\sin(\pi/3) \\ \sin(\pi/3) & \cos(\pi/3) \end{pmatrix}$. Supposons qu'une suite (A_k) de matrices diagonalisables converge vers A. Alors (A_k^2) tend vers A^2. On a

$$A_k = P \begin{pmatrix} \lambda_k & 0 \\ 0 & \mu_k \end{pmatrix} P^{-1} \quad , \quad A_k^2 = P \begin{pmatrix} \lambda_k^2 & 0 \\ 0 & \mu_k^2 \end{pmatrix} P^{-1},$$

où P est une matrice de changement de base. On en déduit que

$$\lambda_k^2 + \mu_k^2 = \operatorname{tr}(A_k^2) \to \operatorname{tr}(A^2) = 2\cos(2\pi/3) = -1.$$

C'est absurde. Si $\dim(E) > 2$, on peut compléter la matrice A avec des 0 ou des 1 placés sur la diagonale et conclure de même.

Ex 13 - 2

Soit $a \in \mathbb{Q}[X]$ irréductible avec $d^\circ(a) \geqslant 2$. Supposons que $\alpha \in \mathbb{C}$ soit une racine multiple de a. Alors $a(\alpha) = 0$ et $a'(\alpha) = 0$, avec $d^\circ(a') = d^\circ(a) - 1 < d^\circ(a)$. Cela contredit le fait que a est le polynôme non nul de plus bas degré annulant α. Donc toute racine α de a dans $\mathbb{C}$ est une racine simple.

Si $a \in K[X]$, où K est un corps commutatif, il existe une extension K_0 de K algébriquement close (admis ici). Si $\text{caract}(K) = 0$, on conclut de la même façon que $a(X)$ est scindé simple sur K_0.

Si K est un corps fini, la conclusion est encore vraie. En effet, sa caractéristique est un nombre premier p. D'après 9-1, $\varphi : x \mapsto x^p$ est un homomorphisme du corps K dans lui-même. Il est injectif car $\{0\}$ et K sont les seuls idéaux de K et donc bijectif car K est fini. Supposons que $\alpha \in K_0$ soit racine multiple de $a(X)$. Si $a'(X)$ n'était pas le polynôme nul, comme précédemment cela contredirait le fait que $a(X)$ soit le polynôme minimal de α. Donc $a'(X)$ est nul, ce qui signifie que $a(X)$ est de la forme $a_0 + a_p X^p + a_{2p} X^{2p} + \cdots + a_{sp} X^{sp}$. Pour $i = 0, \ldots, s$, il existe b_i tel que $b_i^p = a_{ip}$. On a alors $a(X) = (b_0 + \cdots + b_s X^s)^p$ car $K[X]$ est de caractéristique p. C'est absurde car $a(X)$ est irréductible. Donc sur K_0, ce polynôme est scindé simple.

Ex 13 - 3

Supposons qu'il existe $h \in K[X]$, tel que $f = p^2 h$. On obtient :
$f' = 2pp'h + p^2 h' = p(2p'h + ph')$ donc p divise f'.
Réciproquement, si p divise f, il existe $h \in K[X]$ tel que $f = hp$ et donc $f' = h'p + hp'$. Si en outre p divise f', alors p divise hp'. D'après le lemme de Gauss, il divise h ou p'. Comme p' n'est pas nul et $d^\circ(p') \leqslant d^\circ(p) - 1$, il est impossible que p divise p'. Donc p divise h et p^2 divise f.

Ex 13 - 4

Reprenons la démonstration d'Euclide montrant qu'il existe une infinité de nombres premiers. La famille $\mathcal{F}$ des polynômes unitaires irréductibles de $K[X]$ n'est pas vide (elle contient tout polynôme de degré un). Supposons $\mathcal{F}$ finie, d'éléments $p_1, \ldots, p_k$. Considérons $p(X) = p_1(X) \cdots p_k(X) + 1$. On a $d^\circ(p) \geqslant 1$ donc p possède un diviseur q irréductible. Or $q \notin \mathcal{F}$ sinon q diviserait 1. C'est absurde. Donc $\mathcal{F}$ est infinie.
On peut aussi démontrer le résultat en utilisant le fait que les polynômes $X^{2^k} + 1$, où $k \in \mathbb{N}^*$, sont deux à deux premiers entre eux (voir Ex. 12-20).

Ex 13 - 5

Supposons qu'il existe un polygone régulier $P = A_1 \cdots A_n$, avec $n \geqslant 3$, dont les sommets A_k d'affixes z_k appartiennent à $R = \mathbb{Z} + i\mathbb{Z}$. L'isobarycentre O des sommets, d'affixe $z_0 = \frac{1}{n}(z_1 + \cdots + z_n)$ appartient au corps $\mathbb{Q}(i)$ donc $\zeta = \frac{z_2 - z_0}{z_1 - z_0} = e^{2i\pi/n} \in \mathbb{Q}(i)$. Cela nécessite que $\mathbb{Q}(\zeta) \subset \mathbb{Q}(i)$ et donc que $[\mathbb{Q}(\zeta) : 1]$ divise $[\mathbb{Q}(i) : 1] = 2$. Comme $\zeta \notin \mathbb{Q}$, on doit avoir $2 = [\mathbb{Q}(\zeta) : 1] = \varphi(n)$ (voir 14-6, prop.). Or, $\varphi(n) = 2$ n'est possible que si $n = 3, 4$ ou 6. Pour $n \notin \{2, 3, 6\}$, le problème n'a pas de solution.

Si $n = 3$ ou 6 (P est un triangle équilatéral ou un hexagone régulier), on doit avoir $\sqrt{3} = 2\,\text{Im}\left(e^{2i\pi/3}\right) = 2\,\text{Im}\left(e^{2i\pi/6}\right) \in \mathbb{Q}$. C'est impossible car $\sqrt{3} \notin \mathbb{Q}$.

Si $n = 4$, il existe de manière évidente des carrés ayant leurs sommets sur le réseau. C'est la seule valeur de n pour laquelle le problème a des solutions.

Généralisation. Soit $d < 0$ un entier sans diviseur carré (autre que 1). Alors $\mathbb{Q}(i\sqrt{|d|})$ est une extension de degré 2 de $\mathbb{Q}$. S'il existait un polygone régulier P à n côtés dont les sommets sont sur le réseau $A = \mathbb{Z} + i\mathbb{Z}|d|$, on aurait $[\mathbb{Q}(\zeta) : 1] = 2$. Comme précédemment, si $n \notin \{2,3,6\}$, le problème est sans solution. Si $n = 3, 4$ ou 6, on a $\zeta = j$ ou i ou $-j^2$. Si P existe, on a $\zeta \in \mathbb{Q}(i\sqrt{|d|})$ et donc $\mathbb{Q}(j)$ ou $\mathbb{Q}(i)$ ou $\mathbb{Q}(j^2)$ égal à $\mathbb{Q}(i\sqrt{|d|})$. Les extensions quadratiques de $\mathbb{Q}$ étant deux à deux non isomorphes (9-9, ex. 2), d est égal à -1 ou -3 ou -6. Dans ces cas il existe des triangles équilatéraux ou des carrés ou des hexagones réguliers ayant leurs sommets sur A.

Ex 13 - 6

$a_1 = \sqrt{2}$ est racine de $p_1(X) = X^2 - 2$. Le critère d'Eisenstein est vérifié pour le nombre premier 2. Donc $p_1(X)$ est irréductible dans $\mathbb{Q}[X]$. D'après 13-1, cor. 2, $p_1(X)$ est le polynôme minimal sur $\mathbb{Q}$ de $a_1 = \sqrt{2}$ et $K_1 = \mathbb{Q}(\sqrt{2})$ est une extension de degré 2 de $\mathbb{Q}$, admettant $\{1, \sqrt{2}\}$ comme base sur $\mathbb{Q}$.

Puisque $a_2 = \sqrt{1 + a_1}$ est tel que $a_1 = (a_2^2 - 1)$, c'est une racine du polynôme $p_2(X) = p_1(X^2 - 1) = X^4 - 2X^2 - 1$. On a $p_2(Y + 1) = Y^4 + 4Y^3 + 4Y^2 - 2$.

Le critère d'Eisenstein est vérifié pour le nombre premier 2. Donc $p_2(X)$ est irréductible. C'est le polynôme minimal de a_2. L'extension $K_2 = \mathbb{Q}(a_2)$ de $\mathbb{Q}$ est de degré 4 et admet comme base $\mathcal{B} = (1, a_2, a_2^2, a_2^3)$ sur $\mathbb{Q}$. Puisque $4 = [K_2 : \mathbb{Q}] = [K_2 : K_1][K_1 : \mathbb{Q}]$ et $K_1 \subset K_2$ car $a_1 \in K_2$, c'est une extension de degré 2 de K_1. Sur K_1, elle admet comme base $(1, a_2)$. Sur $\mathbb{Q}$, elle a comme base $\mathcal{B}' = (1, a_1, a_2, a_1a_2)$ (voir 13-4, prop.).

Puisque $a_3 = \sqrt{1 + a_2}$ est tel que $a_2 = (a_3^2 - 1)$, il est racine du polynôme $p_3(X) = p_2(X^2 - 1) = X^8 - 4X^6 + 4X^4 - 2$. Le critère d'Eisenstein montre qu'il est irréductible. C'est le polynôme minimal de a_3. Ainsi, $K_3 = \mathbb{Q}(a_3)$ est une extension de degré 8 de $\mathbb{Q}$. C'est une extension de degré 2 de K_2. Elle admet comme base $(1, a_3, \ldots, a_3^7)$ sur $\mathbb{Q}$ et également $(1\ ,\ a_1\ ,\ a_2\ ,\ a_1a_2\ ,\ a_3\ ,\ a_1a_3\ ,\ a_2a_3\ ,\ a_1a_2a_3)$.

