Vincent Beck, Yves Belaud

Notes du cours Algèbre Approfondie

1 Arithmétique : anneaux factoriels

Dans cette partie du cours, on va étudier une classe d'anneaux, un peu plus générale que celles vues au premier semestre : les anneaux factoriels. Au contraire des anneaux principaux et euclidiens, cette classe d'anneaux à la remarquable propriété d'être stable par passage aux anneaux de polynômes (c'est l'un des résultats qu'on montrera) : si A est factoriel alors A[X] l'est aussi. L'autre intérêt des anneaux factoriels est qu'ils partagent de très nombreuses propriétés arithmétiques avec les anneaux principaux (unicité de la décompositions en irréductibles, existence de pgcd et de ppcm,...), la grande différence est que l'on ne dispose pas d'identité de Bézout.

Dans tout ce cours, le mot anneau désigne un anneau commutatif unitaire. Si A est un anneau, on désigne par $\mathrm{A}^\times$ l'ensemble des éléments inversibles de A. La lettre k désigne un corps commutatif.

1.1 Différents types d'éléments dans un anneau

Divisibilité

Ce paragraphe rappelle les définitions sur les notions de divisibilité, diviseur, multiple dans un anneau commutatif quelconque. Lorsqu'on applique ces définitions à l'anneau $\mathbb{Z}$ des entiers relatifs, on retrouve les définitions standards connues depuis le collège.

Proposition-Définition 1 – Divisibilité. Soient A un anneau et $a, b \in \mathrm{A}$. On dit que b divise a (ou que b est un diviseur de a ou que a est un multiple de b) et on écrit $b \mid a$ si l'une des propriétés équivalentes suivantes est vérifiée :

(i) $\exists c \in \mathrm{A}$ tel que $bc = a$
(ii) $a \in (b)$
(iii) $(a) \subset (b)$

Exercice 1 – Relation de préordre. La relation de divisibilité est une relation de préordre sur A c'est-à-dire qu'elle est réflexive et transitive.

Proposition-Définition 2 – Relation être associé. Soit A un anneau. On dit que a et b sont associés si l'une des propriétés équivalentes suivantes est vérifiée :

(i) $b \mid a$ et $a \mid b$;
(ii) $a \in (b)$ et $b \in (a)$;
(iii) $(a) = (b)$.

La relation « être associé » est une relation d'équivalence.

Lorsque A est un anneau **intègre** (ce qui sera le cas pour nous en général), alors a et b sont associés si et seulement si il existe $u \in \mathrm{A}^\times$ tel que $a = bu$.

Exemple 3 Dans $\mathbb{Z}$, deux éléments sont associés s'ils sont égaux ou opposés.

Dans $k[\mathrm{X}]$, deux polynômes sont associés s'ils sont proportionnels.

Exercice 2 – D'un préordre à un ordre : le cas d'un anneau.

a) Soit X un ensemble et $\mathscr{R}$ une relation de préordre sur $\mathscr{R}$. Montrer que la relation $\mathscr{S}$ définie sur X par

$$a\mathscr{S}b \iff (a\mathscr{R}b \quad \text{et} \quad b\mathscr{R}a)$$

est une relation d'équivalence et que $\mathscr{R}$ induit une relation d'ordre sur $\mathrm{X}/\mathscr{S}$.

b) Soit A un anneau. En utilisant l'exercice 1, montrer que la relation $\mathscr{S}$ définie sur A par $a\mathscr{S}b$ si et seulement si $(a) = (b)$ est une relation d'équivalence.

c) Montrer que la relation de divisibilité induit sur $\mathrm{A}/\mathscr{S}$ une relation d'ordre dont la classe de 1 est le plus petit élément et la classe de 0 le plus grand élément. Déterminer les classes de 0 et de 1 pour la relation $\mathscr{S}$.

Remarque 4 — Un anneau dans lequel être associé n'est pas synonyme de différer d'un inversible. Dans l'anneau $\mathrm{A} = \mathbb{Z}[\mathrm{X}, \mathrm{Y}, \mathrm{Z}, \mathrm{T}]/(\mathrm{X}-\mathrm{ZY}, \mathrm{Y}-\mathrm{TX})$, les images x et y des éléments X et Y sont associées mais il n'existe pas $u \in \mathrm{A}^\times = \pm 1$ tel que $x = uy$.

PPCM et PGCD

Maintenant qu'on a défini cette propriété de divisibilité, on étudie les notions de divisibilité commune dans un sens et dans l'autre.

Définition 5 — PPCM. Soit A un anneau et $a, b \in \mathrm{A}$. On dit que c est un ppcm (plus petit commun multiple) de a et b et on écrit $c = \mathrm{ppcm}(a, b)$ si c vérifie les deux propriétés suivantes :

(i) $a \mid c$ et $b \mid c$ (c'est-à-dire c est un multiple commun à a et b)

(ii) si $a \mid m$ et $b \mid m$ alors $c \mid m$ (c'est-à-dire c divise tous les multiples communs à a et b).

Exercice 3 — Quelques cas triviaux. Soit A un anneau.

a) Déterminer $\mathrm{ppcm}(a, 0)$.

b) Déterminer $\mathrm{ppcm}(a, 1)$.

c) Déterminer $\mathrm{ppcm}(a, u)$ pour $u \in \mathrm{A}^\times$.

d) Plus généralement, montrer que, si a et a' sont associés et b et b' sont associés alors $\mathrm{ppcm}(a, b)$ existe si et seulement si $\mathrm{ppcm}(a', b')$ existe et qu'alors $\mathrm{ppcm}(a, b) = \mathrm{ppcm}(a', b')$.

Exercice 4 — Où on explique le terme « petit » de l'expression ppcm. Soit A un anneau et $a, b \in \mathrm{A}$, $\mathscr{S}$ la relation d'équivalence sur A définie dans l'exercice 2 et $\leqslant$ la relation d'ordre définie sur $\mathrm{A}/\mathscr{S}$ par la relation de divisibilité.

a) Montrer que $c \in \mathrm{A}$ est un ppcm de a et b si et seulement si la classe de c modulo $\mathscr{S}$ est la plus petite classe parmi les classes plus grandes que celle de a et celle de b.

b) Montrer que a, b ont un ppcm si et seulement si les classes de a et de b ont une borne supérieure dans $\mathrm{A}/\mathscr{S}$.

Exercice 5 — Caractérisation des couples ayant un ppcm. Soit A un anneau et $a, b \in \mathrm{A}$. Montrer que a et b admettent un ppcm si et seulement si $(a) \cap (b)$ est un idéal principal et que dans ce cas, c est un ppcm de a et b si et seulement si $(a) \cap (b) = (c)$.

Dans $\mathbb{Z}$ ou $k[\mathrm{X}]$, le ppcm (de deux éléments) existe toujours. Plus généralement, dans un anneau principal, le ppcm de deux éléments existe toujours. **Mais** ce n'est pas toujours le cas dans un anneau général.

Cependant, on démontrera que dans un anneau factoriel le ppcm de deux éléments existe toujours et qu'en plus, on dispose même d'une expression du ppcm.

Exercice 6 — PPCM de plus de deux éléments. Soit A un anneau et $(a_i)_{i \in \mathrm{I}}$ une famille d'éléments de A. On dit que c est un ppcm des a_i pour $i \in \mathrm{I}$ et on écrit $c = \mathrm{ppcm}(a_i,\ i \in \mathrm{I})$ si c vérifie les deux propriétés suivantes :

(i) $a_i \mid c$ pour tout $i \in \mathrm{I}$ (c'est-à-dire c est un multiple commun des a_i pour $i \in \mathrm{I}$).

(ii) si $a_i \mid m$ pour tout $i \in \mathrm{I}$ alors $c \mid m$ (c'est-à-dire c divise tous les multiples communs à tous les a_i).

a) On suppose que $c = \mathrm{ppcm}(a_i,\ i \in \mathrm{I})$. Montrer que la classe de c modulo $\mathscr{S}$ (voir l'exercice 2 pour la notation) est la plus petite classe plus grande que les classes de tous les a_i pour $i \in \mathrm{I}$.

b) Montrer que la famille $(a_i)_{i \in \mathrm{I}}$ admet un ppcm si et seulement si la famille des classes de a_i (pour $i \in \mathrm{I}$) dans $\mathrm{A}/\mathscr{S}$ admet une borne supérieure.

c) Montrer que la famille $(a_i)_{i \in \mathrm{I}}$ admet un ppcm si et seulement si l'idéal $\cap_{i \in \mathrm{I}}(a_i)$ est principal. Montrer que dans ce cas, $c = \mathrm{ppcm}(a_i,\ i \in \mathrm{I})$ si et seulement si $(c) = \cap_{i \in \mathrm{I}}(a_i)$.

d) Que se passe-t-il si l'un des a_i est nul ? si l'un des a_i est inversible ? Montrer que le ppcm ne change pas si on change les a_i en des éléments associés.

e) On suppose que pour tous $a, b \in \mathrm{A}$, le ppcm de a et b existe. Montrer que le ppcm de toute famille finie existe.

f) Trouver dans $\mathbb{Z}$ une famille infinie qui n'a pas de ppcm. En déduire que dans la question précédente, on ne peut pas retirer la condition de finitude de la famille considérée.

Après avoir étudié la notion de multiples communs, on s'intéresse maintenant aux diviseurs communs.

Définition 6 – PGCD. Soit A un anneau et $a, b \in \mathrm{A}$. On dit que c est un pgcd de a et b et on écrit $c = \mathrm{pgcd}(a, b)$ si c vérifie les deux propriétés suivantes

(i) $c \mid a$ et $c \mid b$ (c'est-à-dire c est un diviseur commun de a et b)

(ii) si $d \mid a$ et $d \mid b$ alors $d \mid c$ (c'est-à-dire tout diviseur commun à a et b divise c).

On dit que a et b sont *premiers entre eux* si $\mathrm{pgcd}(a, b)$ existe et vaut 1.

Remarque 7 – Critère d'existence du pgcd. Il n'existe pas de proposition équivalente à celle de l'exercice 5 pour l'existence du pgcd.

On a cependant une condition suffisante : si l'idéal $(a) + (b) = (a, b)$ est principal alors le pgcd de a et b existe et il est caractérisé par $d = \mathrm{pgcd}(a, b)$ si et seulement si $(a, b) = (d)$ (Démontrez-le). En particulier dans ce cas-là, on a une relation de Bézout pour le pgcd. Mais cette situation très favorable et n'est pas la situation d'un anneau quelconque, ni même celle d'un anneau factoriel non principal comme $\mathbb{Z}[\mathrm{X}]$ ou $k[\mathrm{X}, \mathrm{Y}]$.

Par exemple dans $\mathbb{Z}[\mathrm{X}]$, on a 2 et X qui sont premiers entre eux et pourtant $1 \notin (2, \mathrm{X})$.

Pour finir sur l'existence des pgcd et des ppcm, on a la condition nécessaire et suffisante d'existence suivante (Démontrez la) : soit A un anneau intègre, alors $\mathrm{ppcm}(a, b)$ existe pour tout $a, b \in \mathrm{A}$ si et seulement si $\mathrm{pgcd}(a, b)$ existe pour tout $a, b \in \mathrm{A}$ si et seulement si $(a) \cap (b)$ est principal pour tout $a, b \in \mathrm{A}$.

On retrouve maintenant les exercices correspondants aux exercices 3, 4 et 6 mais pour le pgcd.

Exercice 7 – Quelques cas triviaux. Soit A un anneau.

a) Déterminer $\mathrm{pgcd}(a, 0)$.

b) Déterminer $\mathrm{pgcd}(a, 1)$.

c) Déterminer $\mathrm{pgcd}(a, u)$ pour $u \in \mathrm{A}^\times$.

d) Plus généralement, montrer que, si a et a' sont associés et b et b' sont associés alors $\mathrm{pgcd}(a, b)$ existe si et seulement si $\mathrm{pgcd}(a', b')$ existe et qu'alors $\mathrm{pgcd}(a, b) = \mathrm{pgcd}(a', b')$.

Exercice 8 – Où on explique le terme « grand » de l'expression pgcd. Soit A un anneau et $a, b \in \mathrm{A}$, $\mathscr{S}$ la relation d'équivalence sur A définie dans l'exercice 2 et $\leqslant$ la relation d'ordre définie sur $\mathrm{A}/\mathscr{S}$ par la relation de divisibilité.

a) Montrer que $c \in \mathrm{A}$ est un pgcd de a et b si et seulement si la classe de c modulo $\mathscr{S}$ est la plus grande classe parmi les classes plus petites que celle de a et celle de b.

b) Montrer que a, b ont un pgcd si et seulement si les classes de a et de b ont une borne inférieure dans $\mathrm{A}/\mathscr{S}$.

Exercice 9 – PGCD de plus de deux éléments. Soit A un anneau et $(a_i)_{i \in \mathrm{I}}$ une famille d'éléments de A. On dit que c est un pgcd des a_i pour $i \in \mathrm{I}$ et on écrit $c = \mathrm{pgcd}(a_i,\ i \in \mathrm{I})$ si c vérifie les deux propriétés suivantes :

(i) $c \mid a_i$ pour tout $i \in \mathrm{I}$ (c'est-à-dire c est un multiple commun des a_i pour $i \in \mathrm{I}$).

(ii) si $m \mid a_i$ pour tout $i \in \mathrm{I}$ alors $m \mid c$ (c'est-à-dire c est un multiple de tous les diviseurs communs à tous les a_i).

a) On suppose que $c = \mathrm{pgcd}(a_i,\ i \in \mathrm{I})$. Montrer que la classe de c modulo $\mathscr{S}$ (voir l'exercice 2 pour la notation) est la plus grande classe plus petite que les classes de tous les a_i pour $i \in \mathrm{I}$.

b) Montrer que la famille $(a_i)_{i\in \mathrm{I}}$ admet un pgcd si et seulement si la famille des classes de a_i (pour $i \in \mathrm{I}$) dans $\mathrm{A}/\mathscr{S}$ admet une borne inférieure.

c) Que se passe-t-il si l'un des a_i est nul ? si l'un des a_i est inversible ? Montrer que le pgcd ne change pas si on change les a_i en des éléments associés.

d) On suppose que pour tous $a, b \in \mathrm{A}$, le pgcd de a et b existe. Montrer que le pgcd de toute famille finie existe.

e) Montrer que dans $\mathbb{Z}$, toute famille d'éléments admet un pgcd.

Différents types d'éléments dans un anneau

Dans ce paragraphe, on définit deux types d'éléments dans un anneau : les éléments irréductibles et les éléments premiers d'un anneau. Ces types d'éléments sont définis à partir de questions de divisibilité. La définition de la factorialité d'un anneau est liée au cas où ces deux notions coïncident.

Définition 8 – Élément irréductible. Soit A un anneau. On dit qu'un élément x est irréductible dans A si les conditions suivantes sont vérifiées

(i) x est non nul et non inversible
(ii) Si $x = bc$ alors b est inversible ou c est inversible.

Remarque 9 – Caractérisation des éléments irréductibles dans un anneau intègre. Si A est un anneau intègre alors x est irréductible si et seulement si $x \neq 0$ et (x) est un élément maximal de l'ensemble des idéaux principaux de A distincts de A.

Une conséquence de cette remarque est que, dans une anneau intègre, un élément associé à un élément irréductible est irréductible. En effet, la propriété « être irréductible » se lit sur l'idéal engendré par l'élément en question. Dans un anneau non nécessairement intègre, un élément associé à un élément irréductible est-il irréductible ?

Exemple 10 – Le cas des entiers et des polynômes. Dans $\mathbb{Z}$, les éléments irréductibles sont les nombres premiers et leurs opposés.

Dans $k[\mathrm{X}]$, les éléments irréductibles sont ceux qu'on a appelé les polynômes irréductibles c'est-à-dire les polynômes tels que si $\mathrm{P} = \mathrm{QR}$ alors Q ou R est un polynôme constant (en effet, on a $k[\mathrm{X}]^\times$ qui est formé des polynômes constants non nuls).

Exercice 10 – Stabilité de l'irréductibilité par isomorphisme. Soient A et B deux anneaux et $\varphi : \mathrm{A} \to \mathrm{B}$ un isomorphisme d'anneaux. Montrer que x est irréductible dans A si et seulement si $\varphi(x)$ est irréductible dans B.

Exercice 11 – Dans un corps. Déterminer les éléments irréductibles d'un corps.

On passe maintenant à la définition d'éléments premiers dans un anneau. Dans un anneau intègre, les éléments premiers sont des cas particuliers d'éléments irréductibles (voir le lemme 13). Dans un anneau principal, les deux notions coïncident ; dans un anneau factoriel aussi.

Proposition-Définition 11 – Élément premier. Soit A un anneau. On dit qu'un élément x est premier dans A si l'une des conditions équivalentes suivantes est vérifiée

(i) x non nul et non inversible et si $x \mid ab$ alors $x \mid a$ ou $x \mid b$.
(ii) $x \neq 0$ et (x) est un idéal premier de A
(iii) $x \neq 0$ et $\mathrm{A}/(x)$ est intègre

Remarque 12 – Élément premier et relation « être associé ». Un élément associé à un élément premier est premier. C'est immédiat puisque la propriété être premier se lit sur l'idéal engendré par l'élément en question.

Exercice 12 – Stabilité de la primalité par isomorphisme. Soient A et B deux anneaux et $\varphi : \mathrm{A} \to \mathrm{B}$ un isomorphisme d'anneaux. Montrer que x est premier dans A si et seulement si $\varphi(x)$ est premier dans B.

Lemme 13 – Premier $\implies$ irréductible. Dans un anneau intègre, les éléments premiers sont irréductibles.

Preuve. Soit p un élément premier de A. Alors p est non nul et non inversible. Montrons que si $p = ab$ alors a ou b est inversible. Comme $p = ab$, on a $p \mid ab$ et donc $p \mid a$ ou $p \mid b$. Si $p \mid a$ alors $a = pc$ et donc $p = ab = pbc$. Ainsi $p(1 - bc) = 0$. Comme $p \neq 0$ et A intègre, on a $bc = 1$ et donc b inversible. De même si $p \mid b$ alors a est inversible.

Exemple 14 Soit A un anneau et $a \in \mathrm{A}$. Montrer que $\mathrm{X} - a$ est un élément premier de A[X] si et seulement si A est intègre.

Lemme 15 – Anneau principaux et élément premier. Dans un anneau principal, tout élément irréductible x est premier. De plus $\mathrm{A}/(x)$ est alors un corps.

Preuve. Comme A est intègre, la remarque 9 assure que (x) est maximal parmi les idéal principaux de A distincts de A. Or A est principal, cette famille d'idéaux de A est donc la famille de tous les idéaux de A distincts de A c'est-à-dire que (x) est un idéal maximal et donc $\mathrm{A}/(x)$ est un corps. En particulier, c'est un anneau intègre et donc (x) est premier.

Ainsi, comme A est intègre, le lemme 13 assure que dans un anneau principal, éléments premiers et irréductibles coïncident.

Remarque 16 – Nombre premier– Élément premier. Comme $\mathbb{Z}$ est principal, l'exemple précédent montre que les nombres premiers (qui sont les éléments irréductibles de $\mathbb{Z}$) sont les éléments premiers de $\mathbb{Z}$. Ouf !

Exemple 17 – Le cas des corps. Dans un corps, les éléments sont nuls ou inversibles. Il n'y a donc pas d'éléments non nuls non inversibles et donc pas d'éléments premiers.

1.2 Différentes classes d'anneaux

Au premier semestre, vous avez vu trois grandes classes d'anneaux : les anneaux intègres, les anneaux principaux et les anneaux euclidiens. Rappelons les définitions et les premières propriétés.

ANNEAU INTÈGRE

Définition 18 – Anneau intègre. Soit A un anneau. On dit que A est intègre si, $\mathrm{A} \neq \{0\}$ et si pour tous $a, b \in \mathrm{A}, ab = 0$ implique $a = 0$ ou $b = 0$: les anneaux intègres sont ceux dans lesquels un produit est nul si et seulement si l'un des facteurs est nul.

Remarque 19 Il est clair qu'un corps est intègre : si $xy = 0$ et $x \neq 0$ alors en multipliant par x^{-1}, on a $x^{-1}xy = y = 0$. Par ailleurs, il est clair qu'un sous anneau d'un anneau intègre est encore intègre. On en déduit qu'un sous-anneau d'un corps est nécessairement intègre.

Il est remarquable que le réciproque soit vraie : si A est un anneau intègre, il existe un corps K et un morphisme injectif d'anneaux de $\mathrm{A} \to \mathrm{K}$. Ainsi A s'identifie à un sous-anneau du corps K. On peut même construire un corps minimal K vérifiant cette propriété (voir le TD 1) : c'est la notion de corps de fractions.

CORPS DE FRACTION D'UN ANNEAU INTÈGRE

Proposition-Définition 20 – Corps de fractions. Soit A un anneau **intègre**. Il existe un corps K vérifiant les propriétés suivantes :

(i) Il existe un morphisme injectif d'anneaux $i : \mathrm{A} \hookrightarrow \mathrm{K}$ (c'est-à-dire A s'identifie à un sous-anneau de K).

(ii) Pour tout morphisme injectif d'anneaux $j : \mathrm{A} \hookrightarrow \mathrm{L}$ où L est un corps, il existe un unique morphisme de corps $\varphi : \mathrm{K} \to \mathrm{L}$ tel que $j = \varphi \circ i$ (lorsqu'on part de A et qu'on va dans un corps, on peut passer par K).

Si K′ est un autre corps vérifiant les propriétés (i) et (ii) alors K et K′ sont isomorphes.

Le corps K peut se construire de la façon suivante : on considère l'ensemble suivant : $\mathrm{E} = \mathrm{A} \times \mathrm{A} \setminus \{0\}$ et la relation d'équivalence $\sim$ sur E définie par

$$(a, b) \sim (a', b') \iff ab' = ba' .$$

On pose alors $\mathrm{K} = \mathrm{E}/\sim$. La classe d'équivalence de (a, b) se note a/b. L'application i est donnée par $i(a) = a/1$ pour tout $a \in \mathrm{A}$: ainsi $i(a)$ est la classe d'équivalence de $(a, 1)$.

Le corps K ainsi construit s'appelle le *corps des fractions de* A et est noté Frac(A).

Preuve. Supposons que K et K′ sont deux corps vérifiant (i) et (ii). On note $i : \mathrm{A} \hookrightarrow \mathrm{K}$ et $i' : \mathrm{A} \hookrightarrow \mathrm{K}'$ les morphismes injectifs donnés par (i).

Comme K vérifie le point (ii), il existe $\varphi : \mathrm{K} \to \mathrm{K}'$ tel que $i' = i \circ \varphi$. De même, K′ vérifie le point (ii) donc il existe $\psi : \mathrm{K}' \to \mathrm{K}$ tel que $i = i' \circ \psi$. On a alors $i = i \circ \varphi \circ \psi$. L'unicité dans le point (ii) assure alors que $\varphi \circ \psi = \mathrm{id}_{\mathrm{K}}$. De même, $\psi \circ \varphi = \mathrm{id}_{\mathrm{K}'}$. Ainsi φ et ψ sont deux isomorphismes réciproques l'un de l'autre.

Il s'agit à présent de vérifier que la construction donnée de K et i vérifie les propriétés souhaitées. Pour l'instant E n'est qu'un ensemble. On va construire deux lois sur K : une addition et une multiplication. Pour $a/b, c/d \in \mathrm{E}$, on pose

$$\frac{a}{b} + \frac{c}{d} = \frac{ad + bc}{bd} \qquad \text{et} \qquad \frac{a}{b} \times \frac{c}{d} = \frac{ac}{bd}.$$

Première étape : il s'agit de vérifier que ces définitions ont bien un sens c'est-à-dire que si $a/b = a'/b'$ et $c/d = c'/d'$ alors

$$\frac{ad + bc}{bd} = \frac{a'd' + b'c'}{b'd'} \qquad \text{et} \qquad \frac{ac}{bd} = \frac{a'c'}{b'd'}.$$

Exercice !

On vérifie ensuite que les lois $+$ et $\times$ sont associatives et commutatives (Exercice !). On vérifie que $0/1$ est élément neutre pour $+$ et que $1/1$ est élément neutre pour $\times$ (Exercice !). On vérifie que $\dfrac{-a}{b}$ est l'opposé de $\dfrac{a}{b}$ pour $+$ (Exercice !). Ainsi $(\mathrm{K}, +)$ est un groupe. On vérifie ensuite que $\times$ est distributive par rapport à $+$. Ainsi K est un anneau commutatif unitaire. On vérifie que $a/b = 0/1$ si $a = 0$ (Exercice). On considère alors $a/b \in \mathrm{K}$ avec $a/b \neq 0$. On vérifie que b/a est l'inverse de a/b pour $\times$ (Exercice !). Ainsi $(\mathrm{K}, +, \times)$ est un corps.

On vérifie (Exercice !) que i est un morphisme d'anneaux unitaires. Vérifions que i est injectif. Si $a/1 = 0/1$, on a $a = 0$ et donc i injectif.

Montrons que K vérifie le point (ii). On veut définir $\varphi(a/b)$. On pose $\varphi(a/b) = j(a)j(b)^{-1}$ (cela a bien un sens puisque $j(b) \neq 0$ et donc est inversible dans L puisque j est injectif et $b \neq 0$). Il s'agit ensuite de vérifier que φ est bien définie c'est-à-dire que si $a/b = a'/b'$ alors $j(a)j(b)^{-1} = j(a')j(b')^{-1}$.

On a alors $\varphi(a/1) = j(a)j(1)^{-1} = j(a)$ c'est-à-dire $\varphi \circ i = j$

Enfin, pour conclure, il reste à montrer qu'il n'y a pas d'autre choix pour construire φ. Comme on veut que $\varphi \circ i = j$, on a $\varphi(a/1) = j(a)$ nécessairement pour tout $a \in \mathrm{A}$. Pour $b \neq 0$, comme $\varphi(1/b) = \varphi((b/1)^{-1}) = \varphi(b/1)^{-1} = j(b)^{-1}$, on obtient que nécessairement $\varphi(a/b) = \varphi(a/1 \cdot 1/b) = \varphi(a/1)\varphi(1/b) = j(a)j(b)^{-1}$.

Remarque 21 — Les nombres rationnels. Lorsqu'on applique cette construction à l'anneau intègre $\mathbb{Z}$, le corps qu'on construit ainsi est le corps des nombres rationnels $\mathbb{Q}$.

Remarque 22 — Fractions rationnelles. Lorsqu'on applique cette construction à l'anneau intègre $k[\mathrm{X}]$, le corps qu'on construit ainsi est le corps des fractions rationnelles en X : $k(\mathrm{X})$.

Exercice 13 — Anneaux intermédiaires. Soit A un anneau intègre et K son corps de fraction. Déterminer les sous-anneaux de K contenant A : montrer qu'ils sont caractérisés par une partie multiplicative de A (c'est-à-dire une partie $\mathrm{S} \subset \mathrm{A}$ telle que $1 \in \mathrm{S}$ et $ss' \in \mathrm{S}$ si $s, s' \in \mathrm{S}$).

Que se passe-t-il pour $\mathbb{Z}$? Et pour un anneau factoriel ?

ANNEAU EUCLIDIEN

Définition 23 — Anneau euclidien. Soit A un anneau. On dit que A est euclidien si les deux conditions suivantes sont vérifiées

(i) A est intègre

(ii) Il existe une fonction $\varphi : \mathrm{A} \setminus \{0\} \to \mathbb{N}$ (appelée stathme) vérifiant la propriété suivante :

$$\forall\, (a, b) \in \mathrm{A} \times \mathrm{A} \setminus \{0\}, \qquad \exists\, (q, r) \in \mathrm{A}^2, \qquad a = bq + r \quad \text{et} \quad (r = 0 \text{ ou } \varphi(r) < \varphi(b))$$

Au premier semestre, vous avez vu une version différente d'anneau euclidien :

Définition 24 — Anneau euclidien Semestre 1. Soit A un anneau. On dit que A est euclidien si les deux conditions suivantes sont vérifiées

(i) A est intègre

(ii) Il existe une fonction $\delta : \mathrm{A} \smallsetminus \{0\} \to \mathbb{N}$ (appelé stathme) vérifiant les propriétés suivantes :

$$\forall (a,b) \in \mathrm{A} \times \mathrm{A} \smallsetminus \{0\}, \qquad \exists (q,r) \in \mathrm{A}^2, \qquad a = bq + r \quad \text{et} \quad (r = 0 \text{ ou } \delta(r) < \delta(b))$$

et

$$\forall (a,b) \in (\mathrm{A} \smallsetminus \{0\})^2, \qquad \delta(a) \leqslant \delta(ab)$$

Les deux définitions sont équivalentes. La première est utile pour montrer qu'un anneau est euclidien : on a moins de contraintes sur le stathme qu'on cherche. La deuxième sert lorsqu'on sait qu'on a un anneau euclidien, on peut utiliser un stathme euclidien avec plus de propriétés que simplement la division euclidienne : cela peut être utile pour simplifier des calculs.

Exercice 14 — Équivalence. Montrer l'équivalence entre les deux définitions.

Indications : on pourra poser $\delta(a) = \min(\varphi(ab),\ b \in \mathrm{A} \smallsetminus \{0\})$ et effectuer la division euclidienne (pour φ) de a par bc où c est tel que $\delta(b) = \varphi(bc)$.

Les anneaux euclidiens sont ceux dans lequel on dispose d'un algorithme explicite pour calculer le pgcd : l'algorithme d'Euclide et aussi pour calculer les coefficients de Bézout (c'est-à-dire u et v tel que $ua + vb = d$ où $d = \mathrm{pgcd}(a,b)$). Cela a été vu au premier semestre.

Exemple 25 L'anneau $\mathbb{Z}$ est euclidien avec pour stathme la valeur absolue. Si k est un corps alors $k[\mathrm{X}]$ est euclidien avec pour stathme le degré.

Exercice 15 — À quelle condition un anneau de polynômes est-il euclidien ?. Soit A un anneau. Montrer que les propriétés suivantes sont équivalentes :

(i) A est une corps

(ii) $\mathrm{A}[\mathrm{X}]$ est euclidien

(iii) $\mathrm{A}[\mathrm{X}]$ est principal

La propriété suivante sert essentiellement à montrer qu'un anneau n'est pas euclidien, comme par exemple dans l'application 27.

Propriété 26 Soit A un anneau euclidien. Il existe $x \in \mathrm{A} \smallsetminus \mathrm{A}^\times$ tel que la restriction à $0 \cup \mathrm{A}^\times$ de la surjection canonique $\pi : \mathrm{A} \to \mathrm{A}/(x)$ est surjective.

Dans ces conditions, $\mathrm{A}/(x)$ est alors un corps.

Preuve. Si A est un corps alors $x = 0$ convient. Sinon, A n'est pas un corps, donc $\mathrm{A}^\times \cup \{0\} \subsetneq \mathrm{A}$. On peut donc choisir x tel que $\varphi(x) = \inf\{\varphi(y),\ y \in \mathrm{A} \smallsetminus (\mathrm{A}^\times \cup \{0\})\}$.

Il s'agit à présent pour $z \in \mathrm{A}/(x)$ de trouver $r \in \mathrm{A}^\times \cup \{0\}$ tel que $z = \pi(r)$. On écrit $z = \pi(y)$. On effectue la division de y par x : $y = qx + r$ avec $r = 0$ ou $\varphi(r) < \varphi(x)$.

Si $r = 0$ alors $y = qx$ et donc $\pi(y) = 0 = \pi(0)$. Si $r \neq 0$ alors, comme $\varphi(r) < \varphi(x)$, on en déduit que r est inversible. Comme $\pi(y) = \pi(r)$, on obtient le résultat souhaité.

Montrons à présent que $\mathrm{A}/(x)$ est un corps. Comme $x \notin \mathrm{A}^\times$, $\mathrm{A}/(x) \neq \{0\}$. Par ailleurs, tout élément non nul de $\mathrm{A}/(x)$ est l'image d'un élément inversible de A donc est inversible dans $\mathrm{A}/(x)$: si $z = \pi(r)$ avec r inversible alors, si r' est l'inverse de r (dans A), $\pi(r')$ est l'inverse de z dans $\mathrm{A}/(x)$.

Application 27 Soit $\alpha = (1+i\sqrt{19})/2 \in \mathbb{C}$. L'anneau $\mathrm{A} = \mathbb{Z}[\alpha] = \{\mathrm{P}(\alpha), \mathrm{P} \in \mathbb{Z}[\mathrm{X}]\}$ n'est pas euclidien.

En effet, $\mathrm{A}^\times = \{\pm 1\}$ (démontrez-le, on pourra introduire la norme). Ainsi $\mathrm{A}^\times \cup \{0\}$ a 3 éléments.

Si A était euclidien d'après la remarque ci-dessous alors il existerait x tel que $\mathrm{A}/(x)$ soit un corps à 2 ou 3 éléments c'est-à-dire $\mathbb{Z}/2\mathbb{Z}$ ou $\mathbb{Z}/3\mathbb{Z}$. Par ailleurs, comme $\alpha^2 - \alpha + 5 = 0$, l'image β de α dans $\mathrm{A}/(x)$ vérifie la même relation c'est-à-dire $\beta^2 - \beta + 5 = 0$. Mais aucun élément de $\mathbb{Z}/2\mathbb{Z}$ ou $\mathbb{Z}/3\mathbb{Z}$ ne vérifie cette relation.

ANNEAU PRINCIPAL

Définition 28 — Anneau principal. Soit A un anneau. On dit que A est principal si les deux conditions suivantes sont vérifiées

(i) A est intègre

(*ii*) Tout idéal de A est principal c'est-à-dire tout idéal de A est engendré par un élément ou encore pour tout idéal I de A, il existe $a \in \mathrm{A}$ tel que $\mathrm{I} = (a) := \{ab,\ b \in \mathrm{A}\} = a\mathrm{A}$.

Théorème 29 – Euclidien $\Longrightarrow$ Principal. Un anneau euclidien est principal.

Preuve. Soit I un idéal non nul. À l'aide de la division euclidienne, on montre que $\mathrm{I} = (a)$ où a vérifie $\varphi(a) = \inf\{\varphi(b),\ b \in \mathrm{I} \setminus \{0\}\}$

Exercice 16 – Anneau non principaux. Montrer que $\mathbb{Z}[\mathrm{X}]$ n'est pas principal (indication : on pourra considérer $(2, \mathrm{X})$). Montrer que $k[\mathrm{X}, \mathrm{Y}]$ n'est pas principal (indication : on pourra considérer (X, Y)).

Au premier semestre, le théorème suivant a été vu. Avec ce qu'on va voir par la suite, il s'énonce sous la forme un anneau principal est factoriel.

Théorème 30 – Principal $\Longrightarrow$ Factoriel. Soit A un anneau principal. Alors tout élément non nul de A se décompose comme un produit d'irréductibles : $a = p_1 \cdots p_s$ avec p_i irréductible pour tout i.

De plus, cette décomposition est unique à l'ordre et aux inversibles près : si $a = q_1 \cdots q_r$ avec q_i irréductible pour tout i alors $r = s$ et il existe $\sigma \in \mathfrak{S}_s$ tel que, pour tout $i \in [\![1\,,\, s]\!]$, $q_{\sigma(i)}$ et p_i soient associés.

Définition des anneaux factoriels

On a vu que $k[\mathrm{X}, \mathrm{Y}]$ ou $\mathbb{Z}[\mathrm{X}]$ n'était pas principal : on a cependant envie de factoriser les polynômes en réduisant leur degré au fur et à mesure jusqu'à ce qu'on ne puisse plus et on se pose la question de savoir si cette décomposition est unique : les anneaux factoriels qu'on va étudier sont précisément ceux dans lesquels on peut le faire.

Définition 31 Soit A un anneau. On dit que A est factoriel s'il vérifie les trois propriétés suivantes :

(*i*) A est intègre

(*ii*) tout élément non nul de A se décompose comme un produit d'irréductibles :

$$\forall\, a \in \mathrm{A} \setminus \{0\}\,, \qquad \exists\, p_1, \ldots, p_s \text{ irréductibles tels que } a = p_1 \cdots p_s \tag{EI}$$

(*iii*) La décomposition en irréductible d'un élément non nul de A est unique à l'ordre et au inversible près : si $a = q_1 \cdots q_r$ avec q_i irréductible pour tout i alors $r = s$ et il existe $\sigma \in \mathfrak{S}_s$ tel que, pour tout $i \in [\![1\,,\, s]\!]$, $q_{\sigma(i)}$ et p_i soient associés. (UI)

Remarque 32 L'axiome (*ii*) est appelé (EI) pour « Existence d'un décomposition en Irréductibles ». L'axiome (*iii*) est appelé (UI) pour « Unicité de la décomposition en Irréductibles ».

Au vu de la définition qui précède, le théorème 30 se résume ainsi : un anneau principal est factoriel.

1.3 Étude des anneaux factoriels

Caractérisation des anneaux factoriels

L'objectif de ce paragraphe est de voir différentes caractérisations des anneaux factoriels qui permettent de montrer plus facilement qu'un anneau est factoriel.

Commençons par deux lemmes.

Lemme 33 – Élément premier et irréductible dans un anneau factoriel. Soit A un anneau factoriel. Les éléments irréductibles et les éléments premiers sont les mêmes.

Preuve. Un anneau factoriel est intègre donc les éléments premiers sont irréductibles (lemme 13).

Considérons à présent un élément irréductible x et montrons qu'il est premier. Par hypothèse, x est non nul et non inversible. Supposons que $x \mid ab$ et posons c tel que $xc = ab$. On veut montrer que $x \mid a$ ou $x \mid b$.

Si $a = 0$ ou $b = 0$ alors $x0 = a$ ou $x0 = b$ c'est-à-dire $x \mid a$ ou $x \mid b$.

Sinon, a et b sont non nuls. On écrit la décomposition de a en irréductible $a = p_1 \cdots p_s$ avec p_i irréductible pour tout i. De même, on écrit $b = q_1 \cdots q_r$ avec q_i irréductible pour tout i. Enfin, il existe $c \in \mathrm{A}$ tel que $xc = ab$ et $c = c_1 \cdots c_t$ avec c_i irréductible pour tout i.

Ainsi $xc_1 \cdots c_t = p_1 \cdots p_s q_1 \cdots q_r$ sont deux décompositions en irréductibles de ab. On en déduit, par l'axiome (UI) d'unicité, que x est associée à l'un des p_i (et donc $x \mid a$) ou à l'un des q_i (et donc $x \mid b$).

Lemme 34 — Décomposition en éléments premiers. Soit A un anneau intègre. Soit $p_1, \ldots, p_s$, $q_1, \ldots, q_r$ des éléments premiers de A. Si $p_1 \cdots p_s = q_1 \ldots q_r$ alors $r = s$ et il existe $\sigma \in \mathfrak{S}_s$ tels que p_i et $q_{\sigma(i)}$ sont associés.

Preuve. On raisonne par récurrence sur s. Si $s = 0$ et $r \neq 0$ alors $q_1 \cdots q_r = 1$ et les q_i sont inversibles ce qui est absurde puisqu'ils sont premiers. Donc $r = 0$.

Supposons $s > 0$. On a $p_1 \mid q_1 \cdots q_r$. Donc comme p_1 est premier, il existe j tel que $p_1 \mid q_j$. Il existe donc x tel que $p_1 x = q_j$. Ainsi $q_j \mid x p_1$ et donc $q_j \mid x$ ou $q_j \mid p_1$.

Dans le premier cas, on écrit $q_j y = x$ et on a alors $p_1 q_j y = q_j$ et donc $q_j(1 - p_1 y) = 0$. Comme A est intègre et $q_j \neq 0$, on obtient $p_1 y = 1$ et p_1 est inversible. NON. On est donc dans le second cas.

Ainsi, on a les relations de divisibilité $q_j \mid p_1$ et $p_1 \mid q_j$. On en déduit que p_1 et q_j sont associés c'est-à-dire il existe u tel que $u p_1 = q_j$ puisque A est intègre.

Toujours par intégrité de A, on en déduit alors

$$p_2 \cdots p_s = q_1 \cdots q_{j-1} u q_{j+1} \cdots q_r.$$

Comme $q_{j-1} u$ est premier puisque q_{j-1} l'est et u est inversible, on retrouve une égalité entre deux décompositions en élément premier avec cette fois-ci dans le premier membre $s-1$ facteurs. On applique alors l'hypothèse de récurrence pour conclure en posant $\sigma(1) = j$.

Remarque 35 Ainsi, dans un anneau intègre, il y a unicité de la décomposition en éléments premiers.

Avant de passer au résultat central, présentons une application du lemme qui précède.

Application 36 — Anneaux de polynômes. Soit A un anneau intègre ; $a_1, \ldots, a_s$ des éléments distincts de A, $b_1, \ldots, b_r$ des éléments distincts de A et $n_1, \ldots, n_s, m_1, \ldots, m_r \in \mathbb{N}^*$.

Si $(\mathrm{X} - a_1)^{n_1} \cdots (\mathrm{X} - a_r)^{n_r} = (\mathrm{X} - b_1)^{m_1} \cdots (\mathrm{X} - b_s)^{m_s}$ alors $r = s$ et il existe $\sigma \in \mathfrak{S}_s$ tel que pour tout i, $a_i = b_{\sigma(i)}$ et $n_i = m_{\sigma(i)}$.

Théorème 37 — Caractérisation des anneaux factoriels. Soit A un anneau intègre. On a les équivalences suivantes :

(i) A est factoriel

(ii) Dans A, les éléments irréductibles sont premiers et tout élément admet une décomposition en irréductibles (EI).

(iii) Tout élément non nul de A se décompose en produit d'éléments premiers :

$$\forall a \in \mathrm{A} \setminus \{0\}, \quad \exists p_1, \ldots, p_r \text{ premiers}, \qquad a = p_1 \cdots p_r$$

Preuve. Le lemme 33 assure que (i) $\Rightarrow$ (ii).
(ii) $\Rightarrow$ (iii). C'est évident.
(iii) $\Rightarrow$ (i). Comme A est intègre, un premier est irréductible. On a donc (EI). Montrons que sous l'hypothèse (iii), un élément irréductible est premier. L'axiome (UI) résultera alors du lemme 34.