Puisqu'il existe une suite $K_0 = \mathbb{Q} \subset K_1 \subset K_2 \subset K_3$ d'extensions de $\mathbb{Q}$, où chacune est de degré 2 sur la précédente, le th. de Wantzel montre que a_1, a_2, a_3 sont constructibles. D'ailleurs, leur construction est facile en utilisant le th. de Pythagore. Pour $a_1 = \sqrt{2}$, c'est la longueur de la diagonale d'un carré $OABC$ de côté OA. En plaçant la pointe sèche du compas en O, on peut rabattre OB sur l'axe des abscisses en $A_1(a_1, 0)$. Pour a_2, c'est la longueur de la diagonale d'un rectangle OA_1BC_1, etc...

Le point $B(1 + \sqrt[3]{2}, 0)$ n'est pas constructible, sinon $C(\sqrt[3]{2}, 0)$ le serait également. Or la duplication du cube, à la règle et au compas, est impossible.

Ex 13 - 7

a) Soit $x \in J$. Si $1 - x$ n'était pas inversible dans A, l'idéal $(1 - x)A$ serait distinct de A et serait donc contenu dans un idéal maximal M de A. Ayant $x \in J$ et $J \subset M$, on en déduirait que $1 \in M$ et donc $M = A$. C'est absurde.

b) Soit $a \in K[X]$ non nul. Si on avait $a \in J$, le polynôme $Xa(X)$ appartiendrait à J et $1 - Xa(X)$ serait inversible. C'est absurde car les unités de $K[X]$ sont les constantes non nulles.

Soit $p \in K[X]$, non nul. Nous venons de voir que $p \notin J$. Il existe donc un idéal maximal M de $K[X]$ ne contenant pas p. Si q est un générateur de M, c'est un polynôme irréductible de $K[X]$. D'après 13-1, $L = K[X]/M$ est un corps. C'est une extension de K de degré fini égal à $\mathrm{d}^\circ(q)$. En notant α la classe de X dans L, le polynôme minimal de α est q. On a $p(\alpha) \neq 0$, sinon p serait un multiple de q, ce qui est exclu car $p \notin M$.

Ex 13 - 8

Soit $p(X) = a_0 + \cdots + a_s X^s$ un facteur irréductible unitaire de $a(X)$ dans l'anneau $L[X]$. Soit $q \in L[X]$ tel que $a(X) = p(X)q(X)$. D'après 11-8, prop., l'idéal (p) engendré par p dans $L[X]$, est maximal et $M = L[X]/(p)$ est un corps. C'est une extension de L (comme en 11-8, pour la construction de $\mathbb{C}$) et donc de K. La classe $x \in M$ du polynôme X est telle que $0 = a_0 1 + \cdots + a_s x^s$. Dans M, c'est une racine de $p(X)$ (M est corps de rupture pour $p(X)$). D'après 13-1, prop. et cor. 2, on a $M = L(x)$ et $p(X)$ est le polynôme minimal de x sur L. Donc $[M : L] = \mathrm{d}^\circ(p)$ et

$$[M : K] = [M : L]\,[L : K] = d^\circ(p) \times m\,.$$

De plus, $x \in M$ est racine de $a(X) = p(X)q(X)$. Comme $a(X)$ est irréductible sur K, c'est le polynôme minimal de x sur K. On a $K(x) \subset M$ et donc :

$$[M : K] = [M : K(x)]\,[K(x) : K] = [M : K(x)]\,d^\circ(a) = [M : K(x)]\,n\,.$$

Comme $m \wedge n = 1$, on voit que $n = \mathrm{d}^\circ(a)$ divise $\mathrm{d}^\circ(p)$ et donc que $\mathrm{d}^\circ(a) \leqslant \mathrm{d}^\circ(p)$. Comme $p(X)$ divise $a(X)$, on a $a(X) = p(X)$, irréductible dans $L[X]$.

Exemple 1. $\sqrt[3]{2}$ est racine de $a(X) = X^3 - 2$. Le critère d'Eisenstein montre que $a(X)$ est irréductible sur $\mathbb{Q}$. L'extension $L = \mathbb{Q}(i)$ de $\mathbb{Q}$ est de degré 2 sur $\mathbb{Q}$. Puisque $2 \wedge 3 = 1$, ce qui précède montre que $a(X) = X^3 - 2$ est irréductible sur L. C'est donc le polynôme minimal de $\sqrt[3]{2}$ sur $L = \mathbb{Q}(i)$. On a donc :

$$[\mathbb{Q}(i)(\sqrt[3]{2}) : \mathbb{Q}] = [\mathbb{Q}(i)(\sqrt[3]{2}) : \mathbb{Q}(i)]\,[\mathbb{Q}(i) : \mathbb{Q}] = \mathrm{d}^\circ(a) \times 2 = 6\,.$$

On a $i\sqrt[3]{2} \in \mathbb{Q}(i, \sqrt[3]{2})$ et donc $\mathbb{Q}(i\sqrt[3]{2}) \subset \mathbb{Q}(i, \sqrt[3]{2})$. Par ailleurs, on a $(i\sqrt[3]{2})^3 = -2i$ et donc $i \in \mathbb{Q}(i\sqrt[3]{2})$ et $\sqrt[3]{2} = -i(i\sqrt[3]{2}) \in \mathbb{Q}(i\sqrt[3]{2})$. On en déduit que $\mathbb{Q}(i, \sqrt[3]{2}) \subset \mathbb{Q}(i\sqrt[3]{2})$ et donc que $\mathbb{Q}(i, \sqrt[3]{2}) = \mathbb{Q}(i\sqrt[3]{2})$. Le polynôme minimal $q(X)$ de $i\sqrt[3]{2}$ sur $\mathbb{Q}$ est donc de degré 6. Comme $X^6 + 4$ admet pour racine $i\sqrt[3]{2}$, il est multiple de $q(X)$. Etant unitaire, de même degré, il lui est égal. Ainsi $X^6 + 4$ est le polynôme minimal de $i\sqrt[3]{2}$. Il est donc irréductible.

Exemple 2. D'après le critère d'Eisenstein, $a(X) = X^5 - 7$ est irréductible dans $\mathbb{Q}[X]$. C'est donc le polynôme minimal de $\alpha = \sqrt[5]{7}$ et $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 5$. De même, $\beta = e^{2i\pi/5}$ est racine du polynôme cyclotomique $\Phi_5(X) = X^4 + X^3 + X^2 + X + 1$, qui est irréductible (voir 14-6 ou appliquer le critère d'Eisenstein à $\Phi_5(Y + 1)$). Donc $\Phi_5(X)$ est le polynôme minimal de β et $[\mathbb{Q}(\beta) : \mathbb{Q}] = 4$.

Comme $5 \wedge 4 = 1$, ce qui précède montre que $a(X)$ est irréductible sur $\mathbb{Q}(\beta)$. Comme dans l'exemple précédent, on en déduit que $\mathbb{Q}(\beta)(\alpha) = \mathbb{Q}(\alpha, \beta)$ est de degré $4 \times 5 = 20$ sur $\mathbb{Q}$. Ce corps est le sous-corps de $\mathbb{C}$ engendré par les racines du polynôme $X^5 - 7$ (corps de décomposition de $X^5 - 7$).

Notons que $\mathbb{Q}(\alpha) \cap \mathbb{Q}(\beta)$ est un sous-corps de $\mathbb{Q}(\alpha)$ et de $\mathbb{Q}(\beta)$ par suite $[\mathbb{Q}(\alpha) \cap \mathbb{Q}(\beta) : \mathbb{Q}]$ divise $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 5$ et $[\mathbb{Q}(\beta) : \mathbb{Q}] = 4$. On en déduit que $[\mathbb{Q}(\alpha) \cap \mathbb{Q}(\beta) : \mathbb{Q}] = 1$ et que $\mathbb{Q}(\alpha) \cap \mathbb{Q}(\beta) = \mathbb{Q}$.

Chapitre 14

Anneaux factoriels

14.1 Une généralisation des anneaux principaux

Comme nous l'avons vu, les anneaux principaux possèdent des propriétés relatives à la divisibilité, qui les rendent à bien des égards très proches de $\mathbb{Z}$. C'est notamment le cas de l'anneau $K[X]$, où K est un corps commutatif.

Toutefois, si l'anneau A est principal, l'anneau $A[X]$ n'est en général pas principal. Par exemple, $\mathbb{Z}[X]$ n'est pas principal (11-2, ex.). Or l'étude des nombres algébriques, qui sont comme $\sqrt{2}$, $\sqrt{\sqrt{2}-1}$, ... racines de polynômes à coefficients entiers, utilise les propriétés de l'anneau $\mathbb{Z}[X]$, notamment pour caractériser leur polynôme minimal.

On est conduit à introduire une catégorie d'anneaux plus générale que celle d'anneau principal, dans laquelle on ait encore une bonne théorie de la divisibilité. Pour cela, on prend comme définition, une propriété démontrée en 11-5, prop. pour les anneaux principaux qui rentreront ainsi dans cette nouvelle catégorie d'anneaux.

Définition 1.

Un anneau commutatif unifère A est dit factoriel, s'il est intègre et si tout $a \in A$ non nul, non inversible, admet une décomposition $a = p_1 \cdots p_k$, où $k \in \mathbb{N}$ et où $p_1, \ldots, p_k$, sont irréductibles dans A, cette décomposition étant unique dans le sens suivant : si $a = q_1 \cdots q_m$, est une autre expression de ce type, alors $m = k$ et il existe une permutation $s \in \mathcal{S}_k$ telle que p_i et $q_{s(i)}$ soient associés pour $i = 1, \ldots, k$.