Soit q irréductible, il est non nul. On peut donc écrire $q = p_1 \cdots p_s$ avec p_i premier. Comme q est irréductible, il est non inversible et donc $s \neq 0$. De plus, on a p_1 inversible ou $p_2 \cdots p_s$ inversible. Le premier cas est impossible, donc on est dans le deuxième cas et nécessairement $s = 1$. Ainsi $q = p_1$ est premier.

ÉCRITURE DANS UN ANNEAU FACTORIEL

Définition 38 — Système de représentants. Soit A un anneau factoriel. La relation « être associés » est une relation d'équivalence sur l'ensemble des éléments irréductibles (ou premier, c'est la même chose) de A. On note $\mathscr{P}$ une famille de représentants des classes d'équivalence de l'ensemble des éléments irréductibles pour la relation « être associés » : ce choix signifie que pour tout élément irréductible x de A, il existe un unique élément de $\mathscr{P}$ qui est associé à x.

Exemple 39 — Les anneaux classiques. Le cas de $\mathbb{Z}$. On a vu que les éléments irréductibles sont les $\pm p$ où p est un nombre premier. Par ailleurs, $\mathbb{Z}^\times = \{\pm 1\}$. Ainsi l'ensemble des nombres premiers est

une famille de représentants des classes d'équivalence de l'ensemble des éléments irréductibles pour la relation « être associés ».

Le cas $k[X]$. Les éléments irréductibles sont les polynômes irréductibles. Par ailleurs $k[X]^\times = k^*$. Ainsi tout élément non nul de $k[X]$ (pas seulement les irréductibles) est associé à un unique polynôme unitaire (il suffit de multiplier par l'inverse du coefficient dominant). Finalement, on peut choisir comme représentants des classes d'équivalence, l'ensemble des polynômes irréductibles unitaires.

Proposition-Définition 40 – Multiplicités. Soit A un anneau factoriel et $\mathscr{P}$ une famille de représentants des classes d'équivalence de l'ensemble des éléments irréductibles pour la relation « être associés ».

Soit $a \in A \setminus \{0\}$. Pour $p \in \mathscr{P}$, il existe un unique élément $\nu_p(a) \in \mathbb{N}$ tel que $p_p^\nu(a) \mid a$ et $p^{\nu_p(a)+1} \nmid a$. Il y a seulement un nombre fini de $p \in \mathscr{P}$ pour lequel $\nu_p(a)$ est non nul. Cet entier $\nu_p(a)$ est le nombre d'éléments associés à p dans une décomposition de a en produit d'irréductibles.

L'entier $\nu_p(a)$ s'appelle la multiplicité de p dans A ou la valuation de a relativement à p.

Preuve. Considérons une décomposition de $a = p_1 \cdots p_s$ en irréductibles. Montrons que si $p \in \mathscr{P}$ alors p^i ne divise pas a pour $i > s$. En effet, sinon on peut écrire $a = p^i c$ et en décomposant c en irréductibles, on obtient une décomposition de a en irréductibles avec au moins i facteurs, ce qui contredit l'unicité de la décomposition en irréductible dans A.

Ainsi, l'ensemble des entiers tel que p^i divise a est non vide (il contient 0) et majoré (par s). Il contient donc un plus grand élément, qu'on note $\nu_p(a)$. De plus, si $n < \nu_p(a)$ alors $p^{n+1} \mid a$. D'où l'unicité de $\nu_p(a)$.

Supposons que $\nu_p(a) \neq 0$ alors $p \mid a$. Or il n'y a qu'un nombre fini d'éléments de $\mathscr{P}$ qui divise a [1] En effet, si $p \mid a$, on peut écrire $a = pc = p_1 \cdots p_s$ et en considérant une décomposition en irréductible de c et l'unicité de la décomposition en irréductible de a, on obtient que p est associé à l'un des p_i. On a donc au plus s éléments de p qui vérifient $\nu_p(a) > 0$.

Soit m le nombre d'indices i tels que p_i est associé à p. Montrons que $m = \nu_p(a)$. Quitte à réordonner le produit, on peut supposer que ce sont $p_1, \ldots, p_m$ qui sont associés à p. En écrivant $p_i = u_i p$ pour $1 \leqslant i \leqslant m$, on obtient $a = p^m u_1 \cdots u_m p_{m+1} \cdots p_s$ et donc $p^m \mid a$. Il reste à montrer que p^{m+1} ne divise pas a. Mais si $p^{m+1} \mid a$ alors on peut écrire $a = p^{m+1} c = p_1 \cdots p_s$. En décomposant c en irréductibles, l'unicité de la décomposition en irréductible de a fournit alors $m+1$ indices i tel que p_i soit associés à p ce qui contredit la définition de m.

Proposition 41 – Joli écriture. Soit A un anneau factoriel et $\mathscr{P}$ une famille de représentants des classes d'équivalence de l'ensemble des éléments irréductibles pour la relation « être associés ». Tout élément $a \in A \setminus \{0\}$ s'écrit sous la forme

$$a = u \prod_{p \in \mathscr{P}} p^{\nu_p(a)}$$

où $u \in A^\times$.

Par ailleurs, s'il existe une famille d'entiers $(\mu_p)_{p \in \mathscr{P}}$ dont seul un nombre fini est non nul et un élément $v \in A^\times$ tels que

$$a = v \prod_{p \in \mathscr{P}} p^{\mu_p}$$

alors $u = v$ et $\mu_p = \nu_p(a)$ pour tout $p \in \mathscr{P}$.

Preuve. Soit $a = p_1 \ldots p_s$ une décomposition en irréductibles. En écrivant p_i sous la forme $u_i q_i$ où $q_i \in \mathscr{P}$ et u_i inversible et comme $\nu_p(a)$ est le nombre d'indice i tel que $q_i = p$, on obtient

$$a = u_1 \cdots u_m \prod_{\{p \in \mathscr{P}, \nu_p(a) > 0\}} p^{\nu_p(a)}.$$

En posant $u = u_1 \cdots u_m \in A^\times$, et en utilisant le fait que $p_p^\nu(a) = 1$ si $\nu_p(a) = 0$, on obtient l'écriture souhaitée.

En effet, pour $p \in \mathscr{P}$, on a $p_p^\mu \mid a$ donc $\mu_p \leqslant \nu_p(a)$. Comme A est intègre, on peut simplifier par p_p^μ pour obtient

1. Attention, il peut exister une infinité d'irréductibles qui divise a : pensez par exemple à $k[X]$: si $P \mid Q$ alors $\lambda P \mid Q$ pour tout $\lambda \in k^*$, c'est l'un des intérêts de considérer une famille de représentants plutôt que l'ensemble des tous les éléments irréductibles.

$$v = u \prod_{p \in \mathscr{P}} p^{\nu_p(a) - \mu_p}$$

S'il existe p tel que $\nu_p(a) > \mu_p$ alors l'égalité précédent montre que p est inversible. NON. On obtient ainsi $\nu_p(a) = \mu_p$ pour tout p puis $u = v$.

Corollaire 42 — Divisibilité-PPCM-PGCD dans une anneau factoriel. Soit A un anneau factoriel et $\mathscr{P}$ une famille de représentants des classes d'équivalence de l'ensemble des éléments irréductibles pour la relation « être associés ».

Soit $a, b \in \mathrm{A} \setminus \{0\}$. On a les caractérisations suivantes

(i) Pour tout $p \in \mathscr{P}$, on a $\nu_p(ab) = \nu_p(a) + \nu_p(b)$.
(ii) $a \mid b$ si et seulement si pour tout $p \in \mathscr{P}$, on a $\nu_p(a) \leqslant \nu_p(b)$.
(iii) a et b associée si et seulement si, pour tout $p \in \mathscr{P}$, on a $\nu_p(a) = \nu_p(b)$.
(iv) $\mathrm{ppcm}(a, b)$ existe et vérifie $\nu_p(\mathrm{ppcm}(a, b)) = \max(\nu_p(a), \nu_p(b))$ pour tout $p \in \mathscr{P}$.
(v) $\mathrm{pgcd}(a, b)$ existe et vérifie $\nu_p(\mathrm{pgcd}(a, b)) = \min(\nu_p(a), \nu_p(b))$ pour tout $p \in \mathscr{P}$.
(vi) a et b sont premiers entre eux si et seulement si $\nu_p(a)\nu_p(b) = 0$ pour tout $p \in \mathscr{P}$.

Preuve. Le point (i) résulte immédiatement de l'associativité et de la commutativité de la multiplication.

Montrons le point (ii). Si pour tout $p \in \mathscr{P}$, on a $\nu_p(a) \leqslant \nu_p(b)$, alors on écrit $b = ac$ avec

$$c = u^{-1} v \prod_{p \in \mathscr{P}} p^{\nu_p(b) - \nu_p(a)}.$$

où $u \in \mathrm{A}^\times$ est défini par a et $v \in \mathrm{A}^\times$ est défini par b.

Si $a \mid b$, on écrit $ac = b$ et on a $\nu_p(b) = \nu_p(a) + \nu_p(c)$ pour tout $p \in \mathscr{P}$.

Le point (iii) est immédiat à partir du point (ii). Les points (iv) et (v) aussi puisque le point (ii) dit que la relation de divisibilité se lit sur les multiplicités. Par exemple pour être un multiple comme de a et b, il faut que la multiplicité de p soit plus grand que celle de a et b c'est-à-dire plus grande que le max. Et pour être un ppcm, il faut qu'elle soit le plus petit possible...

Le point (vi) vient du fait que $min(\nu_p(a), \nu_p(b)) = 0$ si et seulement si l'un des deux nombres est nul.

La factorialité d'un anneau est suffisante pour obtenir les lemmes de Gauss. On peut même donner une caractérisation des anneaux factoriels à partir du lemme de Gauss (voir l'exercice 17).

Corollaire 43 — Lemmes de Gauss. Soit A un anneau factoriel et $a, b, c \in \mathrm{A} \setminus \{0\}$ vérifiant a et b premier entre eux.

Si $a \mid bc$ alors $a \mid c$.
Si $a \mid c$ et $b \mid c$ alors $ab \mid c$.

Preuve. Par hypothèse, on a $\nu_p(a) \leqslant \nu_p(b) + \nu_p(c)$ pour tout $p \in \mathscr{P}$. Si $\nu_p(a) = 0$ alors $\nu_p(a) \leqslant \nu_p(c)$. Si $\nu_p(a) = 0$ alors $\nu_p(b) = 0$ puisque a et b sont premiers entre eux (voir le corollaire 42 point (vi)). Ainsi $\nu_p(a) \leqslant \nu_p(c) + 0$. Finalement pour tout $p \in \mathscr{P}$, on a $\nu_p(a) \leqslant \nu_p(b)$.

Montrons le deuxième résultat : soit $p \in \mathscr{P}$, d'après le point (vi) du corollaire 42, on a $\nu_p(a) = 0$ ou $\nu_p(b) = 0$. Si $\nu_p(a) = 0$, on a $\nu_p(ab) = \nu_p(b) \leqslant \nu_p(c)$ puisque $b \mid c$. Si $\nu_p(b) = 0$, on a $\nu_p(ab) = \nu_p(a) \leqslant \nu_p(c)$ puisque $a \mid c$. Ainsi pour tout $p \in \mathscr{P}$, on a $\nu_p(ab) \leqslant \nu_p(c)$ et donc $ab \mid c$.

Exercice 17 — Factorialité et lemme de Gauss. Soit A un anneau intègre vérifiant (EI). Les deux propriétés suivantes sont équivalentes :

(i) Les irréductibles de A sont premiers (c'est-à-dire A est factoriel (voir 37)).
(ii) Si $a \mid bc$ et a est premier avec b alors $a \mid c$.

Proposition 44 — Corps de fraction d'un anneau factoriel. Soit A un anneau factoriel et $\mathrm{K} = \mathrm{Frac}(\mathrm{A})$. Tout élément $x \in \mathrm{K} \setminus \{0\}$ admet un représentant sous la forme

$$x = a/b \qquad \text{avec} \qquad a \text{ et } b \text{ premiers entre eux}.$$

De façon plus précise, on peut écrire

$$x = \frac{u \prod_{p \in \mathscr{P}} p^{m_p}}{\prod_{p \in \mathscr{P}} p^{n_p}}$$

avec $m_p n_p = 0$ pour tout p.

Unicité. De plus, si $x = a'/b'$ avec a' et b' premiers entre eux, alors a et a' sont associés et b et b' aussi.

Preuve. On écrit $x = a/b$ avec

$$x = \frac{u \prod_{p \in \mathscr{P}} p^{\nu_p(a)}}{v \prod_{p \in \mathscr{P}} p^{\nu_p(b)}} = \frac{uv^{-1} \prod_{p \in \mathscr{P}} p^{\nu_p(a)}}{\prod_{p \in \mathscr{P}} p^{\nu_p(b)}}.$$

On simplifie alors les puissances de p convenables pour obtenir

$$x = \frac{uv^{-1} \prod_{\{p \in \mathscr{P}, \nu_p(a) > \nu_p(b)\}} p^{\nu_p(a) - \nu_p(b)}}{\prod_{\{p \in \mathscr{P}, \nu_p(b) > \nu_p(a)\}} p^{\nu_p(b) - \nu_p(a)}}.$$

Unicité. On a $ab' = ba'$. Comme a et b sont premiers entre eux, on en déduit que $a \mid a'$. De même $a' \mid a$ et a et a' sont associés. En simplifiant par a, on obtient que b et b' sont associés.

Proposition 45 Soit A un anneau factoriel, $x \in \mathrm{Frac(A)}$ qui est racine d'un polynôme unitaire à coefficients dans A. Alors $b = 1$.

Preuve. Soit $\mathrm{P} = \mathrm{X}^n + a_1 \mathrm{X}^{n-1} + \cdots + a_n \in \mathrm{A}$ tel que $\mathrm{P}(x) = 0$. On écrit $x = a/b$ avec a et b premiers entre eux. On a alors $(a/b)^n + a_1(a/b)^{n-1} + \cdots + a_n = 0$. En multipliant par b^n, on en déduit que $a^n + a_1 ab + \cdots + a_n b^n = 0$. On écrit $a^n = -(a_1 ab + \cdots + a_n b^n)$. Ainsi $b \mid a^n$. Comme a et b sont premiers entre eux, on obtient que $b = 1$.

1.4 Anneaux de polynômes et anneaux factoriels : théorème de transfert

Définition 46 — Contenu. Soit A un anneau factoriel et $\mathrm{K} = \mathrm{Frac(A)}$. Soit $\mathrm{P} = a_0 + a_1 \mathrm{X} + \cdots + a_n \mathrm{X}^n \in \mathrm{A[X]}$. On dit que P est primitif si $\mathrm{pgcd(coeff(P))} = \mathrm{pgcd}(a_0, \ldots, a_n) = 1$.

Exemple 47 Un polynôme unitaire est toujours primitif, $2\mathrm{X} + 3 \in \mathbb{Z}[\mathrm{X}]$ est aussi primitif.

Proposition-Définition 48 Soit $\mathrm{P} \in \mathrm{K[X]} \smallsetminus \{0\}$. Il existe $u \in \mathrm{K}^\times$, $\mathrm{Q} \in \mathrm{A[X]}$ primitif tel que $\mathrm{P} = u\mathrm{Q}$. De plus, si $\mathrm{P} = v\mathrm{R}$ avec $v \in \mathrm{K}^\times$ et $\mathrm{R} \in \mathrm{A[X]}$ primitif alors il existe $w \in \mathrm{A}^\times$ tel que $u = wv$ et $\mathrm{Q} = w^{-1}\mathrm{R}$.

On note $u = c(\mathrm{P})$ et on l'appelle le contenu de P. On a $c(\mathrm{P}) \in \mathrm{A}$ si et seulement si $\mathrm{P} \in \mathrm{A[X]}$.

Preuve. Soit $\mathrm{P} = \sum_{i=0} n \frac{a_i}{b_i} \mathrm{X}^i = \frac{1}{q_1 \cdots q_n} \sum_{i=0}^{n} a_i \prod_{j \neq i} b_j \mathrm{X}^i$. On note

$$\mathrm{S(X)} = \sum_{i=0}^{n} a_i \prod_{j \neq i} b_j \mathrm{X}^i = \sum_{i=0}^{n} r_i \mathrm{X}^i$$

On pose alors $a = \mathrm{pgcd}(r_i)$ et on écrire $\mathrm{S} = a\mathrm{Q}$ avec Q primitif (puisque $\mathrm{pgcd}(cc_1, \ldots, cc_n) = c\,\mathrm{pgcd}(c_1, \ldots, c_n)$). On pose alors $u = a/(q_1 \cdots q_n)$.

Unicité. On a $v^{-1}u\mathrm{Q} = \mathrm{R}$. On va montrer que $v^{-1}u \in \mathrm{A}$. On écrit $\mathrm{Q} = \sum_{i=0}^{n} a_i \mathrm{X}^i$ et $\mathrm{R} = \sum_{i=0}^{n} b_i \mathrm{X}^i$ avec $a_i, b_i \in \mathrm{A}$ et $v^{-1}u = x/y$ avec $x, y \in \mathrm{A} \smallsetminus \{0\}$ et x, y premiers entre eux.

Si y non inversible dans A alors il existe p irréductible dans A tel que $p \mid y$. Mais $v^{-1}ua_i = b_i$ pour tout i donc $p \mid a_i$ pour tout i. Mais alors $p \mid \mathrm{pgcd}(a_0, \ldots, a_n)$ ce qui contredit que Q est primitif.

Ainsi $v^{-}1u \in \mathrm{A}$. De même, $u^{-1}v \in \mathrm{A}$ et $v^{-1}u \in \mathrm{A}^\times$.

Si $c(\mathrm{P}) \in \mathrm{A}$ alors comme Q est dans A[X], $\mathrm{P} = c(\mathrm{P})\mathrm{Q}$ est dans A[X]. Si $\mathrm{P} \in \mathrm{A[X]}$ alors on met en facteur $c \in \mathrm{A}$, le pgcd des coefficients de P : $\mathrm{P} = c\mathrm{Q}$. Comme $\mathrm{pgcd}(cc_1, \ldots, cc_n) = c\,\mathrm{pgcd}(c_1, \ldots, c_n)$ pour tous $c, c_i \in \mathrm{A}$, on a Q qui est primitif. Ainsi c est associé à $c(\mathrm{P})$ et donc $c(\mathrm{P}) \in \mathrm{A}$.

Proposition 49 — Lemme de Gauss. Le contenu est multiplicatif : pour $\mathrm{P}, \mathrm{Q} \in \mathrm{K[X]} \smallsetminus \{0\}$, on a $c(\mathrm{PQ}) = c(\mathrm{P})c(\mathrm{Q})$. En particulier, si $\mathrm{P}, \mathrm{Q} \in \mathrm{A[X]}$ sont primitifs alors PQ l'est aussi.

Preuve. On écrit $\mathrm{P} = c(\mathrm{P})\widetilde{\mathrm{P}}$ et $\mathrm{Q} = c(\mathrm{Q})\widetilde{\mathrm{Q}}$ avec $\widetilde{\mathrm{P}}$ et $\widetilde{\mathrm{Q}}$ primitifs. Si $\widetilde{\mathrm{P}}\widetilde{\mathrm{Q}}$ primitif, on obtient le résultat souhaité grâce à la propriété d'unicité ci-dessus.

Il s'agit donc de montrer que le produit de deux polynômes primitifs P et Q l'est. Si ce n'est pas le cas, il existe p irréductible de A tel que p divise tous les coefficients de PQ. On considère alors le morphisme d'anneaux

$$\varphi\colon \begin{cases} \mathrm{A}[\mathrm{X}] & \longrightarrow \mathrm{A}/(p)[\mathrm{X}] \\ \sum_{i=0}^{n} a_i \mathrm{X}^i & \longmapsto \sum_{i=0}^{n} \pi(a_i)\mathrm{X}^i \end{cases}$$

où π est la surjection canonique de $\mathrm{A} \to \mathrm{A}/(p)$. Par hypothèse, on a $\varphi(\mathrm{PQ}) = 0$. Mais $\varphi(\mathrm{PQ}) = \varphi(\mathrm{P})\varphi(\mathrm{Q})$. Or p est premier. Donc $\mathrm{A}/(p)$ est intègre et $\mathrm{A}/(p)[\mathrm{X}]$ aussi. Ainsi $\varphi(\mathrm{P}) = 0$ ou $\varphi(\mathrm{Q}) = 0$ c'est-à-dire que p divise tous les coefficients de P ou Q.

Remarque 50 — Inversibles dans un anneau de polynômes. Comme A est intègre, les éléments inversibles de A[X] sont des polynômes constants : ce sont les éléments inversibles de A : on a $\mathrm{A}[\mathrm{X}]^\times = \mathrm{A}^\times$.

Proposition 51 — Irréductibles dans un anneau de polynômes. Les irréductibles de A[X] sont les irréductibles de A est les $\mathrm{P} \in \mathrm{A}[\mathrm{X}]$ non constant tel que P est irréductible sur K[X] et P primitif.

Preuve. Si $a \in \mathrm{A}$ est irréductible dans A[X]. On écrit $a = pq$ avec p, q dans A. C'est une factorisation dans A[X] donc p ou q inversible dans A[X] et donc dans A d'après la remarque 50. Ainsi a est irréductible dans A.

Si $a \in \mathrm{A}$ irréductible dans A. On écrit $a = \mathrm{PQ}$. Comme A est intègre, on a $\deg \mathrm{P} = \deg \mathrm{Q} = 0$ et c'est une factorisation dans A et donc P ou Q inversible dans A et donc dans A[X].