Comme dans 11-5, déf., il sera commode de choisir un "système d'irréductibles" $\mathcal{P}$, c'est-à-dire une famille d'éléments irréductibles de A telle que tout élément irréductible soit associé à un élément de la famille $\mathcal{P}$ et un seul (on choisit un représentant dans chaque classe d'équivalence modulo "être associé").

Dans toute la suite de ce chapitre, on suppose fait un tel choix. Tout élément $a \in A$ non nul admet alors une expression unique de la forme $a = u p_1^{\alpha_1} \cdots p_k^{\alpha_k}$, où $u \in A_*$, où $p_1, \ldots, p_k \in \mathcal{P}$ sont distincts et où $\alpha_i \in \mathbb{N}^*$ pour $i = 1, \ldots, k$. Les unités de A auront alors une expression de ce type en prenant $k = 0$.

Définition 2.

Nous appellerons "décomposition en facteurs irréductibles" de a, cette expression de $a \in A \setminus \{0\}$.

Nous noterons $\mathrm{irr}(a)$ *l'ensemble $\{p_1, \ldots, p_k\}$ des facteurs irréductibles de a.*

Nous dirons que $a \neq 0$ et $b \neq 0$ sont premiers entre eux, si $\mathrm{irr}(a) \cap \mathrm{irr}(b) = \emptyset$.

Nous noterons $a \wedge b = 1$ cette propriété.

Proposition 1.

Soit A un anneau factoriel. Considérons $a \in A \setminus \{0\}$ et sa décomposition en facteurs irréductibles $a = up_1^{\alpha_1} \cdots p_k^{\alpha_k}$. Les diviseurs de a sont les éléments de la forme :

$$b = vp_1^{\beta_1} \cdots p_k^{\beta_k} \text{ où } v \in A_* \text{ et } 0 \leqslant \beta_i \leqslant \alpha_i \text{, pour } i = 1, \ldots k$$

Démonstration. La démonstration de 11-5, cor.1, s'applique sans rien y changer. ∎

Corollaire 1.

Soit $p \in A$ irréductible. Si p divise a, il est associé à l'un des facteurs $p \in \mathrm{irr}(a)$.

Démonstration. D'après la proposition, $p = vp_1^{\beta_1} \cdots p_k^{\beta_k}$. Comme p est irréductible, le second membre ne comporte qu'un seul irréductible qui est un associé de p. ∎

Corollaire 2.

Soient a, b des éléments non nuls de A. Un élément irréductible p de A divise ab si et seulement si p est associé à l'un des éléments de $\mathrm{irr}(a) U \mathrm{irr}(b)$.

Proposition 2.

Soient A un anneau factoriel et a, b des éléments non nuls de A. Alors a et b s'expriment de manière unique, sous la forme :

$$a = up_1^{\alpha_1} \cdots p_k^{\alpha_k} \qquad , \qquad b = vp_1^{\beta_1} \cdots p_k^{\beta_k}$$

avec $u \in A_*$, $v \in A_*$ et $p_i \in \mathrm{irr}(a) \cup \mathrm{irr}(b)$, $\alpha_i \geqslant 0$, $\beta_i \geqslant 0$ pour $1 \leqslant i \leqslant k$.
Pour $1 \leqslant i \leqslant k$, posons $\gamma_i = \min(\alpha_i, \beta_i)$, $\delta_i = max(\alpha_i, \beta_i)$. Alors,

$$d = p_1^{\gamma_1} \cdots p_k^{\gamma_k} \quad \text{et} \quad m = p_1^{\delta_1} \cdots p_k^{\delta_k}$$

sont un plus grand commun diviseur et un plus petit commun multiple de a et b.
De plus, il existe $w \in A_*$ tel que $ab = wdm$.

Démonstration. Les démonstrations de 11-5, cor.2, s'appliquent encore. Cette propriété s'étend, bien sûr, au cas d'un nombre fini d'éléments. Le plus "grand" diviseur, doit être compris au sens du préordre " x divise y " : tout diviseur commun de a et de b est un diviseur de d et réciproquement. De même, m est le plus "petit" multiple commun dans le sens suivant : tout multiple commun est un multiple de m et réciproquement. Les pgcd de a et b sont les associés de d, les ppcm de a et b sont les associés de m. ∎

Corollaire 3.

Soient $a \in A$ et $b \in A$ non nuls. S'il existe des éléments d, a_1, b_1 de A tels que $a = da_1$, $b = db_1$, avec $a_1 \wedge b_1 = 1$, alors d est un pgcd de a et b.

Démonstration. Il suffit d'écrire la décomposition en facteurs irréductibles de d, a_1, b_1. La proposition montre que d est un pgcd de a et b. ∎

Proposition 3. (lemme de Gauss)

Soient A un anneau factoriel et soient a, b, c des éléments non nuls de A. Si a divise bc et si $a \wedge b = 1$ alors a divise c.

Démonstration. Il existe $d \in A$ tel que $bc = ad$. Considérons les décompositions en facteurs irréductibles $a = up_1 \cdots p_k$, $c = vq_1 \cdots q_\ell$. Si $k \geqslant 1$ alors p_1 qui divise a, divise bc.

Puisque $a \wedge b = 1$, en utilisant le corollaire 2 on voit que p_1 ne divise pas b. C'est un facteur irréductible de c. Quitte à modifier l'ordre des facteurs de c supposons que $p_1 = q_1$. Comme A est intègre, on peut simplifier par p_1 l'égalité $up_1 \cdots p_k d = bvq_1 \cdots q_\ell$. Si a possède un autre facteur premier p_2, on peut recommencer ce raisonnement pour p_2 qui divise $bvq_2 \cdots q_\ell$ mais qui ne divise pas b. On pourra simplifier par $p_2 \ldots$ Une récurrence finie, montre que tous les facteurs irréductibles de a se retrouvent comme facteurs irréductibles de c et donc que a divise c. ∎

Exercice 1. (Cet exercice montre en particulier qu'un sous-anneau d'un anneau factoriel n'est en général pas factoriel.)

a) Soient A un anneau factoriel et $a \in A$ non nul. Montrer que a est irréductible si et seulement si l'idéal aA est premier.

b) On considère l'anneau A des entiers de l' extension quadratique $\mathbb{Q}(i\sqrt{3})$ de $\mathbb{Q}$. Montrer que A est factoriel et que 2 est irréductible dans A.

c) Montrer que le sous-anneau $B = \mathbb{Z} + i\sqrt{3}\mathbb{Z}$ de A n'est pas factoriel.

Solution. a) Dans tout anneau commutatif, unifère intègre, si l'idéal aA est premier, alors a est irréductible (déjà vu en 11-8). En effet, si $xy = a$, on a $xy \in aA$ et donc $x \in aA$ ou $y \in aA$. Si par exemple, $x \in aA$, alors $a|x$ et $x|a$ donc a et x sont associés. De même, si $y \in aA$ alors a et y sont associés (voir 9-1).

Supposons A factoriel et supposons a irréductible. Vérifions que aA est premier. Soient $x \in A, y \in A$ tels que $xy \in aA$. Alors $a|xy$. D'après le lemme de Gauss, $a|x$ ou $a|y$ et donc $x \in aA$ ou $y \in aA$. Ainsi aA est premier.

b) D'après 11-3, pour $d = -3$ l'anneau A_d est euclidien. Il est principal et donc factoriel. Ici $d \equiv -3 \equiv 1 \pmod 4$ donc$A = \mathbb{Z} + \mathbb{Z}\theta$ où $\theta = \frac{1+i\sqrt{3}}{2}$.

Si 2 n'était pas irréductible, il existerait $z = x + iy \in A, z' = x' + iy' \in A$ qui ne seraient pas des unités (tels que $n(z) \neq \pm 1$, $n(z') \neq \pm 1$) tels que $2 = zz'$, d'où $4 = n(z)n(z')$. On aurait donc $n(z) = 2$, $n(z') = 2$, soit $x^2 + 3y^2 = 2$, $x'^2 + 3y'^2 = 2$. C'est impossible. Donc 2 est irréductible dans A.

c) Puisque 2 est irréductible dans A, il est irréductible dans B. En effet, si $2 = zz'$ avec $z \in B$, $z' \in B$, alors dans A cette relation impose $z = \pm 1$, $z' = \pm 2$ ou $z' = \pm 1$, $z = \pm 2$. Vérifions que l'idéal $2B$ de B n'est pas premier. D'après a), B ne sera pas factoriel. On a $x = 1 + i\sqrt{3} \notin 2B, y = 1 - i\sqrt{3} \notin 2B$ et $xy = 4 \in 2B$. (D'ailleurs, on peut vérifier que $2 \times 2 = 4 = (1 + i\sqrt{3})(1 - i\sqrt{3})$ sont deux décompositions de $4 \in B$ en facteurs irréductible non associées dans B.)

Exercice 2. Soit A l'anneau des entiers algébriques du corps $\mathbb{Q}(i\sqrt{5})$. Montrer que $2 + i\sqrt{5}$ et $2 - i\sqrt{5}$ sont irréductibles dans A et que A n'est pas factoriel.

Solution. Comme $-5 \equiv 3 \pmod 4$, l'anneau des entiers algébriques de $\mathbb{Q}(i\sqrt{5})$ est $A = \mathbb{Z} + i\mathbb{Z}\sqrt{5}$ (11-3, prop.). On a $A_* = \{1, -1\}$ (voir Ex. 11-7). La norme $n(z) = z\bar{z}$ de $z = 3, 2 + i\sqrt{5}$ ou $2 - i\sqrt{5}$ est 9. Supposons que $z = ab$, avec $a, b \in A$. On aura $n(z) = n(a)n(b) = 9$ et donc $n(a) = 1, 3$ ou 9. Si on suppose que $a = \alpha + i\beta\sqrt{5}$ est tel que $n(a) = \alpha^2 + 5\beta^2 = 3$, alors nécessairement $\beta = 0$ et $\alpha^2 = 3$ avec $\alpha \in \mathbb{Z}$. C'est impossible. Donc $n(a) = 1$ ou bien $n(a) = 9$ et alors $n(b) = 1$. Ainsi $a \in A_*$ ou $b \in A_*$. (11-6, lemme). Cela prouve que tout élément de A de norme 9 est irréductible dans A. Comme $9 = 3 \times 3 = (2 + i\sqrt{5})(2 - i\sqrt{5})$, avec $2 + i\sqrt{5}$ qui n'est pas associé à 3 on voit que 9 a deux décompositions distinctes comme produit de facteurs irréductibles. L'anneau A n'est pas factoriel. A fortiori, il n'est pas principal.

14.2 Polynômes primitifs

Soit A un anneau factoriel. On voudrait décomposer en facteurs irréductibles un polynôme $f = a_0 + a_1X + \cdots + a_nX^n$ de $A[X]$. Si $b \in A$ divise tous les coefficients de f, alors b se met en facteur et la décomposition en facteurs irréductibles de b dans l'anneau A fournit des facteurs de f, irréductibles dans $A[X]$, de degré zéro.

Définition.

Soient A un anneau factoriel et $f = a_0 + a_1X + \cdots + a_nX^n$ un élément de $A[X]$. Un pgcd $c \in A$ de $a_0, \ldots, a_n$ est appelé un contenu du polynôme f.
Si $a_0, \ldots, a_n$ sont premiers dans leur ensemble, c'est-à-dire si 1 est un contenu de f, on dit que le polynôme f est primitif.

On notera $\mathrm{cont}(f)$ l'ensemble des contenus de f, c'est-à-dire des pgcd des coefficients de f. Cet ensemble constitue une classe d'éléments associés de A.

Si f est unitaire (soit $a_n = 1$), il est évidemment primitif. Si f est irréductible dans $A[X]$, il est primitif, sinon par mise en facteur d'un contenu c dans $f = cf_1$ apparaîtrait une décomposition de f en deux facteurs qui ne seraient pas des unités de A.

Si $f(X) = df_1(X)$ et si $f_1(X) = b_0 + \cdots + b_nX^n$ est primitif, alors $d \in \mathrm{cont}(f)$. En effet, $b_0, \ldots, b_n$ sont premiers entre eux et on a $a_0 = db_0, \ldots, a_n = db_n$. Alors d est un pgcd de $b_0, ..., b_n$, d'après l4-1, cor.3. En particulier, si $f(X) = c_1f_1(X) = c_2f_2(X)$ et si f_1, f_2 sont primitifs, alors c_1 et c_2 sont associés.

Exercice 1. Soit A un anneau factoriel. Montrer que
$f(X) = aX^3 + (b+c)X^2 + (a+b)X + (c-1)$ est primitif dans l'anneau $A[X]$.

Solution. Les coefficients de $f(X)$ vérifient $a + (b+c) - (a+b) - (c-1) = 1$. Ils sont donc premiers entre eux : tout diviseur commun doit diviser 1. (Notons que dans un anneau factoriel des éléments premiers dans leur ensemble ne vérifient pas nécessairement une relation de Bezout, voir par exemple 11-2, ex.)

Exercice 2. Soient K un corps commutatif et $A = K[X]$. Quel est le contenu de $f(Y) = (X+1)Y^3 + (X^2-1)Y^2 - (X^2+X)Y + X^3 + X^2 + X + 1 \in A[Y]$.

Solution. Les coefficients de ce polynôme en Y sont les éléments de $K[X]$ suivants :

$$a_3(X) = X+1 \quad , \quad a_2(X) = (X-1)(X+1),$$
$$a_1(X) = (X+l)X \quad , \quad a_0(X) = (X+1)(X^2+1).$$

Leur pgcd est $X + 1 \in A$. C'est le contenu de $f(Y)$, unique élément unitaire dans $\mathrm{cont}(f)$, et $f_1(Y) = Y^3 + (X-1)Y^2 + XY + (X^2+1)$ est primitif dans $A[Y]$.

Proposition. (Gauss)

Soient A un anneau factoriel et $f, g \in A[X]$ non nuls. Si un élément irréductible p de A divise tous les coefficients de fg, alors p divise tous les coefficients de f ou bien p divise tous les coefficients de g.

Démonstration. Supposons l'assertion fausse. Soit i_0 (resp. j_0) le plus petit indice tel que p ne divise pas le coefficient a_{i_0}, de f (resp. b_{j_0} de g). Pour $k = i_0 + j_0$ le coefficient

$$c_k = (a_0b_k + \cdots + a_{i_0-1}b_{j_0+1}) + a_{i_0}b_{j_0} + (a_{i_0+1}b_{j_0-1} + \cdots + a_kb_0).$$

de fg est divisible par p, ainsi que les deux parenthèses du second membre. Donc p divise $a_{i_0}b_{j_0}$. D'après 14-1, cor.2, p divise a_{i_0} ou b_{j_0}. C'est absurde. ∎

Corollaire 1.

Si $f, g \in A[X]$ sont primitifs, alors fg est primitif.

Corollaire 2.

Soient $f, g \in A[X]$ non nuls. Alors $\text{cont}(fg) = \text{cont}(f)\text{cont}(g)$.

Démonstration. Soient c et d des contenus de $f$et de g. Alors$f(X) = cf_1(X)$ et $g(X) = dg_1(X)$ avec f_1 , g_1 primitifs. On a $(fg)(X) = cd(f_1g_1)(X)$ et f_1g_1 est primitif d'après le cor. 1. Donc cd est un contenu de fg et

$$\text{cont}(fg) = cdA_* = (cA_*)(dA_*) = \text{cont}(f)\text{cont}(g) .$$ ∎

14.3 Irréductibilité des polynômes

Théorème.

Soient A un anneau factoriel, K son corps des fractions et $f \in A[X]$ un polynôme primitif. Pour que f soit irréductible dans $A[X]$, il faut et il suffit que f soit irréductible dans $K[X]$.

Démonstration. 1°/ Supposons f irréductible dans K Soient $g, h \in A[X]$ tels que $f = gh$. Montrons que g ou h est dans $A[X]$ un polynôme constant, élément de A_*. Dans $K[X]$, qui contient $A[X]$, le fait que f soit irréductible nécessite que g ou h soit une unité, c'est-à-dire un polynôme constant non nul. Si, par exemple, g est une constante $b_0 \in A$, alors $f(X) = b_0h(X)$. Comme f est primitif on a $b_0 \in A_*$. Ainsi f est irréductible dans $A[X]$.

2° / Supposons f irréductible dans $A[X]$ Soient $g, h \in K[X]$ tels que $f = gh$, avec :

$$g(X) = \tfrac{a_0}{a'_0} + \cdots + \tfrac{a_n}{a'_n}X^n \qquad , \qquad h(X) = \tfrac{b_0}{b'_0} + \cdots + \tfrac{b_m}{b'_m}X^m ,$$

où les numérateurs et dénominateurs a_i, a'_i, b_j, b'_j des coefficients sont des éléments de A. Soit $r \in A$ un ppcm de $a'_0 \dots a'_n$, dénominateur commun pour les fractions coefficients de g et soit $s \in A$ un ppcm de $b'_0, \dots, b'_m$. Alors $r\,g(X)$ et $s\,h(X)$ sont des polynômes de $A[X]$. Notons $c \in A$ et $d \in A$ leurs contenus. Soient $g_1, h_1 \in A[X]$ des polynômes primitifs tels que $r\,g(X) = c\,g_1(X)$, $s\,h(X) = d\,h_1(X)$. On a :

$$(1) \qquad rs\,f(X) = (r\,g(X))(s\,h(X)) = cd\,g_1(X)h_1(X).$$

D'après 14-2, cor.1, g_1h_1 est primitif et par hypothèse, f est primitif. Donc rs et cd sont associés. Il existe $u \in A$, tel que $cd = urs$. En simplifiant (1) par rs, on obtient :

$$(2) \qquad f(X) = u\,g_1(X)h_1(X) \qquad \text{avec } g_1, h_1 \in A[X].$$

Comme f est irréductible dans $A[X]$, on a $g_1 \in A_*$ ou $h_1 \in A_*$ et donc d°$(g) = 0$ ou d°$(h) = 0$. Ainsi f est irréductible dans $K[X]$. ∎

Corollaire.

Soit $f \in A[X]$. Supposons qu'il existe $g, h \in K[X]$ unitaires tels que $f = gh$. Alors g, h sont éléments de $A[X]$.

Démonstration. Puisque f est unitaire, il est primitif. Reprenons la démonstration précédente. On obtient (2) avec $u \in A_*$. Soient c_n et d_m les coefficients des monômes de plus haut degré de g_1 et de h_1. On a $1 = uc_nd_m$ donc c_n et d_m sont inversibles dans A. Posons $g_2(X) = c_n^{-1}g_1(X)$, $h_2(X) = uc_nh_1(X)$. On a g_2 , $h_2 \in A[X]$ et $f = g_2h_2$. Puisque $f$et g_2 sont unitaires, h_2 est unitaire. Les relations $rg(X) = cg_1(X) = cc_ng_2(X)$ et $sh(X) = dh_1(X) = du^{-1}c_n^{-1}h_2(X)$ nécessitent $r = cc_n$, $s = du^{-1}c_n^{-1}$ car g , g_2 , h , h_2 sont unitaires. On a donc $g = g_2 \in A[X]$ et $h = h_2 \in A[X]$. ∎

Exercice. Montrer que $f(X) = X^3 - 2X + \frac{3}{4}$ est irréductible dans $\mathbb{Q}[X]$.