Soit $\mathrm{P} \in \mathrm{A}[\mathrm{X}]$ non constant et irréductible dans A[X]. Alors P est primitif. En effet, sinon $\mathrm{P} = c(\mathrm{P})\mathrm{Q}$ est une factorisation dans A[X] avec $c(\mathrm{P})$ non inversible et Q non inversible.

Soit $\mathrm{P} \in \mathrm{A}[\mathrm{X}]$ non constant primitif et irréductible dans K[X]. Montrons que P est irréductible dans A[X]. Si $\mathrm{P} = \mathrm{QR}$ avec $\mathrm{Q}, \mathrm{R} \in \mathrm{A}[\mathrm{X}]$. alors $\mathrm{Q}, \mathrm{R} \in \mathrm{K}[\mathrm{X}]$ et donc Q ou R sont dans K (inversible de K[X]). Donc Q ou R est dans A. Si $\mathrm{R} = a \in \mathrm{A}$ alors $\mathrm{P} = a\mathrm{Q}$ et $a \mid c(\mathrm{P}) = 1$ et donc a inversible dans A. De même si $\mathrm{Q} \in \mathrm{A}$, on obtient que Q est inversible dans A.

Enfin si $\mathrm{P} \in \mathrm{A}[\mathrm{X}]$ irréductible dans A[X] alors, on a vu que P est primitif. Montrons qu'il est irréductible dans K[X]. Si $\mathrm{P} = \mathrm{QR}$ avec $\mathrm{Q}, \mathrm{R} \in \mathrm{K}[\mathrm{X}]$. On écrit $\mathrm{P} = c(\mathrm{Q})c(\mathrm{R})\widetilde{\mathrm{Q}}\widetilde{\mathrm{R}}$ avec $\widetilde{\mathrm{Q}}$ et $wt\mathrm{R}$ primitifs. On a $c(\mathrm{Q})c(\mathrm{R}) = c(\mathrm{P}) = 1$. Ainsi $\mathrm{P} = \widetilde{\mathrm{Q}}\widetilde{\mathrm{R}}$ est une factorisation dans A[X]. Donc $\widetilde{\mathrm{Q}}$ ou $\widetilde{\mathrm{R}}$ inversible dans A. Donc Q ou R inversible dans K[X].

Proposition 52 — Factorialité d'un anneau de polynômes. Si A est factoriel, A[X] est factoriel.

Preuve. Comme A est intègre puisque factoriel, A[X] est intègre.

existence de la décomposition. Soit $\mathrm{P} = c(\mathrm{P})\widetilde{\mathrm{P}}$. On factorise $c(\mathrm{P})$ dans A en irréductible dans A qui sont aussi des irréductibles dans A[X]. On factorise $\widetilde{\mathrm{P}}$ en irréductible dans K[X] : on écrit $\widetilde{\mathrm{P}} = \mathrm{Q}_1 \cdots \mathrm{Q}_n$ avec Q_i irréductible dans K[X]. On écrit ensuite $\mathrm{Q}_i = c(\mathrm{Q}_i)\widetilde{\mathrm{Q}_i}$ avec $\widetilde{\mathrm{Q}_i} \in \mathrm{A}[\mathrm{X}]$ primitif et irréductible dans K[X] et donc irréductible dans A[X]. Ainsi, on a $\widetilde{\mathrm{P}} = \widetilde{\mathrm{Q}_1} \cdots \widetilde{\mathrm{Q}_n}$ puisque $c(\widetilde{\mathrm{P}}) = c(\mathrm{Q}_1) \cdots c(\mathrm{Q}_n) = 1$. On obtient ainsi l'existence pour P d'une décomposition en irréductible dans A[X].

unicité de la décomposition. Si $u_1 \cdots u_m \mathrm{P}_1 \cdots \mathrm{P}_{m'} = v_1 \cdots v_n \mathrm{Q}_1 \cdots \mathrm{Q}_{n'}$. sont deux décompositions en irréductibles de A[X] avec $u_i, v_i \in \mathrm{A}$ et $\deg \mathrm{P}_i, \deg \mathrm{Q}_i > 0$. Comme les P_i et les Q_i sont primitifs, on obtient en prenant le contenu que $u_1 \cdots u_m = v_1 \cdots v_n$ qui sont des décompositions en irréductible dans A. On a ainsi l'unicité. De plus, on peut simplifier la premier relation par intégrité pour obtenir $\mathrm{P}_1 \cdots \mathrm{P}_{m'} = \mathrm{Q}_1 \cdots \mathrm{Q}_{n'}$ qui est une décomposition en irréductible dans K[X] qui est factoriel car principal. Ainsi, on a bien l'unicité souhaité.

Exercice 18 Soit A un anneau tel que A[X] est factoriel. Montrer que A est factoriel.

Exercice 19 Soit $\mathrm{P} \in \mathbb{Z}[\mathrm{X}]$ unitaire et $\mathrm{P} = \mathrm{QR}$ avec $\mathrm{Q}, \mathrm{R} \in \mathbb{Q}[\mathrm{X}]$ unitaire. Montrer que $\mathrm{Q}, \mathrm{R} \in \mathbb{Z}[\mathrm{X}]$.

2 Théorie des corps

2.1 Constructibilité

Définition 53 — Corps. Soit $(\mathrm{A}, +, \times)$ un anneau commutatif unitaire. On dit que A est corps si $\mathrm{A} \neq \{0\}$ et tout élément non nul de A est inversible ou encore si $\mathrm{A}^\times = \mathrm{A} \setminus \{0\}$.

Exemples 54 — Les exemples classiques.

Le problème de la constructibilité à la règle et au compas.

Définition 55 — Constructibilité en un pas. Soit $\mathscr{P}$ un plan euclidien et X un sous-ensemble de $\mathscr{P}$. On dit que $\mathrm{M} \in \mathscr{P}$ est *constructible* (à la règle et au compas) *en un pas* à partir de X, si M est obtenu à partir de l'une des constructions suivantes

(*i*) M est l'intersection de deux droites non parallèles (AB) et (A′B′) où $\mathrm{A}, \mathrm{B}, \mathrm{A}', \mathrm{B}' \in \mathrm{X}$ et $\mathrm{A} \neq \mathrm{B}$ et $\mathrm{A}' \neq \mathrm{B}'$.

(*ii*) M est l'intersection du cercle de centre A et de rayon AB et de la droite (A′B′) où $\mathrm{A}, \mathrm{B}, \mathrm{A}', \mathrm{B}' \in \mathrm{X}$ et $\mathrm{A}' \neq \mathrm{B}'$

(*iii*) M est l'intersection du cercle de centre A et de rayon AB avec le cercle de centre A′ et de rayon A′B′.

Exercice 20 Si X est réduit à un élément, déterminer les points constructibles en un pas à partir de X.

Montrer que tout point de X est constructible en un pas à partir de X. (Ouf !)

À partir de maintenant, on suppose $|\mathrm{X}| \geqslant 2$.

Définition 56 — Constructibilité en n pas. Soit $\mathscr{P}$ un plan euclidien et X un sous-ensemble de $\mathscr{P}$. On dit que $\mathrm{M} \in \mathscr{P}$ est *constructible* (à la règle et au compas) *en n pas* à partir de X, s'il existe une suite $\mathrm{M}_1, \ldots, \mathrm{M}_{n-1}, \mathrm{M}_n$ d'éléments de $\mathscr{P}$ tels que, pour tout i, M_i est constructible en un pas à partir de $\mathrm{X} \cup \{\mathrm{M}_1, \ldots, \mathrm{M}_{i-1}\}$

Remarque 57 Pour tout i, le point M_i de la définition précédente est évidemment constructible en i pas.

Définition 58 — Constructibilité. Soit $\mathscr{P}$ un plan euclidien et X un sous-ensemble de $\mathscr{P}$. On dit que $\mathrm{M} \in \mathscr{P}$ est *constructible* (à la règle et au compas) à partir de X s'il existe un entier $n \geqslant 1$ tel que M est constructible en n pas à partir de X.

Définition 59 — Nombre constructible. Soit $\mathbb{C}$ muni de sa structure d'espace euclidien. Un élément $z \in \mathbb{C}$ est dit constructible si le point M d'affixe z est constructible à partir de $\mathrm{X} = \{\mathrm{O}, \mathrm{I}\}$ où O est le point d'affixe 0 et I le point d'affixe 1.

On note $\mathrm{A} = \{z \in \mathbb{C}, z \text{ est constructible}\}$.

Théorème 60 A est un corps.

La démonstration se décompose en une suite de lemmes élémentaires. À partir de maintenant, on suppose $\mathrm{X} = \mathrm{O}, \mathrm{I}$ et la constructibilité se rapporte à cette partie.

Lemme 61 Si $z \in \mathbb{C}$ est constructible alors $-z$ l'est aussi.

Preuve. $-z$ est l'intersection du cercle de centre O passant par z et de la droite $(\mathrm{O}z)$.

Définition 62 Une droite est dite constructible s'il existe $\mathrm{A} \neq \mathrm{B}$ sur cette droite qui sont constructibles.

Lemme 63 Si d est une droite constructible et A un point constructible. Alors la perpendiculaire et la parallèle à d passant par A sont constructibles.

Preuve. *Perpendiculaire à d passant par* A. L'idée est de construire deux points M, N sur d tel que la médiatrice du segment [MN] passe par A. Soient $\mathrm{B} \neq \mathrm{C}$ deux points constructibles de d. On a $\mathrm{A} \neq \mathrm{B}$ ou $\mathrm{A} \neq \mathrm{C}$. Supposons $\mathrm{A} \neq \mathrm{B}$. On trace alors le cercle $\mathscr{C}$ de centre A de rayon [AB]. Il rencontre d en un autre point E (sauf si le cercle est tangent à d auquel cas la droite cherchée est (AB)). On trace

ensuite la médiatrice de [BE] de la façon suivante : on trace ensuite le cercle de centre B de rayon BE et le cercle de centre E et de rayon BE qui se rencontrent en deux points. La droite passant par ces deux points est la droite cherchée.

Parallèle à d passant par A. On trace la perpendiculaire d' à d passant par A puis la perpendiculaire à d' passant par A : c'est la droite cherchée.

Corollaire 64 Si $z, z' \in \mathbb{C}$ sont constructibles alors $z + z'$ est constructible.

Preuve. On suppose que O, z, z' ne sont pas alignés. Le point d'affixe $z + z'$ est à l'intersection de la parallèle à $(\mathrm{O}z)$ passant par z' et de la parallèle à $(\mathrm{O}z')$ passant z. Le lemme 63 permet de conclure.

Avec le lemme 61, on en déduit que A est un sous-groupe additif de $\mathbb{C}$.

Lemme 65 Soit $z = x + iy$ avec $x, y \in \mathbb{R}$. Alors z est constructible si et seulement si y et x le sont.
En particulier, $y \in \mathbb{R}$ est constructible si et seulement si iy l'est.

Preuve. Si z est constructible. On trace la perpendiculaire à la droite (OI) passant par z. L'intersection avec la droite (OI) donne x.

La perpendiculaire à la droite (OI) passant par O est constructible. L'intersection de la parallèle à (OI) passant par z avec cette droite est iy qui est donc constructible.

Enfin l'intersection du cercle de centre O passant par iy avec la droite (OI) est y qui est donc constructible. En particulier, si iy est constructible alors y l'est.

Inversement, supposons x et y constructibles. Alors iy est constructible : c'est l'intersection du cercle de centre O passant par y avec l'axe (OI) et avec le corollaire 64 on obtient que z est constructible.

Lemme 66 Si $z, z' \in \mathbb{C}$ est constructible alors zz' l'est.

Preuve. On écrit $z = x + iy$ et $z' = x' + iy'$. On a alors $zz' = (xx' - yy') + i(xy' + yx')$. Si on montre que le produit de deux nombres réels constructibles est constructible, alors on pourra conclure. En effet, x, y, x', y' sont constructibles d'après le lemme 65 et, $xx' - yy'$ et $xy' + yx'$ seront alors constructibles puisqu'un produit de nombres réels constructibles l'est et que la somme l'est aussi d'après le corollaire 64.

Pour démontrer que le produit de deux nombres réels constructibles est constructibles, il suffit de le faire pour deux nombres réels positifs. En effet, si les deux sont négatifs alors $xy = (-x)(-y)$ avec $-x \geqslant 0$ et $-y \geqslant 0$ qui sont constructibles d'après le lemme 61. Si $x \leqslant 0$ et $y \geqslant 0$ alors $xy = -((-x)y)$ avec $-x \geqslant 0$ et $y \geqslant 0$ constructibles. On en déduit que $(-x)y$ constructible et son opposé l'est aussi.

Finalement, on considère x et y réels positifs et constructibles. On trace le point P d'affixe iy intersection du cercle de centre O passant par y avec la perpendiculaire à (OI) passant par O. On trace la parallèle à (IP) passant par x. Elle coupe la perpendiculaire à (OI) passant par O au point d'affixe ixy (théorème de Thalès). On en déduit que ixy est constructible et donc xy aussi.

Lemme 67 Si $z \neq 0$ est constructible alors $1/z$ l'est.

Preuve. On a $1/z = \overline{z}/|z|^2$. Or $\overline{z} = z - iy - iy$ est constructible d'après le lemme 65 et le corollaire 64.

Par ailleurs, $|z|$ est constructible puisque c'est l'intersection du cercle de centre O de rayon $\mathrm{O}z$ avec l'axe (OI). Le lemme 66 assure que $|z|^2$ est constructible.

Ainsi, si on montre que si x est un réel positif constructible alors $1/x$ est constructible alors on pourra conclure grâce au lemme 66 puisque $\overline{z}$ et $1/|z|^2$ seront constructibles.

Soit J l'intersection de la perpendiculaire à (OI) passant par O avec le cercle de centre O passant par I. On trace alors la parallèle à $(x\mathrm{J})$ passant par I. L'intersection de cette droite avec de la perpendiculaire à (OI) passant par O est le point d'axe i/x. Ainsi $1/x$ est bien constructible.

2.2 Propriétés des corps

SOUS-CORPS

Définition 68 Soient K un corps. On dit que $k \subset \mathrm{K}$ est un sous-corps de K si

(i) Pour tout $x, y \in k$, $x + y \in k$.
(ii) Pour tout $x, y \in k$, $xy \in k$.
(iii) Pour tout $x \in k$, $x^{-1} \in k$
(iv) $-1 \in k$.

Lorsque k est un sous-corps de K, les lois $+$ et $\times$ de K induisent des lois sur k qui sont de k un corps.

Exercice 21 Soient K un corps. Montrer que $k \subset \mathrm{K}$ est un sous-corps de K si et seulement si

(i) Pour tout $x, y \in k$, $x - y \in k$.
(ii) Pour tout $x, y \in k$, $xy \in k$.
(iii) Pour tout $x \in k$, $x^{-1} \in k$.
(iv) $1 \in k$.

Idéaux d'un corps

Proposition 69 Soit K un corps. Alors K a exactement deux idéaux qui sont $\{0\}$ et K.

Preuve. Comme $\mathrm{K} \neq \{0\}$. On a bien au moins deux idéaux. Soit I un idéal non nul et $x \in \mathrm{I}$, on a $1 = x^{-1}x \in \mathrm{I}$ grâce à la propriété d'idéal et donc pour $y \in \mathrm{K}$, $y = y1 \in \mathrm{I}$ et $\mathrm{I} = \mathrm{K}$.

Exercice 22 Soit A un anneau commutatif unitaire qui a exactement deux idéaux. Montrer que A est un corps.

On suppose que A n'est pas nécessairement commutatif. Montrer que si A n'a que deux idéaux à gauche alors A est un anneau à division c'est-à-dire $\mathrm{A} \neq \{0\}$ et tout élément non nul est inversible.

Montrer que ce n'est pas le cas si on remplace idéal à gauche par idéal bilatère (penser à $\mathrm{M}_n(k)$).

CORPS ENGENDRÉ

Lemme 70 Soit K un corps et $(\mathrm{K}_i)_{i\in\mathrm{I}}$ une famille de sous-corps de K. Alors

$$\bigcap_{i\in\mathrm{I}} \mathrm{K}_i$$

est un sous-corps de K.

Proposition 71 – Corps engendré. Soit K un corps et S une partie de K, il existe un plus petit sous-corps $\langle \mathrm{S} \rangle_{\text{corps}}$ de K contenant S. C'est l'intersection de tous les sous-corps de K qui contiennent S.

Exercice 23 Décrire la forme des éléments de $\langle \mathrm{S} \rangle_{\text{corps}}$.

Application 72 Soit K un corps. Il existe un plus petit sous-corps de K : c'est $\langle \varnothing \rangle$. On l'appelle le sous-corps premier de K.

CARACTÉRISTIQUE D'UN CORPS

Morphismes qui partent de $\mathbb{Z}$

Proposition 73 Soit A un anneau commutatif **unitaire**. Il existe un unique morphisme d'anneaux unitaires de $\mathbb{Z} \to \mathrm{A}$. Il est donné par

$$\iota_{\mathrm{A}} : \begin{cases} \mathbb{Z} \longrightarrow \mathrm{A} \\ n \longmapsto n1_{\mathrm{A}} \end{cases}$$

Preuve. *Rappel :* si M est un groupe abélien noté additivement et $x \in \mathrm{M}$ alors pour $n \in \mathbb{N}$, nx est défini récursivement par $0x = 0$ et $(n+1)x = nx + x$. Pour $n \in \mathbb{Z}$ et $n < 0$, on pose $nx = (-n)(-x)$ qui a bien un sens puisque $-n > 0$.

L'application $m \mapsto mx$ est alors un morphisme de groupes de $\mathbb{Z} \to \mathrm{M}$. En effet, vérifions que $(m+n)x = mx + nx$ pour tous $n, m \in \mathbb{Z}$.

On suppose d'abord $n, m \in \mathbb{N}$. On va montrer que par récurrence sur m que le résultat est vrai. Il est évidemment vrai pour $m = 0$ (et $m = 1$). On le suppose vrai pour m. On a alors

$$(m+n+1)x = (m+n)x + x = mx + nx + x = nx + (m+1)x$$

La première égalité résulte de la définition de $(m+n+1)x$, la deuxième égalité résulte de l'hypothèse de récurrence, la troisième égalité résulte de la définition de $(m+1)x$.

Si $n < 0$ et $m < 0$, on a alors

$$(n+m)x = (-n-m)(-x) = -n(-x) + -m(-x) = nx + mx$$

La première égalité résulte de la définition de $(m+n)x$ puisque $m+n<0$, la deuxième égalité résulte du cas $n \geqslant 0, m \geqslant 0$, la troisième égalité est la définition de mx et nx pour $n, m \geqslant 0$.

Avant de passer au cas où m et n sont de signe contraire, montrons par récurrence sur n, que pour $x, y \in \mathrm{M}$ et $n \in \mathbb{N}$, on a $n(x+y) = nx + ny$. Pour $n = 0$, c'est la définition. On suppose que c'est vrai pour n. On a alors

$$(n+1)(x+y) = n(x+y) + x + y = nx + ny + x + y$$

La première égalité est la définition de $(n+1)(x+y)$, la deuxième est l'hypothèse de récurrence et la troisième est la définition de $(n+1)x$ et $(n+1)y$.

Si $n<0$ et $m>0$. On suppose $m+n \geqslant 0$, on a alors $m \geqslant -n$ et donc $m = -n+u$ avec $u \geqslant 0$. Ainsi $(m+n)x = ux$ et $mx + nx = (-n)x + ux + nx$ (d'après le cas $n \geqslant 0, m \geqslant 0$).

Or $-n > 0$ et donc $-nx + nx = -nx + (-n)(-x) = -n(x + (-x)) = -n0 = 0$ (la dernière égalité résultant d'une récurrence triviale). Ainsi $mx + nx = ux$ et on a l'égalité souhaitée.

Si $n<0$ et $m>0$ avec $m+n<0$, on a alors $(m+n)x = (-m-n)(-x)$ avec $-m-n>0$ et $-m<0$ et $-n>0$, le cas précédent montre que $(-m-n)(-x) = (-m)(-x) + (-n)(-x) = nx + mx$.

Si un tel morphisme d'anneaux existe, on a nécessairement $\iota_{\mathrm{A}}(1) = 1_{\mathrm{A}}$. Et donc, par récurrence sur n, $\iota_{\mathrm{A}}(n) = n1_{\mathrm{A}}$ pour $n \in \mathbb{N}$ et $\iota_{\mathrm{A}}(n) = n1_{\mathrm{A}}$. Par passage à l'opposé, on a $\iota_{\mathrm{A}}(n) = n1_{\mathrm{A}}$ pour $n \in \mathbb{Z}$.

Pour conclure, il suffit donc de montrer que $mn1_{\mathrm{A}} = m1_{\mathrm{A}} \times n1_{\mathrm{A}}$ pour tous $n, m \in \mathbb{Z}$ ce qui se démontre par récurrence sur m si $m \in \mathbb{N}$ et par passage à l'opposé lorsque m est négatif.

Caractéristique d'un anneau.

Définition 74 Soit A un anneau commutatif unitaire. Le noyau de ι_{A} est un idéal de $\mathbb{Z}$. Il est donc de la forme $n\mathbb{Z}$ pour un unique $n \in \mathbb{N}$. Cet entier n est la **caractéristique de** A et on la note $\operatorname{car} \mathrm{A}$.

Proposition 75 Soit A un anneau de caractéristique n. On a $nx = 0$ pour tout $x \in \mathrm{A}$.

Preuve. On a $nx = n1_{\mathrm{A}} \times x = 0$.

Caractéristique et intégrité.

Proposition 76 Soit A un anneau **intègre** alors $\operatorname{car} \mathrm{A} = 0$ ou $\operatorname{car} \mathrm{A}$ est un nombre premier.

Preuve. Version 1. Supposons $\operatorname{car} \mathrm{A} = n \neq 0$ et montrons que n est premier. Sinon, il existe $n_1, n_2 \in \mathbb{N}$ avec $n_1 \neq 1$ et $n_2 \neq 1$ tel que $n = n_1 n_2$. On a alors $0 < n_1 < n$ et par définition de n, $n_1 1_{\mathrm{A}} \neq 0$. De même $n_2 1_{\mathrm{A}} \neq 0$ et donc $n_1 1_{\mathrm{A}} \times n_2 1_{\mathrm{A}} = n1_{\mathrm{A}} \neq 0$ puisque A est intègre. Mais $n1_{\mathrm{A}} = 0$ par définition de la caractéristique.

Version 2. Comme $n\mathbb{Z}$ est le noyau de $\iota_{\mathrm{A}} : \mathbb{Z} \to \mathrm{A}$, on en déduit, par passage au quotient un morphisme **injectif** d'anneaux $\mathbb{Z}/n\mathbb{Z} \to \mathrm{A}$. Ainsi $\mathbb{Z}/n\mathbb{Z}$ s'identifie à un sous-anneau d'un anneau intègre et en donc intègre c'est-à-dire que l'idéal $n\mathbb{Z}$ est un idéal premier de $\mathbb{Z}$ c'est-à-dire $n = 0$ ou n est un nombre premier.

Exercice 24 Pour tout $n \in \mathbb{N}$. Déterminer un anneau de caractéristique n.

Morphisme de corps.

Définition 77 Soient K et K′ deux corps. Un morphisme de corps de K dans K′ est un morphisme d'anneaux unitaires de K dans K′ c'est-à-dire une application $f : \mathrm{K} \to \mathrm{K}'$ vérifiant

(*i*) $f(x+y) = f(x) + f(y)$ pour tous $x, y \in \mathrm{K}$.
(*ii*) $f(xy) = f(x)f(y)$ pour tous $x, y \in \mathrm{K}$.
(*iii*) $f(1) = 1$

Un morphisme de corps est forcément injectif puisque le noyau est un idéal de K différent de K (puisque $1 \notin \operatorname{Ker} f$) et qu'un corps n'a que deux idéaux $\{0\}$ et K.

Lemme 78 Soient K, K' deux corps. Si $f, f' : \mathrm{K} \to \mathrm{K}'$ sont deux morphismes de corps alors l'ensemble des $\{x \in \mathrm{K},\ f(x) = f'(x)\}$ est un sous-corps de K. En particulier, si deux morphismes de corps coïncident sur une partie génératrice de K, ils sont égaux.

Preuve. On a $f(1) = 1 = f'(1)$. Si $x, y \in \mathrm{K}$ vérifient $f(x) = f'(x)$ et $f(y) = f'(y)$ alors $f(xy) = f(x)f(y) = f'(x)f'(y) = f'(xy)$ et $f(x-y) = f(x) - f(y) = f'(x) - f'(y) = f'(x-y)$.

Caractéristique d'un corps.

Corollaire 79 Soit K un corps. Alors $\operatorname{car} \mathrm{K} = 0$ ou est un nombre premier.

Si $\operatorname{car} \mathrm{K} = 0$ alors il existe un unique morphisme de corps de $\mathbb{Q}$ dans K. L'image de ce morphisme est le sous-corps premier de K qui est isomorphe à $\mathbb{Q}$

Si $\operatorname{car} \mathrm{K} = p$ alors il existe un unique morphisme de corps de $\mathbb{F}_p := \mathbb{Z}/p\mathbb{Z}$ dans K. L'image de ce morphisme est le sous-corps premier de K qui est isomorphe à $\mathbb{Z}/p\mathbb{Z}$.

Preuve. Un corps est un anneau intègre donc sa caractéristique est 0 ou un nombre premier.

Plaçons-nous dans le premier cas $\operatorname{car} \mathrm{K} = 0$.

On a alors $\iota_{\mathrm{K}} : \mathbb{Z} \to \mathrm{K}$ qui est injectif. Or par la propriété de définition du corps de fraction, il existe $j : \mathbb{Q} \to \mathrm{K}$ tel que $j \circ \iota_{\mathbb{Q}} = \iota_{\mathrm{K}}$ (où $\iota_{\mathbb{Q}}$ est l'unique morphisme d'anneau de $\mathbb{Z}$ dans $\mathbb{Q}$ et donc aussi le morphisme naturel de $\mathbb{Z}$ dans son corps de fraction).

De plus, si $j' : \mathbb{Q} \to \mathrm{K}$ est un autre morphisme alors $j' \circ \iota_{\mathbb{Q}} : \mathbb{Z} \to \mathrm{K}$. Par unicité du morphisme de $\mathbb{Z}$ dans A, on a $j' \circ \iota_{\mathbb{Q}} = \iota_{\mathrm{K}}$. Or toujours par définition/construction du corps de fraction, le morphisme de corps φ tel que $\varphi \circ \iota_{\mathbb{Q}} = \iota_{\mathrm{K}}$ est unique et donc $j' = j$.

Le morphisme j est défini par $j(p/q) = (p1_{\mathrm{K}})(q1_{\mathrm{K}})^{-1}$. Par **abus de notation**, on le note $p/q1_{\mathrm{K}}$. L'image de j est un sous-corps de K (exercice : l'image d'un corps par un morphisme de corps est un sous-corps). donc contient le sous-corps premier. Mais le sous-corps premier contient 1 et donc $p1_{\mathrm{A}}$ pour tout $p \in \mathbb{N}$ (par récurrence) puis $p \in \mathbb{Z}$ (en passant à l'opposé) et enfin les $(p1_{\mathrm{K}})^{-1}$ (par passage à l'inverse) et donc toute l'image de j.

Plaçons-nous dans le premier cas $\operatorname{car} \mathrm{K} = p$.

En passant ι_{K} au quotient par $p\mathbb{Z}$ qui est son noyau, on obtient un morphisme injectif j de $\mathbb{F}_p$ dans K (vérifiant $\iota_{\mathrm{K}} = j \circ \pi$ où $\pi : \mathbb{Z} \to \mathbb{F}_p$ est la surjection canonique).

Si $j' : \mathbb{F}_p \to \mathrm{K}$ est un morphisme de corps alors $j' \circ \pi = \iota_{\mathrm{K}}$ par unicité du morphisme de $\mathbb{Z}$ dans K. Par unicité du morphisme obtenu par passage au quotient, on obtient $j' = j$.

Le morphisme j est défini par $j(\overline{n}) = n1_{\mathrm{K}}$. Son image est un sous-corps de K qui contient donc le sous-corps premier. Par ailleurs, le sous-corps premier contient évidemment les $n1_{\mathrm{K}}$ pour $n \in \{0, \ldots, p-1)$ qui est l'image de j.

Exercice 25

a) Soit $\mathrm{A}, \mathrm{B}, \mathrm{C}$ trois anneaux commutatifs unitaires et $f : \mathrm{A} \to \mathrm{B}$, $g : \mathrm{B} \to \mathrm{C}$ et $h : \mathrm{A} \to \mathrm{C}$ trois morphismes d'anneaux vérifiant $gf = h$. Déterminer une relation en $\operatorname{Ker} f$ et $\operatorname{Ker} h$.

b) Soient A, B deux anneaux commutatifs unitaires. Déterminer une condition nécessaire portant sur les caractéristiques de A et B pour qu'il existe un morphisme d'anneaux de A dans B.

c) En déduire pour tous $n, m \in \mathbb{N}$, le nombre et la forme des morphisme d'anneaux de $\mathbb{Z}/m\mathbb{Z}$ dans $\mathbb{Z}/n\mathbb{Z}$.

d) Déduire aussi de la question 2, que si deux corps ont des caractéristiques différentes, il n'existe pas de morphisme de corps entre les deux.

Le Frobenius

Proposition 80 Soit A un anneau commutatif unitaire avec $\operatorname{car} \mathrm{A} = p$ un nombre premier. L'application

$$\mathrm{F} : \begin{cases} \mathrm{A} \longrightarrow \mathrm{A} \\ x \longmapsto x^p \end{cases}$$

est un endomorphisme d'anneau.

Preuve. On a évidemment $\mathrm{F}(xy) = \mathrm{F}(x)\mathrm{F}(y)$ pour tous $x, y \in \mathrm{A}$ (car A est commutatif) et $\mathrm{F}(1) = 1$. Il s'agit donc de montrer que $\mathrm{F}(x+y) = \mathrm{F}(x) + \mathrm{F}(y)$ pour tous $x, y \in \mathrm{A}$. Comme x et y commutent, la formule du binôme de Newton donne

$$(x+y)^p = \sum_{i=0}^{p} \binom{p}{i} x^i y^{p-i} = x^p + y^p + \sum_{i=1}^{p-1} \binom{p}{i} 1_{\mathrm{A}} \times x^i y^{p-i}$$

Il suffit donc de montrer que, pour $1 \leqslant i \leqslant p-1$, on a $p \mid \binom{p}{i}$ puisqu'alors $\binom{p}{i} 1_{\mathrm{A}} = 0$.

Or on a $i!\binom{p}{i} = p(p-1)\cdots(p-i+1)$. Comme $i > 0$, on en déduit que $p \mid i!\binom{p}{i}$ (le produit $p(p-1)\cdots(p-i+1)$ a au moins un facteur qui est p). De plus, comme $i < p$, p est premier avec $i!$ et donc $p \mid \binom{p}{i}$.

Remarque 81 Si A ne contient pas d'élément nilpotent alors F est injectif. C'est en particulier le cas si A est intègre ou un corps.

2.3 k-algèbres

Deux points de vue identiques

k-algèbre : point de vue 1

Définition 82 Soit k un corps. Une k-algèbre (associative unitaire) A est un anneau (unitaire) qui est en même temps un k-espace vectoriel avec les relations de compatibilité

(i) La loi + de la structure d'anneau et la loi + de la structure d'espace vectoriel coïncident.
(ii) La multiplication dans A est k-bilinéaire : pour tous $a, a' \in \mathrm{A}$ et tous $\lambda \in \mathrm{A}$, on a

$$(\lambda a) \times a' = \lambda(a \times a') = a \times \lambda a'$$

Définition 83 — Morphisme de k-algèbres. Soient A et B deux k-algèbres. Un morphisme de k-algèbres est une application $f : \mathrm{A} \to \mathrm{B}$ qui est en même temps k-linéaire et un morphisme d'anneaux.

k-algèbre : point de vue 2

Définition 84 — k-algèbre. Soit k un corps. Une k-algèbre est un couple (A, ρ) où A est un anneau unitaire et $\rho : k \to \mathrm{A}$ un morphisme d'anneaux unitaires

Définition 85 Soient k un corps et $(\mathrm{A}, \rho_\mathrm{A})$, $(\mathrm{B}, \rho_\mathrm{B})$ deux k-algèbres. Un morphisme de k-algèbres de A dans B est un morphisme d'anneau $f : \mathrm{A} \to \mathrm{B}$ tel que $f \circ \rho_\mathrm{A} = \rho_\mathrm{B}$.

Concordance des points de vue

Proposition 86 Les deux définitions d'algèbres coïncident. De façon précise, si A est une k-algèbre au sens 1, on définit $\rho_\mathrm{A} : k \to \mathrm{A}$ par $\rho_\mathrm{A}(\lambda) = \lambda \cdot 1_\mathrm{A}$ pour tout $\lambda \in k$ (où $\cdot$ est donné par la structure de k-espace vectoriel).

Inversement si (A, ρ) est une k-algèbre au sens 2, on définit la structure de k-espace vectoriel sur A par $\lambda \cdot a := \rho(\lambda) \times a$

Preuve. Il s'agit de montrer que ρ_A est un morphisme d'anneaux. Par définition, on a $\rho_\mathrm{A}(\lambda + \mu) = (\lambda + \mu) \cdot 1_\mathrm{A}$. Les axiomes des espaces vectoriel assurent que

$$\rho_\mathrm{A}(\lambda + \mu) = (\lambda + \mu) \cdot 1_\mathrm{A} = \lambda \cdot 1_\mathrm{A} + \mu \cdot 1_\mathrm{A} = \rho_\mathrm{A}(\lambda) + \rho_\mathrm{A}(\mu).$$

Toujours grâce au axiomes d'espaces vectoriels, on a $\rho_\mathrm{A}(1) = 1 \cdot 1_\mathrm{A} = 1_\mathrm{A}$. Il reste à montrer que $\rho_\mathrm{A}(\lambda\mu) = \rho_\mathrm{A}(\lambda)\rho_\mathrm{A}(\mu)$. Mais $\rho_\mathrm{A}(\lambda\mu) = \lambda\mu \cdot 1_\mathrm{A}$ et $\rho_\mathrm{A}(\lambda)\rho_\mathrm{A}(\mu) = (\lambda \cdot 1_\mathrm{A}) \times (\mu 1_\mathrm{A})$. L'égalité entre les deux quantités résulte alors de bilinéarité.

L'axiome sur l'égalité entre les deux lois + n'est pas apparu. L'a-t-on utilisé ? Où ?

Inversement, par définition, la loi + pour la structure d'espace vectoriel est la même que celle de A. Il s'agit ensuite de vérifier les axiomes des espaces vectoriels puis de vérifier la bilinéarité.

Pour finir il s'agit de vérifier que si on part d'une algèbre avec le point de vue 1 qu'on passe au point de vue 2 et qu'on revient au point de vue 1, on n'a rien changé et idem dans l'autre sens.

Proposition 87 Les notions de morphismes d'algèbres dans les deux points de vue sont les mêmes.

Preuve. Soit $f : \mathrm{A} \to \mathrm{B}$ un morphisme d'algèbres pour le premier point de vue. Pour $\lambda \in k$, on a $f(\lambda 1_\mathrm{A}) = \lambda f(1_\mathrm{A}) = \lambda 1_\mathrm{B}$ ce qui assure que $f \circ \rho_\mathrm{A} = \rho_\mathrm{B}$.

Si f est un morphisme d'algèbre pour le deuxième point de vue. Il s'agit de montrer que f est k-linéaire. Pour $\lambda \in k$ et $a \in \mathrm{A}$, on a

$$f(\lambda a) = f(\lambda 1_{\mathrm{A}} \times a) = f(\lambda 1_{\mathrm{A}}) f(a) = \lambda 1_{\mathrm{B}} f(a) = \lambda f(a)\,;$$

l'avant dernière égalité résultant du fait que $f \circ \rho_{\mathrm{A}} = \rho_{\mathrm{B}}$.

SOUS-ALGÈBRES.

Exercice 26 — Sous-algèbre. Soit A une k-algèbre.

a) Définir une notion de sous-k-algèbre.

b) Montrer qu'une intersection de sous-algèbres est une sous-algèbre.

c) En déduire une notion de sous-algèbre engendrée.

d) Lorsque A est une k-algèbre commutative (c'est-à-dire que A est un anneau commutatif) et S une partie de A, déterminer la forme générale est des éléments de $k[\mathrm{S}]$ la sous-algèbre de A engendrée par S.

e) Montrer qu'il existe sur k une unique structure de k-algèbre sur k Déterminer le morphisme $\rho_k : k \to k$ associé.

f) Déterminer les morphismes de k-algèbres de k dans A.

g) Montrer que $\{0\}$ est une k-algèbre et déterminer les morphismes d'algèbres de A dans $\{0\}$. Existe-t-il des morphismes de k-algèbres de $\{0\}$ dans A ?

h) Montrer que $k[\mathrm{X}]$ est une k-algèbre. Déterminer les morphismes de k-algèbres de $k[\mathrm{X}]$ dans A.

2.4 Extensions de corps

DÉFINITION

Définition 88 — Extension de corps. Soit k un corps. Une **extension de** k est une k-algèbre (K, i) où K est un corps c'est-à-dire un couple où K est un corps et $i : k \to \mathrm{K}$ un morphisme d'anneaux unitaires.

Exemples 89 $\mathbb{C}$ (ou plutôt $(\mathbb{C}, i)$ avec $i : x \in \mathbb{R} \mapsto x1_{\mathbb{C}} \in \mathbb{C}$) est une extension de corps de $\mathbb{R}$.
$\mathbb{R}(\mathrm{T})$ est une extension de $\mathbb{R}$.
A (le corps des nombres constructibles) est une extension de $\mathbb{Q}$.

Remarque 90 Le morphisme i est injectif et permet d'identifier k au sous-corps $i(k)$ de K (attention, ce n'est pas toujours très malin !).

On peut munir K d'une structure de k-espace vectoriel. Comment ? La dimension de K sur k est notée $[\mathrm{K} : k]$. D'une manière générale, dans ce cours, si E est un k-espace vectoriel, on note

$$[\mathbf{E} : \mathbf{k}] = \dim_{\mathbf{k}} \mathbf{E}$$

.

MORPHISME D'EXTENSIONS

Définition 91 — Morphisme d'extensions. Soient (K, i) et (L, j) deux extensions de k. Un *morphisme d'extensions de* k de (K, i) dans (L, j) est un morphisme de k-algèbres c'est-à-dire un morphisme d'anneaux $f : \mathrm{K} \to \mathrm{L}$ vérifiant $f \circ i = j$. Le diagramme suivant est commutatif

$$\begin{tikzcd} \mathrm{K} \arrow[rr, "f"] & & \mathrm{L} \\ & k \arrow[ul, "i"] \arrow[ur, "j"'] & \end{tikzcd}$$

Exercice 27 Soit (K, i) une extension de k. Vérifier que id_{K} est un morphisme d'extensions de K dans lui-même.

Vérifier que la composée de deux morphismes d'extensions est un morphisme d'extensions.

Définir la notion de isomorphisme d'extensions puis montrer qu'un morphisme d'extension est un isomorphisme si et seulement si il est bijectif.

Exemple 92 — Deux versions des nombres complexes. On considère l'ensemble $\mathbb{C}_1 := \mathbb{R}^2$ muni des lois $(x,y)+(x',y') = (x+x', y+y')$ et $(x,y)(x',y') = (xx'-yy', xy'+yx')$ et du morphisme $i_1 : x \in \mathbb{R} \mapsto (x,0) \in \mathbb{C}_1$. Vérifier que c'est une extension de corps de $\mathbb{R}$. Vérifier que la structure naturelle d'espace vectoriel sur $\mathbb{R}$ de $\mathbb{C}_1$ coïncide avec la structure d'espace vectoriel donnée par la structure d'extension.

On considère l'extension $\mathbb{C}_2 := \mathbb{R}[\mathrm{X}]/(\mathrm{X}^2+1)$ de $\mathbb{R}$. Quel est le morphisme de $\mathbb{R}$ dans $\mathbb{C}_2$ sous-jacent à l'extension ?

Vérifier que $\mathbb{C}_1$ et $\mathbb{C}_2$ sont deux extensions isomorphes de $\mathbb{R}$.

Propriété 93 — Injectivité. Un morphisme d'extensions est nécessairement injectif (car c'est un morphisme d'anneaux unitaires qui part d'un corps) et est aussi k-linéaire (car c'est un morphisme de k-algèbres).

Remarque 94 Pour qu'il existe un morphisme d'extensions de K dans L, il faut que $[\mathrm{L} : k] \geqslant [\mathrm{K} : k]$. (La condition est-elle suffisante ?)

SOUS-EXTENSION

Définition 95 — Sous-extension. Soit k un corps et (K, i) une extension de k.

Une sous-k-extension de (K, i) est un sous-corps L de K contenant $i(k)$ ou ce qui revient au même une sous-algèbre de K qui est un corps.

Le couple (L, i) est alors une extension de k et l'inclusion de L dans K est un morphisme d'extensions.

Remarque 96 Une intersection de sous-extensions est une sous-extension. En considérant l'intersection de toutes les sous-extensions contenant une partie donnée, on définit la notion d'*extension engendrée*

Notation 97 Soit k un corps et (K, i) une extension de k. Soit A une partie de K. La sous-extension engendré par A est notée $k(\mathrm{A})$ c'est le plus petit sous-corps contenant k et A.

Exemples 98 Dans $\mathbb{C}$, le sous-corps engendré par i est $\mathbb{Q}(i)$ qui est un $\mathbb{Q}$-espace vectoriel de dimension 2, la sous-$\mathbb{R}$-algèbre de $\mathbb{C}$ engendré par i est $\mathbb{C}$: $\mathbb{C} = \mathbb{R}(i)$.

Sous-algèbre VS Sous-extension

Exemples 99 Ne pas confondre la sous-algèbre de K engendrée par A notée $k[\mathrm{A}]$ et la sous-extension de K engendrée par A notée $k(\mathrm{A})$.

Dans $\mathbb{R}(\mathrm{T})$, si $\mathrm{A} = \{\mathrm{T}^2\}$, on distingue $\mathbb{R}[\mathrm{T}^2]$ et $\mathbb{R}(\mathrm{T}^2)$.