Solution. La question revient à montrer que $g(X) = 4X^3 - 8X + 3$ est irréductible dans $\mathbb{Q}[X]$, ou encore dans $\mathbb{Z}[X]$ puisque $g(X)$ est primitif. Raisonnons par l'absurde. Supposons qu'il soit décomposable dans $\mathbb{Z}[X]$. Il n'a pas de facteur de degré zéro car il est primitif. Il a donc dans $\mathbb{Z}[X]$ un facteur de degré un et un facteur de degré deux :

$$g(X) = (aX + b)(cX^2 + dX + e) = acX^3 + (bc + ad)X^2 + (bd + ae)X + be\,,$$

Comme on peut changer de signe les deux facteurs, on peut supposer $a \in \mathbb{N}^*$, $c \in \mathbb{N}^*$. On doit avoir $4 = ac$, $0 = bc + ad$, $-8 = bd + ae$, $3 = be$.

- Si $a = c = 2$ on obtient $b + d = 0$, $2e - d^2 = -8$, $-de = 3$. 0n en déduit que 2 divise d et que d divise 3. C'est impossible.

- Si $a = 4$, $c = 1$ on obtient $b + 4d = 0$, $4e - 4d^2 = -8$, $-4de = 3$. C'est impossible car 4 ne divise pas 3.

- Si $a = 1, c = 4$ on obtient $4b + d = 0$, $e - 4b2 = -8$, $be = 3$. On voit que 2 divise e et que e divise 3. C'est impossible.

Donc $g(X)$ est irréductible dans $\mathbb{Z}[X]$ et $f(X)$ est irréductible dans $\mathbb{Q}[X]$.

14.4 Anneau des polynômes sur un anneau factoriel

Théorème.

Soit A un anneau factoriel. L'anneau $A[X]$ est factoriel.

Démonstration. On sait que si A est intègre, alors$A[X]$ est intègre (10-1, prop.).

1° / *Montrons que tout $f \in A[X]$ admet une décomposition en facteurs irréductibles.*

On a $f = cf_1$ où $c \in A$ est un contenu de f et où $f_1 \in A[X]$ est primitif. La décomposition en facteurs irréductibles de c dans A, est une décomposition de c en facteurs irréductibles dans $A[X]$. Il suffit d'étudier f_1. On peut supposer f primitif.

Dans $K[X]$ qui est principal et donc factoriel, f a une décomposition $f = f_1 \cdots f_n$ où $f_i \in K[X]$ est irréductible pour $i = 1, \ldots n$. Pour $i = 1, \ldots, n$ considérons une expression $f_i = \sum_{k=0}^{n_i} \frac{a_k}{b_k} X^k$ de f_i, puis un ppcm r_i des dénominateurs $b_0, \ldots, b_{n_i}$. Alors r_if_i est un élément de $A[X]$. Soient $c_i \in \text{cont}(r_if_i)$ et $g_i \in A[X]$ primitif tels que $r_if_i = c_ig_i$. Alors $g_1 \cdots g_n$ est primitif d'après 14-2, cor. 1. Comme f est lui aussi primitif, tel que $r_1 \cdots r_nf = c_1 \cdots c_ng_1 \cdots g_n$, il existe $u \in A_*$ tel que $c_1 \cdots c_n = ur_1 \cdots r_n$. Après simplification, on obtient $f = ug_1 \cdots g_n$. Comme $g_1, \ldots, g_n$ sont primitifs, irréductibles dans $K[X]$ car $f_1, \ldots, f_n$ le sont, ces polynômes sont irréductibles dans A[X], d'après 14-3.

2° / *Montrons que cette décomposition est unique.*

Soient $f = p_1 \cdots p_mf_1 \cdots f_n = q_1 \cdots q_rg_1 \cdots g_s$ deux décompositions de f en facteurs

irréductibles avec$p_1, \ldots, p_m, q_1, \ldots, q_r \in$ A de degré zéro et $f_1, \ldots, f_n, g_1, \ldots, g_s \in A[X]$ de degré au moins égal à 1. Les polynômes f_i, g_j étant irréductibles dans $A[X]$ sont primitifs. D'après 14-2, cor.1, $f' = f_1 \cdots f_n$ et $g' = g_1 \cdots g_s$, sont primitifs. On en déduit que $p_1 \cdots p_m$ et $q_1 \cdots q_r$, sont deux contenus de f et donc qu'il existe $u \in A_*$ tel que $p_1 \cdots p_m = uq_1 \cdots q_r$. L'unicité de la décomposition en facteurs irréductibles dans l'anneau factoriel A montre que $m = r$ et que $p_1, \ldots, p_m$ sont associés à $q_1, \ldots, q_r$ énumérés dans un ordre convenable.

En simplifiant, il vient $f_1 \cdots f_n = vg_1 \cdots g_s$ où $v \in A_*$. Alors $f_1, \ldots, f_n, g_1, \ldots, g_s$ étant primitifs irréductibles dans $A[X]$, ils sont irréductibles dans $K[X]$. De l'unicité de la décomposition dans l'anneau principal $K[X]$, il résulte que $n = s$ et que $f_1, \ldots, f_n$ sont associés à $g_1, \ldots, g_s$ énumérés dans un ordre convenable. Par exemple, si f_1 et g_1 sont associés dans $K[X]$, ils le sont encore dans $A[X.]$ En effet, si on a $g_1 = \frac{a_1}{b_1} f_1$ où $a_1 \neq 0$ et $b_1 \in A_*$, on a $b_1 g_1 = a_1 f_1$. Alors a_1, b_1 sont alors deux contenus du même polynôme. Il existe $u \in A_*$ tel que $a_1 = ub_1$. Après simplification on obtient $g_1 = uf_1$. Il en est de même pour les autres termes. ∎

Corollaire.

Soient A un anneau factoriel. L'anneau $A[X_1, \ldots, X_n]$ des polynômes de n variables est factoriel. En particulier, si K est un corps commutatif l'anneau $K[X_1, \ldots, X_n]$ est factoriel.

Démonstration. En ordonnant les polynômes de $A[X_1, \ldots, X_n]$ par rapport à la variable X_n on peut les considérer comme des polynômes de la variable X_n, à coefficients dans l'anneau $A[X_1, \ldots, X_{n-1}]$. La proposition montre que $A[X_1]$ est factoriel, puis que $A[X_1, X_2] = (A[X_1])[X_2]$ est factoriel, que $A[X_1, X_2, X_3] = (A[X_1, X_2])[X^3]$ est factoriel... d'où le résultat par une récurrence. ∎

Exercice 1. Dans l'anneau $\mathbb{Z}[X, Y]$ décomposer $f(X, Y) = Y^3 - X^3$ en facteurs irréductibles.

Solution. Identifions $\mathbb{Z}[X, Y]$ avec $A[Y]$ où $A = \mathbb{Z}[X]$. On a
$f(X, Y) = (Y - X)(Y^2 + XY + X^2)$. Le facteur $Y - X$ est primitif dans $A[X]$ car unitaire, de degré un et donc irréductible (14-3, th.). Le facteur $Y^2 + XY + X^2$) est primitif. Il n'a donc pas de facteurs irréductibles de degré zéro (éléments de A). Supposons qu'il existe $a(X), b(X), a'(X), b'(X)$ dans $A = \mathbb{Z}[X]$, tels que :

$$Y^2 + XY + X^2 = [a(X)Y - b(X)][a'(X)Y - b'(X)]\,.$$

On aura $a(X)a'(X) = 1$ et donc $a(X) = a'(X) = \pm 1$ (unités de $\mathbb{Z}[X]$). Quitte à changer les signes des deux facteurs, on a $a(X) = a'(X) = 1$ et

$$Y^2 + XY + X^2 = [Y - b(X)][Y - b'(X)] = Y_2 - (b(X) + b'(X))Y + b(X)b'(X),$$

d'où $b(X) + b'(X) = -X$, $b(X)b'(X) = X^2$ et donc $b(X)^2 + Xb(X) + X^2 = 0$. Ainsi, X irréductible de $A = \mathbb{Z}[X]$ divise $b(X)$. Il existe $c(X)$ dans A, de degré un, tel que $b(X) = Xc(X)$. On obtient $c(X)^2 + c(X) + 1 = 0$. C'est impossible car pour tout $n \in \mathbb{Z}$, l'élément $k = c(n)$ vérifierait $k^2 + k + 1 = 0$. Or la fonction polynomiale $X^2 + X + 1$ ne s'annule pas sur $\mathbb{R}$. Donc $Y^2 + XY + X^2$ est irréductible dans $\mathbb{Z}[X, Y]$.
Autre justification :
si on avait $Y^2 + XY + X^2 = [Y - -b(X)][Y - b'(X)]$ dans $(\mathbb{Z}[X])[Y]$, dans l'anneau factoriel $(\mathbb{C}[X])[Y]$ on aurait $Y^2 + XY + X^2 = [Y - b(X)][Y - -b'(X)] = (Y - jX)(Y - \bar{j}X)$ et donc $b(X) = jX$ ou $\bar{j}X$ absurde.

Exercice 2. Soit K un corps commutatif. Dans l'anneau $A = K[X, Y]$, soit $I = (X)$ l'idéal engendré par le polynôme X. Etudier l'anneau A/I. En déduire que (X) est premier. Proposer une généralisation.