Exercice 28 Comparer

(*i*) $\mathbb{R}[i]$ et $\mathbb{R}(i)$
(*ii*) $\mathbb{Q}[i]$ et $\mathbb{Q}(i)$
(*iii*) $\mathbb{R}[\mathrm{T}^2]$ et $\mathbb{R}(\mathrm{T}^2)$
(*iv*) $\mathbb{Q}[\pi]$ et $\mathbb{Q}(\pi)$
(*v*) $\mathbb{Q}[\sqrt{2}]$ et $\mathbb{Q}(\sqrt{2})$
(*vi*) $\mathbb{Q}[e]$ et $\mathbb{Q}(e)$

Exercice 29 Soient k un corps, (K, i) une extension de k et A une partie de K. Montrer que

$$k[\mathrm{A}] = \{\mathrm{P}(a_1,\dots,a_n),\ n \in \mathbb{N},\ a_1,\dots,a_n \in \mathrm{A},\ \mathrm{P} \in k[\mathrm{X}_1,\dots,\mathrm{X}_n]\}$$

$$k(\mathrm{A}) = \{\mathrm{P}(a_1,\dots,a_n)/\mathrm{Q}(a_1,\dots,a_n),\ n \in \mathbb{N},\ a_1,\dots,a_n \in \mathrm{A},\ \mathrm{P},\mathrm{Q} \in k[\mathrm{X}_1,\dots,\mathrm{X}_n],\ \mathrm{Q}(a_1,\dots,a_n) \neq 0\}$$

2.5 Extensions algébriques

ALGÈBRE MONOGÈNE

Lemme 100 Soit A une k-algèbre. Pour tout $x \in \mathrm{A}$, il existe un unique morphisme de k-algèbres de $k[\mathrm{X}]$ dans A tel que $\varphi_x(\mathrm{X}) = x$. Il est donné par $\varphi_x(\mathrm{P}) = \mathrm{P}(x)$.

Son image est $k[x] \subset \mathrm{K}$.

Deux cas peuvent se produire

- φ_x est injectif (c'est-à-dire $\mathrm{P}(x) = 0$ implique $\mathrm{P} = 0$) et on a $k[\mathrm{X}] \overset{k\text{-alg.}}{\simeq} k[x]$.
- φ_x n'est pas injectif, auquel cas $\operatorname{Ker}\varphi_x$ est un idéal non nul de $k[\mathrm{X}]$, il existe donc un unique polynôme unitaire $\pi_x \in \mathrm{K}[\mathrm{X}]$ tel que $\operatorname{Ker}\varphi_x = (\pi_x)$. On l'appelle le *polynôme minimal de x*. Les éléments de $\operatorname{Ker}\varphi_x$ sont appelés **polynômes annulateurs de** x.

  De plus, on a $k[\mathrm{X}]/(\pi_x) \overset{k\text{-alg.}}{\simeq} k[x]$ et

$$\deg \pi_x = \dim_k k[x] = \min\{\ell \in \mathbb{N}, (1, x, \ldots, x^\ell) \text{ soit liée}\}$$

Preuve. Comme la k-algèbre est engendré par X, il existe au plus un seul tel morphisme (l'ensemble des éléments de $k[\mathrm{X}]$ où coïncident deux morphismes de k-algèbres est une sous-k-algèbre de $k[\mathrm{X}]$, si elle contient X c'est tout !).

Un polynôme $\mathrm{P} \in k[\mathrm{X}]$ s'écrit sous la forme $\sum_{i=0}^{n} a_i \mathrm{X}^i$ avec $a_i \in k$ et $a_n \neq 0$. Une telle écriture étant unique. Posons alors $\varphi_x(\mathrm{P}) = \sum_{i=0}^{n} a_i x^i$ (qui a bien un sens puisque A est une k-algèbre).

Ainsi φ_x est bien défini. C'est un morphisme de k-algèbres grâce aux règles de calculs dans une k-algèbre.

L'image est une sous-k-algèbre de A qui contient x, elle contient donc $k[x]$. Mais on a bien sûr $\varphi_x(\mathrm{P}) \in k[x]$ pour tout P. En effet, par récurrence sur i, $x^i \in k[x]$ et ensuite par des combinaisons linéaires, on obtient le résultat.

ÉLÉMENTS ALGÉBRIQUES.

Soit (K, i) une extension de k et $x \in \mathrm{K}$.

Proposition-Définition 101 Soit (K, i) une extension de k et $x \in \mathrm{K}$. Les propriétés suivantes sont équivalentes

(i) La famille $(x^k, k \in \mathbb{N})$ est liée sur k

(ii) Il existe $\mathrm{P} \in k[\mathrm{X}] \setminus \{0\}$ tel que $\mathrm{P}(x) = 0$

(iii) φ_x n'est pas injectif

(iv) $k[x] = k(x)$

(v) $[k[x] : k] < +\infty$

(vi) $[k(x) : k] < +\infty$

(vii) $k[\mathrm{X}]/\operatorname{Ker}\varphi_x$ est un corps

$(viii)$ $k[x]$ est un corps

(ix) Il existe une sous-algèbre L de K contenant x telle que $[\mathrm{L} : k] < +\infty$

(x) Il existe une sous-extension L de K contenant x telle que $[\mathrm{L} : k] < +\infty$

Un tel x est dit *algébrique sur k*.

Preuve. L'équivalence de (i), (ii) et (iii) résulte directement des définitions.

L'équivalence de (vii) et $(viii)$ résulte du fait que $k[\mathrm{X}]/\operatorname{Ker}\varphi_x$ est isomorphe à $k[x]$.

L'équivalence entre $(viii)$ et (iv) résulte de la définition de l'extension engendrée par x.

L'implication $(viii)$ donne (ii) résulte de la disjonction de cas du lemme 100.

On a $(v) \Leftrightarrow (ix)$: dans un sens on pose $\mathrm{L} = k[x]$ qui convient. Dans l'autre sens, $k[x]$ est contenu dans L qui est de dimension finie. De même $(vi) \Leftrightarrow x$.

Toujours grâce au lemme 100, on a (iii) qui implique (v) puisque $\dim k[x] = \deg \pi_x$. Inversement, si φ_x est injectif alors $k[x] \overset{k\text{-alg.}}{\simeq} k[\mathrm{X}]$ et donc $\dim k[x] = +\infty$. Finalement, on a $(iii) \Leftrightarrow (v)$.

On suppose $k[x]$ est un corps. Si $x = 0$ alors $k[x] = k$ et $\operatorname{Ker}\varphi_x = (\mathrm{X})$. Si $x \neq 0$ alors $x^{-1} \in k[x]$ et donc on peut écrire

$$x^{-1} = \sum_{i=0} m a_i x^i$$

avec au moins l'un des $a_i \in k$ non nul puisque $x^{-1} \neq 0$. En multipliant par x, on obtient un polynôme annulateur de x non nul. Ainsi $(viii)$ implique (ii).

Dans la preuve de la proposition 103, on montre que (iii) implique $(viii)$ puisque π_x est irréductible. De plus, $k[x]$ est alors de dimension finie et donc aussi (iii) implique (vi).

Enfin (vi) implique (v).

Éléments transcendants.

Proposition-Définition 102 — Élément transcendant. Soit (K, i) une extension de k et $x \in \mathrm{K}$. Les propriétés suivantes sont équivalentes

(i) La famille $(x^k,\ k \in \mathbb{N})$ est libre sur k
(ii) Si $\mathrm{P}(x) = 0$ avec $\mathrm{P} \in k[\mathrm{X}]$ alors $\mathrm{P} = 0$
(iii) φ_x est injectif
(iv) $k[\mathrm{X}] \overset{k\text{-alg.}}{\simeq} k[x]$
(v) $k(\mathrm{X}) \overset{k\text{-ext.}}{\simeq} k(x)$
(vi) $[k[x] : k] = +\infty$
(vii) $[k(x) : k] = +\infty$
$(viii)$ $k(x) \neq k[x]$;
(ix) $k[x] \subsetneq k(x)$;

Un tel x est dit *transcendant sur k*.

Preuve. Hormis les points (iv), (v) et (ix), les points sont les négations des points de la proposition-définition précédente.

On a évidemment (iii) implique (iv). De plus si (iv) est vérifiée alors $k[x]$ est de dimension infini. Et si $\operatorname{Ker} \varphi_x \neq 0$ alors $\dim_k k[x]$ est fini. Donc (iv) implique (iii).

Évidemment (ix) implique $(viii)$. Par ailleurs, comme on a toujours $k[x] \subset k(x)$ $(viii)$ implique (ix).

Enfin, supposons (iv). On a alors une application injective de $k[\mathrm{X}]$ dans $k(x)$ et donc par la propriété du corps de fraction un morphisme injectif de $k(\mathrm{X})$ dans $k(x)$. L'image est une sous-extension qui contient x et donc c'est $k(x)$. D'où (v).

Pour terminer supposons (v) alors $k(x)$ est de dimension infinie sur k puisque $k(\mathrm{X})$ l'est (par exemple, $k(\mathrm{X})$ contient la famille des X^k pour $k \in \mathbb{N}$ comme famille libre).

Proposition 103 — Élément algébrique (suite). Soit (K, i) une extension de k et $x \in \mathrm{K}$ un élément algébrique. Le polynôme minimal π_x de x sur k est **irréductible**.

Inversement, soit $\mathrm{P} \in k[\mathrm{X}]$ un polynôme irréductible qui est un polynôme annulateur de x. Alors, il existe $\lambda \in k^\times$ tel que $\mathrm{P} = \lambda \pi_x$.

On a $[k[x] : k] = \deg \pi_x$. Cet entier est noté $\deg_k(x)$ et appelé *degré de x sur k*.

Preuve. Démonstration 1. Si π_x n'est pas irréductible alors on peut écrire $\pi_x = \mathrm{PQ}$ avec P, Q non inversibles. On a alors $\pi_x(x) = 0 = \mathrm{P}(x)\mathrm{Q}(x)$. Mais cette relation est dans l'anneau intègre K. Donc $\mathrm{P}(x) = 0$ ou $\mathrm{Q}(x) = 0$ et P ou Q sont dans $\operatorname{Ker} \varphi_x$. Mais $\deg \mathrm{P} < \deg \pi_x$ et $\deg \mathrm{Q} < \deg \pi_x$ et π_x est un générateur de $\operatorname{Ker} \varphi_x$ donc un élément non nul de $\operatorname{Ker} \varphi_x$ de degré minimal. Non.

Démonstration 2. $k[\mathrm{X}]/(\varphi_x) \overset{k\text{-alg.}}{\simeq} k[x] = k(x)$ qui est un corps donc intègre. Donc, φ_x est un élément premier de $k[\mathrm{X}]$ donc irréductible.

Rapprocher ces deux démonstrations de celle de la proposition 76.

Si $\mathrm{P}(x) = 0$ et P irréductible alors on a $\pi_x \mid \mathrm{P}$ et donc $\pi_x \mathrm{Q} = \mathrm{P}$. Mais P est irréductible donc π_x inversible (non !) ou Q inversible et on a le résultat.

Des exemples

Des nombres algébriques.

Le nombre $\sqrt{2}$ est racine de $\mathrm{X}^2 - 2 \in \mathbb{Q}[\mathrm{X}]$. Ainsi $\sqrt{2}$ est algébrique sur $\mathbb{Q}$. Ainsi $\mathbb{Q}(\sqrt{2})$ la sous-$\mathbb{Q}$-extension de $\mathbb{C}$ engendrée par $\sqrt{2}$ est de dimension finie sur $\mathbb{Q}$ et est aussi $\mathbb{Q}[\sqrt{2}]$. Par ailleurs, le polynôme minimal de $\sqrt{2}$ sur $\mathbb{Q}$ est un diviseur de $\mathrm{X}^2 - 2$. Mais celui-ci est irréductible sur $\mathbb{Q}$ puisqu'il est de degré 2 et sans racine dans $\mathbb{Q}$. Ainsi $\mathrm{X}^2 - 2$ est le polynôme minimal de $\sqrt{2}$ sur $\mathbb{Q}$ qui est de

degré 2 et donc $(1, \sqrt{2})$ est une $\mathbb{Q}$-base de $\mathbb{Q}(\sqrt{2}) = \mathbb{Q}[\sqrt{2}]$: un élément de $\mathbb{Q}(\sqrt{2})$ s'écrit sous la forme $a + b\sqrt{2}$ avec $a, b \in \mathbb{Q}$.

Lemme 104 Soit k un corps et $\mathrm{P} \in k[\mathrm{X}]$ de degré 2 ou 3. Alors P est irréductible si et seulement si il n'a pas de racine.

Preuve. Si x est une racine de P alors $(\mathrm{X} - x) \mid \mathrm{P}$ qui n'est donc pas irréductible.

Si P est réductible, on écrit $\mathrm{P} = \mathrm{QR}$ avec Q et R non inversible donc $\deg \mathrm{Q} \geqslant 1$ et $\deg \mathrm{R} \geqslant 1$. Comme $\deg \mathrm{Q} + \deg \mathrm{R} = 2$ ou 3, on a soit Q ou R qui est de degré 1 et donc P a une racine.

Le nombre $\sqrt[n]{2}$ est racine de $\mathrm{X}^n - 2 \in \mathbb{Q}[\mathrm{X}]$. Ainsi $\sqrt[n]{2}$ est algébrique sur $\mathbb{Q}$. Ainsi $\mathbb{Q}(\sqrt[n]{2})$ la sous-$\mathbb{Q}$-extension de $\mathbb{C}$ engendrée par $\sqrt[n]{2}$ est de dimension finie sur $\mathbb{Q}$ et est aussi $\mathbb{Q}[\sqrt[n]{2}]$. Par ailleurs, le polynôme minimal de $\sqrt[n]{2}$ sur $\mathbb{Q}$ est un diviseur de $\mathrm{X}^n - 2$. Mais celui-ci est irréductible sur $\mathbb{Q}$ en appliquant le critère d'Eisenstein pour $p = 2$. Ainsi $\mathrm{X}^n - 2$ est le polynôme minimal de $\sqrt[n]{2}$ sur $\mathbb{Q}$ qui est de degré n et donc $(1, \sqrt[n]{2}, \ldots, \sqrt[n]{2}^{n-1})$ est une $\mathbb{Q}$-base de $\mathbb{Q}(\sqrt[n]{2}) = \mathbb{Q}[\sqrt[n]{2}]$: un élément de $\mathbb{Q}(\sqrt[n]{2})$ s'écrit sous la forme $a_0 + a_1 \sqrt[n]{2} + \cdots + a_{n-1} \sqrt[n]{2}^{n-1}$ avec $a_i \in \mathbb{Q}$ pour tout i.

On peut évidemment remplacer 2 par un nombre premier quelconque p ou un produit de nombres premiers deux à deux distincts.

i est algébrique sur $\mathbb{Q}$, de degré 2 de polynôme minimal $\mathrm{X}^2 + 1$.

$\sqrt{5} + \sqrt[3]{7} + i\sqrt[4]{2}$ est un élément algébrique sur $\mathbb{Q}$. Il n'est pas facile de déterminer son degré (24) ni le polynôme minimal de cet élément. Même un polynôme annulateur n'est pas aisé à déterminer.

Des nombres transcendants

X est évidemment un élément transcendant de $k(\mathrm{X})$ sur k.

Les nombres π (Lindemann, 1882) et e (Hermite, 1873) sont transcendants sur $\mathbb{Q}$.

Proposition 105 – Cantor (1874). Soit k un corps infini et K une extension de k. La fermeture algébrique L de k dans K a le même cardinal que k.

En particulier, la fermeture algébrique de $\mathbb{Q}$ dans $\mathbb{C}$ est dénombrable et il existe des nombres réels transcendants et même une infinité non dénombrable !

Preuve. Comme les éléments de k sont algébriques, le cardinal de L est plus grand que celui de k. Par ailleurs, on a $\mathrm{L} = \cup_{\mathrm{P} \in k[\mathrm{X}]} \{\text{racines de P}\}$. C'est une réunion d'ensembles finis. Ainsi $\operatorname{Card} \mathrm{L} \leqslant \operatorname{Card} k[\mathrm{X}]$. Mais $k[\mathrm{X}] = \cup_{n \in \mathbb{N}} k_n[\mathrm{X}]$ et $k_n[\mathrm{X}] \overset{k\text{-ev.}}{\simeq} k^{n+1}$ qui a le même cardinal que k puisque k est infini. Ainsi $\operatorname{Card} k[\mathrm{X}] = \operatorname{Card} k$ et on obtient le résultat souhaité.

Les nombres de Liouville.

Soit $a = (a_n)_{n \in \mathbb{N}}$ une suite d'entiers avec $a_n \in [\![0 \,,\, 9]\!]$ pour tout $n \in \mathbb{N}$. On note x_a le nombre

$$x_a = \sum_{n \in \mathbb{N}} \frac{a_n}{10^{n!}}$$

Lemme 106 Si $a \neq a'$ alors $x_a \neq x_{a'}$.

Preuve. Supposons que $x_a = x_{a'}$ et $a \neq a'$. Considérons n_0 le plus petit n tel que $a_n \neq a'_n$. On a alors

$$\frac{a_{n_0} - a'_{n_0}}{10^{n_0!}} = \sum_{n > n_0} \frac{a'_n - a_n}{10^{n!}} \,.$$

Ainsi, on obtient

$$\frac{1}{10^{n_0!}} \leqslant \frac{a_{n_0} - a'_{n_0}}{10^{n_0!}} \leqslant \sum_{n > n_0} \frac{9}{10^{n!}} < \sum_{n \geqslant (n_0+1)!} \frac{9}{10^n} = \frac{9}{10^{(n_0+1)!}} \frac{1}{1 - 1/10}$$

et donc
$$1 < \frac{10^{1+n_0!}}{(n_0+1)!} \qquad \text{NON !}$$

Transcendance des nombres de Liouville. **Proposition 107** Si a n'est pas nulle à partir d'un certain rang alors x_a est transcendant sur $\mathbb{Q}$.

Lemme 108 Soit x un élément algébrique sur $\mathbb{Q}$ de degré d. Il existe $c > 0$ tel que

$$\left| x - \frac{p}{q} \right| \geqslant \frac{c}{q^d}$$

pour tout $(p,q) \in \mathbb{Z} \times \mathbb{N}^*$ tel que $x \neq p/q$.

Preuve. Soit P_x le polynôme minimal de x sur $\mathbb{Q}$. On pose $\mathrm{P}_x = c(\mathrm{P}_x)\mathrm{P}$ avec $\mathrm{P} \in \mathbb{Z}[\mathrm{X}]$ primitif. On pose $\mathrm{P} = a_0 + a_1\mathrm{X} + \cdots + a_n\mathrm{X}^n$.

Si $n = 1$ alors $x = p'/q'$ est rationnel et on a alors $|x - p/q| = |qp' - p'q|/qq' \geqslant 1/qq'$ et $c = 1/q'$ convient.

Si $n \geqslant 2$ alors $\mathrm{P}(p/q) \neq 0$ (sinon P ne serait pas irréductible sur $\mathbb{Q}$) et on a alors

$$|\mathrm{P}(p/q)| = \frac{|a_0q^n + a_1pq^{n-1} + \cdots + a_np^n|}{q^n} \geqslant \frac{1}{q^n}$$

On note alors $\mathrm{M} = \sup_{y\in[x-1,x+1]} |\mathrm{P}'(y)|$. On a alors pour $|x - p/q| \leqslant 1$,

$$\mathrm{M}|x - p/q| \geqslant |\mathrm{P}(p/q) - \mathrm{P}(x)| = |\mathrm{P}(p/q)| \geqslant 1/q^n$$

et pour $|x - p/q| > 1$,

$$|x - p/q| > 1 \geqslant 1/q^n$$

Ainsi $c = \inf(1, 1/\mathrm{M})$ contient.

Preuve de la proposition

Preuve. Supposons que x_a soit algébrique de degré n et considérons $m > n$. On pose

$$r_m = \sum_{k=0}^{m} \frac{a_k}{10^{k!}} = \frac{\mathrm{A}_m}{10^{m!}} \in \mathbb{Q}$$

On a alors

$$0 < x - r_m < \frac{1}{10^{(m+1)!-1}} = \frac{1}{10^{m\cdot m!}}$$

Mais d'après le lemme, il existe $c > 0$ tel que

$$\frac{c}{10^{nm!}} \geqslant x - r_m \geqslant \frac{1}{10^{m\cdot m!}}$$

et donc
$$c \geqslant \frac{1}{10^{m!(m-n)}}$$
NON !

Le cardinal de l'ensemble des nombres de Liouville transcendant est égal à celui de $\mathbb{R}$.

En effet, il contient un sous-ensemble en bijection avec les suites à valeurs dans $\{1, \ldots, 9\}$ qui a le même cardinal que celui des suites à valeurs dans $\{0, 1\}$ qui à le même cardinal que celui de $\mathbb{R}$ (développement décimal).

EXTENSIONS ALGÉBRIQUES

Proposition 109 – Ensemble des éléments algébriques. Soit (K, i) une extension de k. L'ensemble des éléments de K algébriques sur k est une sous-extension de k appelée **fermeture algébrique de k dans** K.