Solution. Il est clair que $f : p(X, Y) \mapsto p(0, Y)$ est un homomorphisme d'anneaux de $A = K[X, Y]$ dans K. Il est surjectif car tout polynôme $a(Y)$ d'une variable peut être vu comme un polynôme des variables X, Y, constant en X. Le noyau de f est évidemment $I = (X)$. Par factorisation de f, on obtient un isomorphisme de A/I sur $\mathrm{Im}\,(f)) = K[Y]$ qui est un anneau intègre. Donc A/I est intègre et I est premier.

De manière plus générale, si A est un anneau factoriel, alors $p \in A$ est irréductible, si et seulement si l'idéal (p) est premier, distinct de $\{0\}$ (voir 14-1, ex. 1, a))

14.5 Critère d'irréductibilité d'Eisenstein

Proposition.

Soient A un anneau factoriel, K le corps des fractions de A et $f \in A[X]$ d'expression $f = a_0 + \cdots + a_n X^n$ avec $n \geqslant 1$. Supposons qu'il existe $p \in A$ irréductible qui divise $a_0, \ldots a_{n-1}$, qui ne divise pas a_n et tel que p^2 ne divise pas a_0. Alors f est irréductible dans $K[X]$. S 'il est primitif, il est irréductible dans $A[X]$.

Démonstration. Soit $c \in \mathrm{cont}(f)$. Alors $f = cf_1$ avec $f_1 \in A[X]$ primitif. Comme p ne divise pas a_n, il ne divise pas c. D'après le lemme de Gauss, puisque p divise $a_0, \ldots, a_{n_1}$, il divise les coefficients de degrés $0, \ldots, n-1$ de f_1. Par ailleurs, p ne divise pas le coefficient au degré n de f_1 et p^2 ne divise pas le coefficient au degré zéro de f_1. On peut donc remplacer f par f_1 et supposer $f$primitif. Alors, d'après 14-3, f est irréductible dans $K[X]$ si et seulement s'il est irréductible dans $A[X]$.

Supposons que f ne soit pas irréductible dans $A[X]$. Il existe alors des polynômes $g = b_0 + \cdots + b_r X^r$ et $h = c_0 + - \cdots + c_s X^s$ de $A[X]$ de degrés $r \geqslant 1$ et $s \geqslant 1$ tels que $f = gh$. Par hypothèse, p divise $a_0 = b_0 c_0$. D'après le lemme de Gauss, $p|a_0$ ou $p|b_0$ mais p ne divise pas b_0 et c_0 sinon p^2 diviserait a_0. Supposons par exemple que p divise b_0 sans diviser c_0. Comme p ne divise pas $a_n = b_r c_s$ on voit que p ne divise pas b_r. Considérons le plus petit entier $k \leqslant r$ tel que p ne divise pas b_k. Alors p divise $b_0, \ldots, b_{k-1}$ et p divise $a_k = (b_0 c_k + \cdots + b_{k-1} c_1) + b_k c_0$ par hypothèse. On en déduit que p divise $b_k c_0$. D'après le lemme de Gauss, p divise b_k ou c_0. C'est absurde car p ne divise ni c_0 ni b_k. Donc f est irréductible dans $A[X]$. ∎

Remarques.

a) Le critère d'Eisenstein s'applique parfois après un changement de variable convenable. Par exemple, $X^3 - 3X + 1$ considéré en 13-6, 3 est irréductible car en posant $X = Y - 1$ on obtient $f(Y) = Y^3 - 3Y^2 + 3$ auquel le critère s'applique pour $p = 3$.

De même $Y^2 + XY + X^2$ est irréductible dans $(\mathbb{Z}[X])[Y]$ car en posant, $Y = Z + X$ on obtient $Z^2 + 3XZ + 3X^2$ et $3 \in \mathbb{Z}[X]$ est irréductible. Le critère d'Eisenstein s'applique. On retrouve ainsi qu'il est irréductible dans $\mathbb{Z}[X, Y]$ (14-4, ex. 1).

b) Quel que soit le corps K un polynôme $f = aX + b$ de degré un est irréductible dans $K[X]$. Si A est un anneau factoriel et si $a \wedge b = 1$, alors $f = aX + b$ est irréductible dans $A[X]$ d'après le th. 14-3.

Un corps K est algébriquement clos si et seulement si les polynômes de degré un sont les seuls éléments irréductibles de $K[X]$.

c) Soit K un corps. Pour qu'un polynôme $f \in K[X]$ de degré 2 ou 3 soit irréductible, il faut et il suffit qu'il n'ait pas de racine dans le corps K. En effet, si f est réductible, il existe g, h dans $K[X]$ de degrés $r \geqslant 1$, $s \geqslant 1$ tels que $f = gh$. Ona $r + s = \mathrm{d}^\circ(f) = 2$ ou 3. L'un des degrés r ou s est égal à 1. Par exemple, si $r = 1$, alors g est de la forme $g = aX + b$, où $a \neq 0$ et f admet pour racine $-\frac{b}{a}$. Réciproquement, si f a une racine $\alpha \in K$, il existe $q \in K[X]$, avec $\mathrm{d}^\circ(q) = \mathrm{d}^\circ(f) - 1 \neq 0$, tel que $f = (X - \alpha)q$ et f n'est pas irréductible.

Attention, cette caractérisation ne s'applique plus pour $\mathrm{d}^\circ(f) \geqslant 4$. Par exemple $(X^2 + 1)(X^2 + 2)$ n'est pas irréductible dans $\mathbb{R}[X]$ et il n'a pas de racine dans $\mathbb{R}$.

d) Soit $f \in \mathbb{Z}[X]$ d'expression $f = a_n X^n + \cdots + a_0$ et soit p un nombre premier ne divisant pas a_n. Si le polynôme $\overline{a_n} X^n + \cdots + \overline{a_0}$ à coefficients dans le corps $K = \mathbb{Z}/p\mathbb{Z}$ est irréductible dans $K[X]$, alors nécessairement f est irréductible dans $\mathbb{Z}[X]$.

En effet, si f était égal au produit $(b_r X^r + \cdots + b_0)(c_s X^s + \cdots + c_0)$ de deux polynômes de $\mathbb{Z}[X]$, de degrés $r \geqslant 1$ et $s \geqslant 1$, on en déduirait dans $K[X]$l :

$$\overline{a_n} X^n + \cdots + \overline{a_0} = (\overline{b_r} X^r + \cdots + \overline{b_0})(\overline{c_s} X^s + \cdots + \overline{c_0}) \,,$$

avec $\overline{b_r} \neq \overline{0}$ et $\overline{c_s} \neq \overline{0}$ car $\overline{a_n} \neq \overline{0}$.

De façon générale, soient A, B des anneaux commutatifs unifères, $\varphi \in \mathrm{Hom}\,(A, B)$ et $f = a_n X^n + \cdots + a_0$ dans $A[X]$de degré $n > 1$. Si $f_\varphi = \varphi(a_n) X^n + \cdots + \varphi(a_0)$ est de degré n, irréductible dans $B[X]$, alors f est irréductible dans $A[X]$.

Exercice 1. Montrer que $f = X^n - 2$, où $n \geqslant 1$, est irréductible dans $\mathbb{Z}[X]$ et dans l'anneau $A[X]$ où $A = \mathbb{Z} + \mathbb{Z}\theta$, avec $\theta = \frac{1+i\sqrt{3}}{2}$ (anneau des entiers algébriques de $\mathbb{Q}(i\sqrt{3})$. Calculer $[\mathbb{Q}(j, \sqrt[n]{2}) : \mathbb{Q}]$.

Solution. Puisque f est unitaire, il est primitif. L'anneau $\mathbb{Z}$ est principal et donc factoriel. Le critère d'Eisenstein est vérifié pour $p = 2$ donc f est irréductible dans $\mathbb{Z}[X]$ et dans $\mathbb{Q}[X]$.

D'après 11-3, prop., l'anneau A est un anneau euclidien et donc factoriel. Nous avons vu en 14-1, ex. 1, que 2 est irréductible dans A. Le critère d'Eisenstein montre que $f = X^n - 2$ est irréductible dans $A[X]$. Il est également irréductible dans $\mathbb{Q}(i\sqrt{3})[X]$ car il est primitif et $\mathbb{Q}(i\sqrt{3})$ est le corps des fractions de A. C'est donc le polynôme minimal de $\sqrt[n]{2}$ sur $\mathbb{Q}(i\sqrt{3}) = \mathbb{Q}(j)$. On en déduit

$$[\mathbb{Q}(j, \sqrt[n]{2}) : \mathbb{Q}] = [\mathbb{Q}(j, \sqrt[n]{2}) : \mathbb{Q}(j)][\mathbb{Q}(j) : \mathbb{Q}] = 2n \,.$$

Exercice 2. Soit K un corps. Montrer que le polynôme $f(X, Y) = Y^3 + XY^2 + X^2Y + X(X^2 + 1)$ est irréductible dans l'anneau $K[X, Y]$.

Solution. L'anneau $A = K[X]$ est principal et donc factoriel. Identifions $K[X, Y]$ avec l'anneau $A[Y]$ et $f(X, Y)$ avec $f(Y) = Y^3 + a_2 Y^2 + a_1 Y + a_0$, dont les coefficients sont $a_2(X) = X$, $a_1(X) = X^2$, $a_0(X) = X(X^2 + 1)$. Alors X qui est irréductible dans A, divise a_0, a_1, a_2, sans que X^2 divise a_0. Le critère d'Eisenstein s'applique.

Exercice 3. En effectuant un changement de variable, montrer que $f = X^3 + 3X + 2$ et $\Phi_p = X^{p-1} + X^{p-2} + \cdots + 1$, où p est un nombre premier, sont irréductibles dans $\mathbb{Z}[X]$.