Lemme 110 – Base télescopique. Soient K une extension de k et E un K-espace vectoriel. On a alors

$$[\mathrm{E} : k] = [\mathrm{E} : \mathrm{K}][\mathrm{K} : k]$$

Remarque 111 Quelle est la dimension de $\mathbb{C}^n$ en tant que $\mathbb{R}$-espace vectoriel ? En donner une $\mathbb{R}$-base.

Preuve. On définit une structure de k-espace vectoriel sur E de la façon suivante : pour $\alpha \in k$ et $e \in \mathrm{E}$, on pose $\alpha \cdot e = i(\alpha)e$. On vérifie les axiomes... (ici i est le morphisme de k dans K qui définit l'extension).

Soit $(e_i)_{i\in\mathrm{I}}$ une base de E en tant que K-espace vectoriel et $(\lambda_j)_{j\in\mathrm{J}}$ une base de K en tant que k-espace vectoriel. Montrons que $(\lambda_je_i)_{i,j\in\mathrm{I}\times\mathrm{J}}$ est une base de E comme k-espace vectoriel.

Soit $e \in \mathrm{E}$. On peut écrire $e = \sum_{i\in\mathrm{I}} \mu_ie_i$ avec $\mu_i \in \mathrm{K}$ (puisque $(e_i)_{i\in\mathrm{I}}$ est une K-base de E). On écrit ensuite $\mu_i = \sum_{j\in\mathrm{J}} \alpha_{ij}\lambda_j$ avec $\alpha_{ij} \in k$. Ainsi $e = \sum_{(i,j)\in\mathrm{I}\times\mathrm{J}} \alpha_{ij}\lambda_je_i$ et $(\lambda_je_i)_{i,j\in\mathrm{I}\times\mathrm{J}}$ engendre E sur k.

Il reste à montrer que $(\lambda_j e_i)_{i,j\in \mathrm{I}\times\mathrm{J}}$ est libre sur k. Considérons donc une base $(\beta_{ij})_{(i,j)\in\mathrm{I}\times\mathrm{J}}$ d'éléments de k tel que

$$\sum_{(i,j)\in\mathrm{I}\times\mathrm{J}} \beta_{ij}\lambda_j e_i = 0.$$

On écrit alors la somme sous la forme $\displaystyle\sum_{i\in\mathrm{I}}\left(\sum_{j\in\mathrm{J}}\beta_{ij}\lambda_j\right)e_i$

Comme les $(e_i)_{i\in\mathrm{I}}$ forment une famille libre sur K et que

$$\sum_{j\in\mathrm{J}}\beta_{ij}\lambda_j \in \mathrm{K}$$

On obtient $\sum_{j\in\mathrm{J}}\beta_{ij}\lambda_j = 0$ pour tout $i \in \mathrm{I}$. Mais $\beta_{ij} \in k$ et $(\lambda_j)_{j\in\mathrm{J}}$ est libre sur k. Donc $\beta_{ij} = 0$ pour tout $(i,j) \in \mathrm{I}\times\mathrm{J}$.

Preuve de la proposition

Preuve. Si $x \neq 0$ alors $k(x^{-1}) = k(x)$ (tout sous-extension de K qui contient x contient x^{-1} et inversement).

Tout élément λ de k est algébrique sur k puisque racine du polynôme $\mathrm{X}-\lambda$ (Attention : décoder les abus de langage !).

On va montrer que $k(x,y)$ qui contient $x+y$ et xy est de dimension finie sur k et on utilise le critère (x) pour conclure. On remarque que $k(x,y) = k(x)(y)$. Or

$$[k(x,y):k] = [k(x)(y):k(x)][k(x):k]$$

Comme $[k(x):k] < +\infty$, on a $[k(x,y):k] < +\infty$ si et seulement si $[k(x)(y):k(x)] < +\infty$ c'est-à-dire si et seulement si y est algébrique sur $k(x)$. Or y est racine d'un polynôme non nul à coefficients dans k donc à coefficients dans $k(x)$...

Extension finie **Définition 112** Soit (K,i) une extension de k. On dit que K est une **extension finie de** k si $[\mathrm{K}:k] < +\infty$. On dit que K est une **extension algébrique de** k si tout élément de K est algébrique sur k (ou encore si K est la fermeture algébrique de k dans K).

Une extension finie est toujours algébrique (c'est le point (x) de la définition d'élément algébrique). La réciproque est fausse.

Exercice 30 Montrer que la fermeture algébrique de $\mathbb{Q}$ dans $\mathbb{C}$ est une extension algébrique de $\mathbb{Q}$ qui n'est pas une extension finie.

Déterminer la fermeture algébrique de $\mathbb{R}$ dans $\mathbb{R}(\mathrm{T})$.

Déterminer la fermeture algébrique de $\mathbb{R}(\mathrm{T})$ dans $\mathbb{C}(\mathrm{T})$. Déterminer $[\mathbb{C}(\mathrm{T}):\mathbb{R}(\mathrm{T})]$.

Déterminer la fermeture algébrique de $\mathbb{R}$ dans $\mathbb{C}(\mathrm{T})$.

Transitivité. **Proposition 113 – Transitivité de l'algébricité.** Soit (K,i) une extension algébrique de k et (L,j) une extension de K. Un élément $x \in \mathrm{L}$ de L est algébrique sur k si et seulement si x est algébrique sur K.

Ainsi si L est une extension algébrique de k si et seulement si L est une extension algébrique de K.

Lemme 114 Soit (K,i) une extension de k et $x_1,\dots,x_n \in \mathrm{K}$. Les propositions suivantes sont équivalentes :

(i) x_i algébrique sur k pour tout $i \in \{1,\dots,n\}$

(ii) x_{i+1} algébrique sur $k(x_1,\dots,x_i)$ pour tout $i \in \{0,\dots,n-1\}$

(iii) $[k(x_1,\dots,x_n):k] < +\infty$

(iv) $k(x_1,\dots,x_n)$ algébrique sur k.

Preuve. On a immédiatement $(iii) \Rightarrow (iv)$ et $(iv) \Rightarrow (i)$.

$(i) \Rightarrow (ii)$ résulte de la remarque suivante : x_{i+1} algébrique sur k implique x_{i+1} racine d'un polynôme non nul à coefficients dans k donc dans $k(x_1,\dots,x_i)$.

$(ii) \Rightarrow (iii)$ résulte de la multiplicativité des degrés

$$[k(x_1,\dots,x_n):k] = [k(x_1,\dots,x_n):k(x_1,\dots,x_{n-1})]\cdots[k(x_1):k]$$

chacun des facteurs étant fini puisque x_{i+1} est algébrique sur $k(x_1, \ldots, x_i)$.

Démo de la proposition.

Un élément algébrique sur k est évidemment algébrique sur K (un polynôme à coefficients dans k est à coefficients dans K).

Supposons donc x algébrique sur K. Il est racine d'un polynôme $\mathrm{P} \in \mathrm{K}[\mathrm{X}]$ non nul : $\mathrm{P} = a_0 + a_1\mathrm{X} + \cdots + a_n\mathrm{X}^n$ avec $a_i \in \mathrm{K}$. Ainsi x est algébrique sur $k(a_0, \ldots, a_n)$ qui est de dimension finie sur k d'après le lemme.

Comme x est algébrique sur $k(a_0, \ldots, a_n)$, on a

$$[k(a_0, \ldots, a_n)(x) : k(a_0, \ldots, a_n)] < +\infty$$

Et par multiplicativité des degrés, on conclut

$$[k(a_0, \ldots, a_n, x) : k] = [k(a_0, \ldots, a_n)(x) : k(a_0, \ldots, a_n)][k(a_0, \ldots, a_n) : k] < +\infty$$

ce qui assure que x est algébrique sur k.

Applications

Exercice 31 Soit K un extension de k et L la fermeture algébrique de k dans K. Déterminer la fermeture algébrique de L dans K.

Exercice 32 Soit K une extension de k. Montrer que K est algébrique sur k si et seulement si l'extension $k \mapsto \mathrm{K}$ est engendrée par des éléments algébriques sur k.

Soit K une extension de k et E et F deux sous-extension de K. On suppose que $\mathrm{K} = \mathrm{E}(\mathrm{F})$ c'est-à-dire que K est engendrée comme extension de E par F. Montrer que si F est algébrique sur k alors K est algébrique sur E.

Une étude des extensions de degré 2

Proposition 115 Soit k un corps de caractéristique différente de 2 et K une extension de degré 2 de k.

Pour tout $x \in \mathrm{K} \smallsetminus k$, on a $\mathrm{K} = k(x)$. Il existe $\delta \in \mathrm{K} \smallsetminus k$ tel que $\delta^2 \in k$. Le polynôme minimal de δ est de la forme $\mathrm{X}^2 - a$

Si $\delta' \in \mathrm{K}$ et vérifie $\delta'^2 \in k$, on a $\delta' \in k$ ou $\delta' = b\delta$ avec $b \in k$.

Preuve. Comme $x \in \mathrm{K} \smallsetminus k$, on a $2 = [\mathrm{K} : k] \leqslant [k(x) : k] > 1$ et donc $[k(x) : k] = [\mathrm{K} : k]$. Ainsi $\mathrm{K} = k(x)$.

Le polynôme minimal P de x sur k est de degré 2. On écrit $\mathrm{P} = \mathrm{X}^2 + a\mathrm{X} + b$. En posant $\delta = x + a/2$, on a

$$\delta^2 = x^2 + ax + a^2/4 = \frac{a^2 - 4b}{4} \in k$$

De plus $\delta \notin k$ sinon $\delta - a/2 = x$ le serait aussi.

On a alors $(1, \delta)$ qui est une k-base de K. On peut écrire $\delta' = a + b\delta$. On a alors $\delta'^2 = a^2 + \delta^2 b^2 + 2ab\delta \in k$. Ainsi $ab = 0$. Si $b = 0$ alors $\delta' \in k$. Si $a = 0$, on a le résultat voulu.

Proposition 116 Soit k un corps de caractéristique de 2 et K une extension de degré 2 de k.

S'il existe $x \in \mathrm{K} \smallsetminus k$ tel que $x^2 \in k$ alors pour tout $y \in \mathrm{K} \smallsetminus k$, on a $y^2 \in k$ et le polynôme minimal de y sur k est de la forme $\mathrm{X}^2 - c$ avec $c \in k$

Sinon pour tout $x \in \mathrm{K} \smallsetminus k$ le polynôme minimal de x est de la forme $\mathrm{X}^2 + a\mathrm{X} + b$ avec $a, b \in k$ et $a \neq 0$ et il existe un élément x tel que le polynôme minimal soit de la forme $\mathrm{X}^2 + \mathrm{X} + b$ avec $b \in k$.

Preuve. $(1, x)$ est une k-base de K. On écrit $y = a + bx$ avec $b \neq 0$ sinon $y \in k$. On a alors $y^2 = a^2 + b^2x^2 \in k$. Soit $c = y^2 \in k$. Le polynôme minimal de y est alors $\mathrm{X}^2 - c$.

En effet, sinon, le polynôme minimal est de la forme $\mathrm{X}^2 + b$ et donc on est dans le premier cas. NON ! Et l'élément x/a est alors racine de $\mathrm{X}^2 + \mathrm{X} + b/a^2$.

Exercice 33 — Endomorphisme et automorphisme. Soit k un corps et (K, i) une extension **algébrique** de k et σ un endomorphisme de (K, i). Montrer que σ est un automorphisme de (K, i).

Montrer que σ peut ne pas être un automorphisme si K n'est pas algébrique.

2.6 Algébricité et constructibilité

Objectif : Caractériser les nombres constructibles à la règle et au compas de manière algébrique.

Conséquences : Résoudre les problèmes grecs classiques (duplication du cube, trisection de l'angle, quadrature du cercle).

Idée : des cercles et des droites ne donne que des $\sqrt{}$...

Intersection de deux droites.

Lemme 117 – Question de rationalité. Soit $ax + by + c = 0$ et $a'x + b' + c' = 0$ les équations de deux droites dans le plan.

Lorsqu'elles se rencontrent (c'est-à-dire si $ab' - a'b \neq 0$), les coordonnées du points d'intersection sont dans $\mathbb{Q}(a, b, c, a', b', c')$.

Preuve. On résout le système et on trouve $x = -(b'c - c'b)/(b'a - a'b)$ et $y = -(a'c - c'a)/(b'a - a'b)$.

Intersection de deux cercles.

Lemme 118 – Questions de rationalité. Soit $ax + by + c = 0$ l'équation d'une droite et $x^2 + y^2 + a'x + b' + c' = 0$ l'équation d'un cercle.

Lorsqu'ils se rencontrent, les coordonnées des points d'intersection sont dans une extension quadratique de $\mathbb{Q}(a, b, c, a', b', c')$.

Preuve. On a $a \neq 0$ ou $b \neq 0$. Si $a \neq 0$, on exprime x en fonction de y : $x = -c/a - by/a$, on reporte dans l'équation du cercle. On obtient ainsi une équation de degré 2 en y :

$$\left(\frac{c}{a} + \frac{by}{a}\right)^2 + y^2 - a'\frac{c}{a} - a'\frac{by}{a} + b'y + c' = 0$$

Le discriminant Δ de cette équation est dans $\mathbb{Q}(a, b, c, a', b', c')$. Ainsi $y \in \mathbb{Q}(a, b, c, \sqrt{\Delta})$ qui est de degré 1 ou 2 sur $\mathbb{Q}(a, b, c, a', b', c')$.

Comme $x = -c/a - by/a$, $x \in \mathbb{Q}(a, b, c, \sqrt{\Delta})$.

Intersection de deux cercles.

Lemme 119 – Questions de rationalité. Soit $x^2 + y^2 + ax + by + c = 0$ et $x^2 + y^2 + a'x + b' + c' = 0$ les équations de deux cercles.

Lorsqu'ils se rencontrent, les coordonnées des points d'intersection sont dans une extension quadratique de $\mathbb{Q}(a, b, c, a', b', c')$.

Preuve. Le système d'équation

$$\begin{cases} x^2 + y^2 + ax + by + c &= 0 \\ x^2 + y^2 + a'x + b'y + c' &= 0 \end{cases}$$

est évidemment équivalent au système d'équation

$$\begin{cases} x^2 + y^2 + ax + by + c &= 0 \\ (a' - a)x + (b' - b)y + c' - c &= 0 \end{cases}$$

qui décrit l'intersection d'une droite et d'un cercle. En appliquant le lemme précédent, on obtient que les coordonnées des points d'intersections sont dans une extension quadratique de

$$\mathbb{Q}(a, b, c, a' - a, b' - b, c' - c) = \mathbb{Q}(a, b, c, a', b', c')$$

Une autre description.

On pose $\mathrm{B} = \{z \in \mathbb{C}, \quad \exists \mathrm{L}_0 = \mathbb{Q} \subset \mathrm{L}_1 \subset \cdots \subset \mathrm{L}_n, \quad z \in \mathrm{L}_n\}$ où les L_i forment une suite strictement croissante de sous-corps de $\mathbb{C}$ vérifiant $[\mathrm{L}_{i+1} : \mathrm{L}_i] = 2$.

On veut montrer que $\mathrm{B} = \mathrm{A} := \{z \in \mathbb{C}, z \text{ constructible }\}$

B ⊂ A

Soit $z \in \mathrm{B}$, il existe une suite strictement croissante de sous-corps de $\mathbb{C}$ vérifiant $[\mathrm{L}_{i+1} : \mathrm{L}_i] = 2$ telle que $\mathrm{L}_0 = \mathbb{Q} \subset \mathrm{L}_1 \subset \cdots \subset \mathrm{L}_n$, et $z \in \mathrm{L}_n$.

On va montrer par récurrence sur i que L_i est contenu dans A.

C'est évident pour $i = 0$: on a vu que les nombres constructibles forment un sous-corps de $\mathbb{C}$ et donc contiennent $\mathbb{Q}$.

Supposons que tous les éléments de L_i sont constructibles, d'après l'étude des extensions quadratiques il existe $\delta \in \mathrm{L}_{i+1} \smallsetminus \mathrm{L}_i$ tel que $\delta^2 \in \mathrm{L}_i$ et tout élément de L_{i+1} est alors de la forme $a + \delta b$ avec $a, b \in \mathrm{L}_i$. Ainsi, si δ est constructible, on aura démontré ce qu'on veut.

Il suffit donc de monter que si z^2 est constructible alors z l'est.

Calcul de racine carré

Écrivons $z = a + ib$ et $z^2 = \alpha + i\beta$. Par hypothèse, α et β sont des réels constructibles. On veut montrer que a et b le sont. On a $a^2 - b^2 = \alpha$ et $2ab = \beta$.

Si $\beta = 0$ alors $z = \pm i\sqrt{-\alpha}$ si $\alpha < 0$ ou $z = \pm\sqrt{\alpha}$. Ainsi si on montre que la racine carré d'un nombre réel positif constructible est constructible, on a terminé.

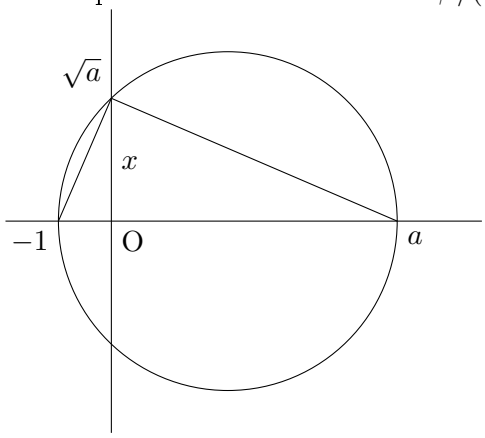
Si $\beta \neq 0$, on écrit $b = \beta/(2a)$ et donc

$$a^2 - \frac{\beta^2}{4a^2} = \alpha$$

c'est-à-dire $4a^4 - 4a^2\alpha - \beta^2 = 0$. On en déduit que $a^2 = \dfrac{\alpha \pm \sqrt{\alpha^2 + \beta^2}}{2}$. Le signe $-$ n'est pas possible car $a^2 \geqslant 0$ et $\beta \neq 0$. Et lorsqu'on met $+$, on obtient bien un nombre positif.

Ainsi $$a^2 = \frac{\alpha + \sqrt{\alpha^2 + \beta^2}}{2} \qquad \text{et} \qquad a = \sqrt{\frac{\alpha + \sqrt{\alpha^2 + \beta^2}}{2}}$$

Là encore, si on montre que la racine carré d'un nombre réel positif constructible est constructible, on aura a qui est constructible et $b = \beta/(2a)$ le sera aussi et finalement z le sera.



En appliquant trois fois le théorème de Pythagore, on a

$$(x^2 + 1) + (x^2 + a^2) = (a + 1)^2$$

et donc $x^2 = a$.

A $\subset$ B.

Pour commencer, on va montrer que B est un sous-corps de $\mathbb{C}$ vérifiant les propriétés suivantes

(i) B est stable par conjugaison

(ii) $i \in \mathrm{B}$

(iii) $z = x + iy \in \mathrm{B}$ si et seulement si $x, y \in \mathrm{B}$

(iv) B est stable par extension quadratique et en particulier par racine carré.

Preuve des propriétés.

(i) Si $\sigma : \mathbb{C} \to \mathbb{C}$ désigne la conjugaison complexe et si $\mathrm{L} \subset \mathrm{L}'$ sont deux sous-corps de $\mathbb{C}$, alors $\sigma(\mathrm{L})$ et $\sigma(\mathrm{L}')$ sont deux sous-corps de $\mathbb{C}$ vérifiant $\sigma(\mathrm{L}) \subset \sigma(\mathrm{L}')$ et $[\sigma(\mathrm{L}') : \sigma(\mathrm{L})] = [\mathrm{L}' : \mathrm{L}]$.

(ii) On a $i \in \mathbb{Q}(i)$ et $[\mathbb{Q}(i) : \mathbb{Q}] = 2$

(iii) Si $z \in \mathrm{B}$, alors $2x = z + \overline{z} \in \mathrm{B}$ et donc $x \in \mathrm{B}$ puis $iy \in \mathrm{B}$ et $y \in \mathrm{B}$ (puisque $i \in \mathrm{B}$). Inversement, cela résulte du fait que B est un corps contenant i.

(iv) Si z est dans une extension quadratique de B, on peut écrire $z = a + b\delta$ avec $a, b, \delta^2 \in \mathrm{B}$. On a alors $\mathrm{L}_0 = \mathbb{Q} \subset \mathrm{L}_1 \subset \cdots \subset \mathrm{L}_n$ avec $[\mathrm{L}_{i+1} : \mathrm{L}_i] = 2$ et $\delta^2 \in \mathrm{L}_n$. On étend la tour d'extension en $\mathrm{L}_0 = \mathbb{Q} \subset \mathrm{L}_1 \subset \cdots \subset \mathrm{L}_n \subset \mathrm{L}_{n+1} = \mathrm{L}_n(\delta)$ avec $[\mathrm{L}_{i+1} : \mathrm{L}_i] = 2$. Ainsi $\delta \in \mathrm{B}$ et donc $a + \delta b$ aussi.

B est un corps.