Solution. Posons $X = Y + 1$ on a $f(Y) = Y^3 + 3Y^2 + 6Y + 6$ auquel le critère d'Eisenstein s'applique pour $p = 3$.

On a $(X-1)\Phi_p = X^p - 1$. Donc en posant $X = Y + 1$ on a $Y\Phi_p(Y+1) = (Y+1)^p - 1$ et donc $\Phi_p(Y+1) = Y^{p-1} + pY^{p-2} + \cdots + C_p^{k+1}Y^k + \cdots + p$ car $\mathbb{Z}[X]$ est intègre. Or p divise C_p^{k+1} pour $k = 0, ..., p-2$ (Voir 9-1) et p^2 ne divise pas le coefficient au degré zéro. Le polynôme cyclotomique Φp est donc irréductible dans $\mathbb{Z}[X]$ et dans $\mathbb{Q}[X]$.

Exercice 4. a) Montrer que $f_1 = X^2 + X + \overline{4}$ et $f_2 = X^3 + \overline{3}X^2 + \overline{3}X + \overline{6}$ sont irréductibles dans $K[X]$, où $K = \mathbb{Z}/7\mathbb{Z}$.

b) Montrer que $g_1 = X^2 + 8X + 4$ et $g_2 = X^3 + 10X^2 + 10X - 1$ sont irréductibles dans $\mathbb{Z}[X]$

Solution. a) Puisque $f_1 = X^2 + X + \overline{4} = X^2 - \overline{6}X + \overline{4} = (X - \overline{3})^2 - \overline{9} + \overline{4} = (X - \overline{3})^2 - \overline{5}$ est de degré deux, il suffit de voir qu'il n'admet pas de racines dans le corps $\mathbb{Z}/7\mathbb{Z}$. Or $\overline{5}^{\frac{7-1}{2}} = -\overline{1}$ donc 5 n'est pas un carré dans $\mathbb{Z}/7\mathbb{Z}$ (voir 12-3).

De même, $f_2 = X^3 + \overline{3}X^2 + \overline{3}X + \overline{6}$ est irréductible dans $K[X]$. En effet, on a $X^3 + \overline{3}X^2 + \overline{3}X + \overline{6} = (X + \overline{1})^3 - \overline{2}$. Or 2 n'est pas un cube dans K. En effet, K_* est un groupe cyclique d'ordre $6 = 3 \times 2$. Il possède donc un unique sous-groupe d'ordre 2 soit $\{y \in K_*\,;\ \exists x,\ x^3 = y\} = \{y \in K_*\,;\ y^2 = \overline{1}\} = \{1, -1\}$. Donc 2 n'est pas un cube dans K. Le polynôme est donc sans racine dans K, de degré 3. Il est irréductible dans $K[X]$, d'après la remarque c).

b) Par $\varphi\ :\ k \mapsto \overline{k}$ de $\mathbb{Z}$ dans $\mathbb{Z}/7\mathbb{Z}$, l'image de g_1 dans $(\mathbb{Z}/7\mathbb{Z})[X]$ est f_1 de degré 2, irréductible. D'après la remarque d), g_1 est irréductible dans $\mathbb{Z}[X]$. De même, g_2 d'image f_2 est irréductible.

Exercice 5. Dans le plan complexe, soit M le point ayant pour affixe l'une des racines cubiques ζ de $\frac{7+3i}{41}$. Montrer qu'il est impossible de construire M à la règle et au compas à partir de l'origine O et du point B d'affixe 1.

Solution. On a $\zeta^3 = \frac{7+3i}{41}$. Donc ζ est racine du polynôme $f = 41X^3 - (7 + 3i)$. Vérifions que ce polynôme est irréductible sur le corps des fractions $\mathbb{Q}(i)$ de l'anneau des entiers de Gauss $A = \mathbb{Z} + i\mathbb{Z}$. Dans l'anneau principal A déterminons les décompositions en facteurs irréductibles de 41 et de $7 + 3i$.

On a $41 \equiv 1\ (\bmod 4)$. D'après 11-6, cor. 1, le nombre premier 41 est somme de deux carrés :

$41 = 5^2 + 4^2 = (5 + 4i)(5 - 4i)$ et $5 + 4i\ ,\ 5 - 4i$ sont irréductibles.

On a $n(7 + 3i) = 49 + 9 = 58 = 2 \times 29 = (1 + i)(1 - i) \times 29$. Comme on a $29 \equiv 1\ (\bmod 4)$, le nombre premier 29 est somme de deux carrés :

$29 = 5^2 + 2^2 = (5 + 2i)(5 - 2i)$, avec $5 + 2i\ ,\ 5 - 2i$ irréductibles dans A.

L'un d'eux divise $7 + 3i$ car $(7 + 3i)(7 - 3i) = 2 \times 29$. En fait, $7 + 3i = (5 - 2i)(1 + i)$ donc

$$41X^3 - (7 + 3i) = (5 + 4i)(5 - 4i)X^3 - (5 - 2i)(1 + i)\,.$$

Le critère d'Eisenstein s'applique par exemple avec $1+i$ qui est irréductible dans l'anneau principal A. Le polynôme f est donc irréductible sur le corps des fractions de A. On a donc $[\mathbb{Q}(i)(\zeta) : \mathbb{Q}(i)] = d^\circ(f) = 3$. Comme $\mathbb{Q}(\zeta)$ contient $\zeta^3 = \frac{7+3i}{41}$, ce corps contient $i = \frac{41\zeta^3-7}{3}$. On a donc $\mathbb{Q}(i) \subset \mathbb{Q}(\zeta)$ et $\mathbb{Q}(i)(\zeta) = \mathbb{Q}(\zeta)$. On en déduit $[\mathbb{Q}(\zeta) : \mathbb{Q}] = [\mathbb{Q}(i)(\zeta) : \mathbb{Q}(i)][\mathbb{Q}(i) : \mathbb{Q}] = 3 \times 2 = 6$. D'après le th. de Wantzel, M n'est pas constructible.

14.6 Irréductibilité des polynômes cyclotomiques

Dans 14-5, ex. 3, nous avons vu que pour tout p premier, le polynôme cyclotomique Φ_p est irréductible dans l'anneau $\mathbb{Q}[X]$. En fait, Φ_n est irréductible pour tout $n \in \mathbb{N}$. C'est donc le polynôme minimal de $\zeta = \exp(i\frac{2\pi}{n})$ sur $\mathbb{Q}$. Nous avons utilisé ce résultat en 13-6, ex. 4, pour caractériser les polygones réguliers constructibles à la règle et au compas. Par ailleurs, le fait que Φ_n soit irréductible sur $\mathbb{Q}$ et donc polynôme minimal de chacune des racines $n^{\text{ièmes}}$ primitives de l'unité, est utile dans la théorie de Galois. Nous allons donc démontrer ce résultat.

Lemme.

Soient $p \in \mathbb{N}$ premier et $K = \mathbb{Z}/p\mathbb{Z}$. Pour tout $f \in K[X]$, on a $[f(X)]^p = f(X^p)$.

Démonstration. Si B est un sous-anneau d'un anneau unifère A et si $1 \in B$, alors caract(A) = caract(B). Ainsi, $K[X]$, qui contient K, a pour caractéristique p. D'après 9-1, p est un nombre premier et on a $(a+b)^p = a^p + b^p$ pour tous $a, b \in K[X]$. Par récurrence, $(a_1 + \cdots + a_k)^p = a_1^p + \cdots + a_k^p$ pour toute famile finie $(a_1, \ldots, a_k)$ de $K[X]$. Pour tout $f(X) = a_0 + \cdots + a_n X^n$ polynôme de $K[X]$ on a donc :

$$[f(X)]^p = (a_0 + a_1 X + \cdots + a_n X^n)^p = a_0^p + a_1^p X^p + \cdots + a_n^p X^{np}\,.$$

D'après le th. de Fermat (Voir 12-2), $a_0 = a_0^p, \ldots, a_n = a_n^p$, d'où le lemme. ∎

Proposition.

Soit $n \in N^*$. Le polynôme cyclotomique Φ_n est irréductible sur $\mathbb{Q}$.

Démonstration. Soit $\omega \in \mathbb{C}$ une racine $n^{\text{ième}}$ primitive de l'unité. Notons f le polynôme minimal de ω sur $\mathbb{Q}$. Puisque $X^n - 1$ annule ω, il existe $h \in \mathbb{Q}[X]$ tel que $X^n - 1 = f\,h$. Puisque $X^n - 1$ est unitaire, à coefficients dans $\mathbb{Z}$, on a $f \in \mathbb{Z}[X]$, $h \in \mathbb{Z}[X]$ (14-3, cor.). Soit $p \in \mathbb{N}$ premier qui ne divise pas n. Montrons que ω^p est racine de f. Comme w^p est une autre racine $n^{\text{ième}}$ primitive de l'unité, son polynôme minimal g sur $\mathbb{Q}$ divise $X^n - 1$. Comme pour f, le polynôme g est unitaire, à coefficients entiers. Nous allons montrer que $f = g$.

Supposons que $g \neq f$. Alors, g est irréductible, il divise $X^n - 1 = f\,h$ et il est premier avec f. D'après le lemme de Gauss, g divise h. Il existe $k \in \mathbb{Q}[X]$ tel que $X^n - 1 = fgk$ et k est à coefficients entiers (14-3, cor.). D'autre part, ω étant racine de $g(X^p)$, ce polynôme est multiple de f. Il existe $\ell \in \mathbb{Q}[X]$, tel que $g(X^p) = f(X)\ell(X)$ et ℓ est à coefficients entiers. Prenons les images $\overline{f}$, $\overline{g}$, $\overline{k}$, $\overline{\ell}$ de ces polynômes dans l'anneau $(\mathbb{Z}/p\mathbb{Z})[X]$. D'après le lemme,

$$X^n - \overline{1} = \overline{f}(X)\overline{g}(X)\overline{k}(X) \quad \text{et} \quad \overline{g}(X)^p = \overline{g}(X^p) = \overline{f}X)\overline{\ell}(X)\,.$$

Soit $\varphi(X) \in (\mathbb{Z}/p\mathbb{Z})[X]$ un facteur irréductible de $\overline{f}(X)$. La deuxième relation montre que $\varphi(X)$ divise $\overline{g}(X)$. De ce fait, la première relation indique que $\varphi(X)$ apparaît au carré dans le polynôme $X^n - \overline{1}$ de $(\mathbb{Z}/p\mathbb{Z})[X]$. Dans la clôture algébrique du corps $\mathbb{Z}/p\mathbb{Z}$, une racine de $\varphi(X)$ serait alors une racine d'ordre deux au moins pour $X^n - 1$. Elle annulera ce polynôme et le polynôme dérivé nX^{n-1}. Comme p ne divise pas n, on a $\overline{n} \neq \overline{0}$ donc le polynôme dérivé admet pour seule racine zéro, qui n'est pas racine de $X^n - 1$. C'est absurde et donc $g = f$ et ω^p qui est racine de g est racine de f.

Toute racine $n^{\text{ième}}$ primitive ω^m, où $m \wedge n = 1$, est racine de f. En effet si $m = p_1 \cdots p_k$ est la décomposition en facteurs premiers de m, alors $p_1, \ldots, p_k$ ne divisent pas n et d'après ce qui précède, $\omega^{p_1}, \omega^{p_1 p_2}, \ldots, \omega^{p_1 \cdots p_k} = \omega^m$ sont des racines de f. Comme Φ_n est produit des facteurs irréductibles distincts $X - \omega^m$, où $0 \leqslant m < n - 1$ et $m \wedge n = 1$, on voit que Φ_n divise f. Comme le polynôme minimal f de ω divise Φ_n, on a $\Phi_n = f$ et Φ_n est irréductible. ∎

Corollaire.

Soit ω une racine $n^{\text{ième}}$ primitive de l'unité dans $\mathbb{C}$. Alors $[\mathbb{Q}(\omega) : \mathbb{Q}] = \varphi(n)$, où φ désigne la fonction d'Euler.

Démonstration. D'après la proposition, Φ_n est irréductible. Il a ω pour racine. D'après 13-1, cor. 2, Φ_n est le polynôme minimal de ω et son degré est $\varphi(n)$. ∎

Exercice 1. Montrer que $X^4 + 1$ est irréductible dans $\mathbb{Z}[X]$ bien qu'il soit réductible dans $F_p[X]$ pour tout nombre premier p.

Solution. Puisque $X^4 + 1$ est le polynôme cyclotomique Φ_8, il est irréductible dans $\mathbb{Z}[X]$. (D'ailleurs, on a $\Phi_8(X + 1) = X^4 + 4X^3 + 6X^2 + 4X + 2$ et le critère d'Eisenstein s'applique pour $p = 2$.)
Si p est un nombre premier, -1 ou 2 ou -2 est égal à un carré a^2 de F_p (voir Ex. 12-11, a)).
Donc Φ_8 a sur F_p l'une des expressions :
$X^4 + 1 = X^4 - a^2 = (X^2 - a)(X^2 + a)$,
$X^4 + 1 = (X^2 + 1)^2 - 2X^2 = (X^2 + 1)^2 - a^2X^2(X^2 + 1 - aX)(X^2 + 1 + aX)$,
$X^4 + 1 = (X^2 - 1)^2 + 2X^2 = (X^2 - -1)^2 - a^2X^2(X^2 - 1 - aX)(X^2 - 1 + aX)$.

Ainsi, Φ_8) est réductible dans $Fp[X]$ pour tout nombre premier p.

Exercice 2. Montrer que $\omega = \frac{\sqrt{2}}{2} + i\frac{\sqrt{2}}{2}$ est algébrique de degré 4 sur $\mathbb{Q}$.

Solution. Puisque ω est une racine huitième primitive de l'unité c'est une racine de $\Phi_8 = X^4 + 1$. Ce polynôme étant irréductible, c'est le polynôme minimal de ω.

Cela se voit directement. On a $\sqrt{2}, i \in \mathbb{Q}(\omega)$ car $\omega^2 = i$ donc $\mathbb{Q}(\omega) = \mathbb{Q}(\sqrt{2})(i)$. Ainsi $[\mathbb{Q}(\sqrt{2})(i) : \mathbb{Q}] = [\mathbb{Q}(\sqrt{2})(i) : \mathbb{Q}(\sqrt{2})][\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 4$. Le polynôme minimal de ω est donc de degré 4 et il divise $\Phi_8 = X^4 + 1$. Il est égal à $X^4 + 1$.

Exercice 3. Décomposer en facteurs irréductibles $X^{12} - 1 \in \mathbb{Z}[X]$.

Solution. Les diviseurs de 12 sont $1, 2, 2^2, 3, 2 \times 3, 2^2 \times 3$. D'après 10-6, ex. 2, $\Phi_{12}(X) = \Phi_6(X^2) = X^4 - X^2 + 1$, d'où la décomposition :

$$X^{12} - 1 = \prod_{d|12} \Phi_d = (X - 1)(X + 1)(X^2 + 1)(X^2 - X + 1)(X^2 + X + 1)(X^4 - X^2 + 1).$$

Index

A

action d'un groupe
  conjugaison, 41
  libre, 42
  orbite, 42
  stabilisateur, 42
  transitive, 42
anneau, 189
anneau
  euclidien, 238
  factoriel, 307
  intègre, 189
  noethérien, 237
  principal, 237
  unifère, 189
application affine, 109
associés (éléments d'un anneau), 189
automorphismes (d'un groupe), 16
automorphismes intérieurs, 16

B

barycentre, 133
Bezout (théorème de Bezout), 243
Burnside (formule de), 43

C

caractéristique d'un anneau, 189
Cardan-Tartaglia (formules de), 224
Cauchy (théorème de), 45
centre d'un groupe, 18
Chasles (relation de), 105
classes (équation des), 43
classes modulo un sous-groupe, 21
commutateurs, 69
composantes primaires, 68
coniques, 107
constructions (règle et compas), 296
contenu d'un polynôme, 310
convexe
  enveloppe, 143
  point extrémal, 144
corps, 200
corps
  algébriquement clos, 216
  des fractions, 202
  quadratique, 201
critères de divisibilité, 263
cycle, 79

D

degré d'une extension, 294
demi-tour, 167
dilatation, 35
diophantienne (équation), 273
Dirichlet (théorème de), 272
diviseurs de zéro, 189
duplication du cube, 298

E

Eisenstein (critère d'), 314
endomorphisme d'un groupe, 16
entiers
  d'un corps quadratique, 240
  de Gauss, 246
Eratosthène (crible d'), 269
espace affine, 105
espace affine euclidien, 153
Euler (fonction de), 59
Euler (relation de), 146

F

facteurs irréductibles, 244
factorisation (homomorphisme), 24
Fermat-Euler (théorème de), 264
Fermat-Wiles (théorème de), 275
forme canonique d'une isométrie, 163

G

Gauss (lemme de), 243, 308
groupe, 15
groupe affine, 118
groupe alterné, 81
groupe des homothéties et translations, 120
groupe orthogonal, 154
groupe symétrique, 79
groupe
  abélien, 15
  cyclique, 59
  monogène, 19

p-groupe, 91
quotient, 23
simple, 64
H
homomorphisme d'anneaux, 192
homomorphisme de groupes, 16
I
idéal, 195
idéal
maximal, 199
premier, 205
principal, 237
indice d'un sous-groupe, 21
invariants d'un groupe abélien, 67
irréductibles(éléments), 241
isomorphisme
affine, 112
de groupe, 16
L
Lagrange (théorème de), 22
Leibniz (fonction de), 133
lemniscate de Bernoulli, 178
loi de composition interne, 13
N
Noether (théorème de), 46
nombre
algébrique, 289
de Liouville, 293
transcendant, 292
nombres
de Fermat, 272
de Mersenne, 270
normalisateur, 45
noyau, 16
O
ordre d'un élément, 19
ordre d'un groupe, 15
orientation, 121
P
permutation
nombre d'inversions, 81
signature, 81
pgcd, ppcm, 242
polyèdre convexe, 146
polynôme, 213
polynôme
cyclotomique, 220
de Lagrange, 224
dérivé, 217
division euclidienne, 215
formule de Leibniz, 218
formule de Taylor, 218
minimal, 239
primitif, 310
premiers dans leur ensemble, 241
produit direct de groupes, 25
produit semi-direct de groupes, 47
Q
quadrature du cercle, 298
R
régulière (opération), 13
résidu quadratique, 267
résoluble (groupe), 69
racine primitive de l'unité, 59
relation d'équivalence, 11
repère affine, 137
repère cartésien, 107
rotation-symétrie, 167
S
similitude, 170
sous-anneau, 194
sous-corps premier, 205
sous-espace affine, 114
sous-groupe
caractéristique, 18
dérivé, 69
de Sylow, 91
distingué, 18
stathme euclidien, 238
strophoïde droite, 179
Sylow (théorème de), 91
symétrie
hyperplane, 157
orthogonale, 157
symétrie glissée, 159
symétrisation, 27
T
théorème chinois, 249
translations, 106
transposition, 79
transposition simple, 79
transvection, 35
trisection d'un angle, 298
V
vissage, 167
W
Wantzel (théorème de), 296
Wilson (théorème de), 265