Lemme 120 Soit K un corps, E, F deux sous-corps de K et k un sous-corps de $\mathrm{E} \cap \mathrm{F}$. Soit F(E) la sous-F-extension de K engendrée par E. On suppose que E est algébrique sur k. Alors

$$[\mathrm{F(E)} : \mathrm{F}] \leqslant [\mathrm{E} : k]$$

Preuve. Par définition, F(E) est le plus petit sous-corps de K contenant E et F. Ces éléments sont de la forme

$$\frac{\sum_{i=1}^{n} f_i e_i}{\sum_{j=1}^{m} f_j e_j}.$$

Comme E est algébrique sur k, tout élément de E est algébrique sur F et donc $\sum_{j=1}^{n} f_j e_j$ est algébrique sur F. Or pour un élément algébrique x, l'inverse de x est un polynôme en x (puisque $x^{-1} \in k(x) = k[x]$.)

On en déduit qu'un élément de EF se met sous la forme $\sum_{\ell=1}^{s} f_\ell e_\ell$.

Grâce à cette écriture, on voit que si $(y_i)_{i\in \mathrm{I}}$ est une k-base de E alors $(y_i)_{i\in \mathrm{I}}$ est une famille F-génératrice de E sur F : on écrit $e_\ell = \sum_i \lambda_{i\ell} y_i$ et

$$\sum_{\ell=1}^{s} f_\ell e_\ell = \sum_i \left(\sum_{\ell=1}^{s} f_\ell \lambda_{i\ell} \right) y_i .$$

Démonstration du fait que B est un corps.

Pour $z, z' \in \mathrm{B}$, on a deux suites

$$\mathrm{L}_0 = \mathbb{Q} \subset \mathrm{L}_1 \subset \cdots \subset \mathrm{L}_n \quad \text{avec} \quad [\mathrm{L}_{i+1} : \mathrm{L}_i] = 2$$

et $z \in \mathrm{L}_n$ et

$$\mathrm{L}'_0 = \mathbb{Q} \subset \mathrm{L}'_1 \subset \cdots \subset \mathrm{L}'_m \quad \text{avec} \quad [\mathrm{L}'_{i+1} : \mathrm{L}'_i] = 2$$

et $z' \in \mathrm{L}'_m$.

On considère alors la suite

$$\mathrm{L}_0 = \mathbb{Q} \subset \mathrm{L}_1 \subset \cdots \subset \mathrm{L}_n \subset \mathrm{L}_n(\mathrm{L}'_1) \subset \cdots \subset \mathrm{L}_n(\mathrm{L}'_m)$$

D'après le lemme, $[\mathrm{L}_n(\mathrm{L}'_{i+1}) : \mathrm{L}_n(\mathrm{L}'_i)] \leqslant 2$ et donc en éliminant les facteurs égaux dans la deuxième partie de la liste, on obtient une suite d'extension quadratique qui contient z et z' et donc $z - z'$ et zz' et z^{-1}. De plus, on a $\mathbb{Q} \subset \mathrm{B}$ et on obtient le résultat souhaité.

Récurrence.

Pour conclure, il reste à montrer que $\mathrm{A} \subset \mathrm{B}$.

Montrons par récurrence sur ℓ qu'un nombre constructible en ℓ pas est dans B. Pour $\ell = 1$, les nombres constructibles sont $0, 1, 2, -1, \exp(i\pi/3)$ et $\exp(-i\pi/3)$. Mais $\exp(i\pi/3)$ et $\exp(-i\pi/3)$ sont racines de $\mathrm{X}^2 - \mathrm{X} + 1 \in \mathbb{Q}[\mathrm{X}]$ et donc dans B.

Supposons que pour tout $j < \ell$, les nombres constructible en j pas sont dans B. Et soit z constructible en ℓ pas. Par définition, il existe $z_1, \ldots, z_\ell = z$ tel que z_ℓ est obtenu soit comme l'intersection de deux droites contenant deux des points de $\mathrm{S} = \{0, 1, z_1, \ldots, z_{\ell-1}\}$, soit comme l'intersection d'une droite contenant deux des points de S et d'un cercle centré en un point de S et passant par un point de S soit comme l'intersection de deux cercles centré en des points de S et passant par des points de S. Or par hypothèse, les points de S sont dans B.

Conclusion.

Ainsi, si on montre que les coefficients de l'équation d'une droite passant par deux points de S sont dans B et que les coefficients de l'équation d'un cercle centré en S et passant par un point de S sont dans B, la remarque préliminaire assurera que les abscisses et ordonnées de z sont dans B et donc z est dans B.

Soit $z = a + ib$ et $z' = a' + ib'$, l'équation de (zz') est

$$(b-b')(x-a')-(a-a')(y-b')=0.$$

L'équation du cercle de centre z passant par z' est

$$(x-a)^2+(y-b)^2-(a-a')^2-(b-b')^2=0$$

Problèmes historiques

Corollaire 121 – Degré d'un élément constructible. Soit $z \in \mathbb{C}$ constructible alors $[\mathbb{Q}(z):\mathbb{Q}]$ est une puissance de 2.

Preuve. Comme $z \in \mathrm{B}$, il existe une suite strictement croissante de sous-corps de $\mathbb{C}$ vérifiant $[\mathrm{L}_{i+1} : \mathrm{L}_i] = 2$ telle que $\mathrm{L}_0 = \mathbb{Q} \subset \mathrm{L}_1 \subset \cdots \subset \mathrm{L}_n$, et $z \in \mathrm{L}_n$.

Par multiplicativité des degrés, on a

$$[\mathrm{L}_n : \mathbb{Q}] = 2^n = [\mathrm{L}_n : \mathbb{Q}(z)][\mathbb{Q}(z) : \mathbb{Q}]\,.$$

Corollaire 122 – Duplication du cube. La duplication du cube est impossible à la règle et au compas.

Preuve. $\sqrt[3]{2}$ est de degré 3 sur $\mathbb{Q}$

Corollaire 123 – Quadrature du cercle. La quadrature et la rectification du cercle ne sont pas réalisable à la règle et au compas

Preuve. Il s'agit de savoir si $\sqrt{\pi}$ et π sont constructibles. Or ils sont transcendants (on a vu que π l'est, si $\sqrt{\pi}$ était algébrique alors $\sqrt{\pi}^2$ le serait aussi).

Définition 124 – Angle constructible. L'angle θ est dit constructible si $\exp(i\theta)$ l'est.

Exemple 125 $\pi/3$ est constructible.

Corollaire 126 L'angle $\pi/3$ n'est pas trisectable à la règle et au compas : $\pi/9$ n'est pas constructible à la règle et au compas.

Preuve. Comme $\sin(2\pi/9) = \sqrt{1-\cos^2(2\pi/9)}$, on a $\exp(2i\pi/9)$ constructible si et seulement si $\cos(2\pi/9)$ l'est.

Or on a $4\cos^3(\theta) - 3\cos(\theta) = \cos(3\theta)$ et donc

$\cos(2\pi/9)$ est racine de $\mathrm{P} = 4\mathrm{X}^3 - 3\mathrm{X} - 1/2$ qui est irréductible sur $\mathbb{Q}$.

Démo1. Il suffit de montrer que P n'a pas de racine dans $\mathbb{Q}$. Si p/q est racine de P avec p et q premiers entre eux, alors en réduisant au même dénominateur, on obtient $8p^3 - 6pq^2 - q^3 = 0$. Ainsi $q \mid 8$ et $p \mid 1$. Il suffit donc de tester les valeurs $\pm 1, \pm 1/2, \pm 1/4, \pm 1/8$.

Démo2. Le polynôme $8\mathrm{X}^3 - 6\mathrm{X} - 1$ n'a pas de racine dans $\mathbb{F}_5$ (on étudie les 5 valeurs de x, ça en fait moins que les 32 précédentes). Il est donc irréductible sur $\mathbb{F}_5$ et donc $8\mathrm{X}^3 - 6\mathrm{X} - 1$ l'est sur $\mathbb{Z}$ (puisqu'il est primitif).

Polygones constructibles

Définition 127 Un polygone régulier à n côtés est dit constructible si $\exp(2i\pi/n)$ l'est.

Pour quelles valeurs de n, un polygone régulier à n côtés est-il constructible ?

Remarque 128 Si le polygone régulier à n côtés est constructible alors pour tout diviseur d de n, le polygone régulier à d côtés est constructible.

En effet, si $n = dm$ avec $\exp(2i\pi/n)^m = \exp(2i\pi/d)$ est constructible à la règle et au compas.

Remarque 129 Si le polygone régulier à n côtés est constructible, celui à $2n$ côtés l'est aussi.

En effet, on a vu que si z^2 est constructible alors z l'est. Or $\exp(2i\pi/2n)^2 = \exp(2i\pi/n)$.

Les remarques précédentes assurent que si m est un nombre impair alors le polygone régulier à m côtés est constructible si et seulement si pour tout ℓ, le polygone régulier à $2^\ell m$ côtés est constructible.

Plus généralement, on a le lemme suivant

Lemme 130 Soient m et n premiers entre eux. Le polygone à mn côtés est constructible si et seulement si le polygone à n côtés et le polygone à m côtés sont constructibles.

Preuve. Le sens direct provient de la première remarque.

Pour la réciproque, il existe u, v tel que $mu + nv = 1$. On a donc,

$$\exp(2i\pi/n)^u \exp(2i\pi/m)^v = \exp(2i\pi(um + nv)/mn) = \exp(2i\pi/mn).$$

Soit $\mathrm{N} = 2^n {p_1}^{\alpha_1} \cdots {p_r}^{\alpha_r}$ avec $p_i \neq 2$ premiers et $p_i \neq p_j$ si $i \neq j$. D'après ce qui précède, on obtient le polygone à N côtés est constructibles si et seulement si pour tout i le polygone à ${p_i}^{\alpha_i}$ côtés est constructibles.

Ainsi pour p premier, il s'agit de déterminer quand $\exp(2i\pi/p^\alpha)$ est constructible.

Proposition 131 Pour tout p premier et tout $\alpha \in \mathbb{N}^*$, le polynôme minimal de $\exp(2i\pi/p^\alpha)$ sur $\mathbb{Q}$ est

$$\Phi_{p^\alpha} = \mathrm{X}^{p^{\alpha-1}(p-1)} + \mathrm{X}^{p^{\alpha-1}(p-2)} + \cdots + \mathrm{X}^{p^{\alpha-1}} + 1 = \mathrm{Q}(\mathrm{X}^{p^\alpha})$$

où $\mathrm{Q} = 1 + \mathrm{X} + \cdots + \mathrm{X}^{p-1}$.

En particulier, $[\mathbb{Q}(\exp(2i\pi/p^\alpha)) : \mathbb{Q}] = p^{\alpha-1}(p-1)$.

Preuve. Posons $z = \exp(2i\pi/p^\alpha)$. On a

$$\Phi_{p^\alpha}(z) = \frac{(z^{p^{\alpha-1}})^p - 1}{z^{p^{\alpha-1}} - 1} = \frac{z^{p^\alpha} - 1}{z^{p^{\alpha-1}} - 1} = 0$$

Il suffit donc de montrer que Φ_{p^α} est irréductible pour conclure. Or un polynôme P est irréductible si et seulement si $\mathrm{P}(\mathrm{X}+1)$ est irréductible.

On va appliquer le critère d'Eisenstein au polynôme $\mathrm{R} = \Phi_{p^\alpha}(\mathrm{X}+1)$ avec l'élément premier p. On a évidemment $\mathrm{R}(0) = \Phi_{p^\alpha}(1) = p$ qui n'est pas divisible par p^2 et le coefficient dominant n'est pas divisible par p. Il s'agit donc de montrer que tous les autres coefficients sont divisibles par p.

Pour cela, on considère le morphisme d'anneaux $\Delta : \mathbb{Z}[\mathrm{X}] \to \mathbb{F}_p[\mathrm{X}]$ qui consiste à réduire tous les coefficients modulo p. On a $\Delta(\mathrm{R}) = (\Delta(\Phi_{p^\alpha}))(\mathrm{X}+1)$.

Calculons $\Delta(\Phi_{p^\alpha})$. Grâce au morphisme de Frobenius, on obtient

$$\Delta(\Phi_{p^\alpha}) = (\mathrm{X}^{p-1} + \cdots + 1)^{p^{\alpha-1}}.$$

Or $(\mathrm{X}-1)(\mathrm{X}^{p-1} + \cdots + 1) = \mathrm{X}^p - 1 = (\mathrm{X}-1)^p$ toujours grâce au morphisme de Frobenius. Ainsi, $\mathrm{X}^{p-1} + \cdots + 1 = (\mathrm{X}-1)^{p-1}$ et donc

$$\Delta(\Phi_{p^\alpha}) = (\mathrm{X}-1)^{(p-1)p^{\alpha-1}}$$

Finalement $\Delta(\mathrm{R}) = \mathrm{X}^{(p-1)p^{\alpha-1}}$ ce qui donne le résultat souhaité.

Un premier bilan.

Soit p un nombre premier impair. Pour qu'un polygone à p^α côtés soit constructible, il faut que $p^{\alpha-1}(p-1)$ soit une puissance de 2. Cela impose que $\alpha = 1$ et que $p = 1 + 2^m$.

On peut même être plus précis, si $1 + 2^m$ est premier alors m est une puissance de 2. En effet, si m n'est pas une puissance de 2, on peut écrire $m = 2^\ell j$ avec $j > 1$ et j impair et

$$1 + 2^m = (1 + 2^\ell)(1 - 2^\ell + 2^{2\ell} - \cdots + 2^{\ell(j-1)}))$$

qui est une factorisation non triviale si $j \neq 1$.

Finalement, pour qu'un polygone à p^α côtés soit constructible, il faut que $\alpha = 1$ et p soit un nombre premier de Fermat c'est-à-dire que la forme $\mathrm{F}_n = 2^{2^n} + 1$.

Attention, tous les F_n ne sont pas des nombres premiers. Par exemple F_5 ne l'est pas : il est divisible par 641. Les seuls nombres de Fermat premier qu'on connaissent sont les $\mathrm{F}_0, \mathrm{F}_1, \mathrm{F}_2, \mathrm{F}_3$ et F_4. On ne sait rien sur F_{33}. On sait factoriser $\mathrm{F}_5, \ldots, \mathrm{F}_{11}$, on sait que F_{12} n'est pas premier mais on en connaît aucun facteur premier. On sait que $\mathrm{F}_{12}, \ldots, \mathrm{F}_{32}$ sont factorisables. On ne sait pas si F_{33} est premier ou non.

Bilan : polygone constructible.

Pour qu'un polygone à $\mathrm{N} = 2^n {p_1}^{\alpha_1} \cdots {p_s}^{\alpha_s}$ (avec p_i premier et $p_i \neq p_j$ si $i \neq j$) soit constructible, il faut que $\alpha_1 = \cdots = \alpha_s = 1$ et p_i soit un nombre de Fermat.

La réciproque est vraie : c'est un théorème dû à Gauss.

2.7 Cyclotomie

Définition 132 Cyclotomie = étude des racines de l'unité dans un corps.

Notation 133 Soit k un corps, on définit $\mu_n(k) = \{x \in k, \quad x^n = 1\}$ (c'est un sous-groupe de k^*) et $\mu_n^\circ(k) = \{x \in k^* \text{ d'ordre } n\} \subset \mu_n(k)$.

Les éléments de $\mu_n(k)$ sont appelés les racines n^{e} de l'unité.

Les éléments de $\mu_n^\circ(k)$ sont appelés les racines n^{e} primitives de l'unité.

Proposition 134 – Cardinal. On a $|\mu_n(k)| \leqslant n$.

Si $\mu_n^\circ(k) \neq \varnothing$ alors $|\mu_n(k)| = n$.

Preuve. Les éléments de $\mu_n(k)$ sont les racines dans k du polynôme $\mathrm{X}^n - 1$. Le résultat tombe alors du lemme suivant.

Si $x \in \mu_n^\circ(k)$ alors les x^j sont distincts pour $0 \leqslant j \leqslant n-1$ et vérifient $(x^j)^n = (x^n)^j = 1^j = 1$. Ainsi $|\mu_n(k)| \geqslant n$.

Lemme 135 Soit A un anneau intègre, $\mathrm{P} \in \mathrm{A}[\mathrm{X}]$ et $a_1, \ldots, a_r \in \mathrm{A}$ tel que $a_i \neq a_j$ si $i \neq j$. On suppose que P vérifie $\mathrm{P}(a_i) = 0$ pour tout i alors $\mathrm{P} = 0$ ou $\deg \mathrm{P} \geqslant r$.

Preuve. On raisonne par récurrence sur r. Pour $r = 0$, c'est bon. Supposons le résultat vrai pour tout ensemble $\{a_1, \ldots, a_r\}$ de A à r éléments et tout polynôme $\mathrm{P} \in \mathrm{A}[\mathrm{X}]$.

Considérons $\{a_1, \ldots, a_{r+1}\}$ et P vérifie $\mathrm{P}(a_i) = 0$ pour tout i. En particulier, on a $\mathrm{P}(a_1) = 0$ et donc on peut écrire $\mathrm{P} = (\mathrm{X} - a_1)\mathrm{R}$ avec $\mathrm{R} \in \mathrm{A}[\mathrm{X}]$ (division euclidienne par $\mathrm{X} - a_1$ qui est unitaire, le reste est $\mathrm{P}(a_1)$).

Par intégrité de A, on a $\mathrm{R}(a_i) = 0$ pour tout $i \geqslant 2$ puisque $(a_i - a_1) \neq 0$. L'hypothèse de récurrence assure que $\mathrm{R} = 0$ (et donc $\mathrm{P} = 0$) ou $\deg \mathrm{R} \geqslant r$ (et donc $\deg \mathrm{P} \geqslant r + 1$ car A est intègre).

Sous-groupe fini de k^*.

Proposition 136 Soit k un corps et G un sous-groupe fini de k^*. Alors G est cyclique. De plus, si n est l'ordre de G alors $\mathrm{G} = \mu_n(k)$.

On a besoin du lemme suivant :

Lemme 137 Soit G un groupe abélien fini d'ordre n. Les propositions suivantes sont équivalentes

(i) G est cyclique

(ii) Pour tout $d \mid n$, il existe un unique sous-groupe d'ordre d dans G

(iii) Pour tout $d \mid n$, il existe au plus un sous-groupe d'ordre d dans G

Preuve. $(i) \Rightarrow (ii)$. On a $\mathrm{G} \overset{\text{gr.}}{\simeq} \mathbb{Z}/n\mathbb{Z}$. Les sous-groupes de $\mathbb{Z}/n\mathbb{Z}$ sont en bijection avec les sous-groupes de $\mathbb{Z}$ contenant $n\mathbb{Z}$ c'est-à-dire avec les $d\mathbb{Z}$ pour $d \mid n$. L'implication $(ii) \Rightarrow (iii)$ est évidente. $(iii) \Rightarrow (i)$. On note H_d le sous-groupe de G d'ordre d s'il existe et on note G_d l'ensemble des éléments d'ordre d de G. Par le théorème de Lagrange, on a $\mathrm{G} = \bigsqcup_{d \mid n} \mathrm{G}_d$. **(1)**

Si $\mathrm{G}_d \neq \varnothing$ et $x \in \mathrm{G}_d$, on a $\langle x \rangle_{\text{gr.}}$ est un sous-groupe d'ordre d et donc est H_d qui est donc cyclique d'ordre d. On en déduit que $|\mathrm{G}_d| \geqslant \phi(d)$ (tous les x^j pour $j \wedge d = 1$ sont dans G_d). Mais si $x' \in \mathrm{G}_d$, on a par unicité $\langle x \rangle_{\text{gr.}} = \langle x' \rangle_{\text{gr.}}$ et donc $x' = x^j$ pour un certain j vérifiant $j \wedge d = 1$. Ainsi si $\mathrm{G}_d \neq \varnothing$ alors $|\mathrm{G}_d| = \phi(d)$.

On a donc $|\mathrm{G}_d| = \mu_d$ avec $\mu_d = 0$ ou $\mu_d = \phi(d)$.

On en déduit de **(1)** alors que $n = \sum_{d \mid n} \mu_d$. Par ailleurs, on a $n = \sum_{d \mid n} \phi(d)$. On en déduit que pour tout d, $\mu_d = \phi(d)$ et donc $\mu_n = \phi(n) \neq 0$. Ainsi G admet un élément d'ordre n.

Preuve de la proposition.

Preuve. Montrons que G a au plus un sous-groupe d'ordre d. Considérons H un sous-groupe d'ordre d. D'après le théorème de Lagrange, tout élément de H est dans $\mu_d(k)$. Comme $|\mu_d(k)| \leqslant d$, on en déduit que $\mathrm{H} = \mu_d(k)$. Ainsi G est cyclique d'ordre n. Il admet donc un élément x d'ordre n qui est dans $\mu_n^\circ(k)$ et donc $\mathrm{G} = \langle x \rangle = \mu_n(k)$.

Exercice 34 Pour $k = \mathbb{Q}, \mathbb{R}, \mathbb{C}$, déterminer $\mu_n(k)$ et les valeurs de n pour lesquelles on a $\mu_n^\circ(k) \neq \varnothing$.

Soit k un corps. Montrer que $|\mu_n^\circ(k)| = 0$ ou $\phi(n)$.

L'équivalence suivante est elle vraie ? $x \in \mu_n^\circ(k)$ si et seulement si x engendre $\mu_n(k)$.

Soit k un corps de caractéristique p. Montrer que $\mu_n(k) = \mu_{np^\ell}(k)$ pour tout ℓ. En déduire que si n est divisible par p alors $\mu_n^\circ(k) = \varnothing$.

2.8 Corps de rupture, corps de décomposition, clôture algébrique

Racines d'un polynôme à coefficients dans un corps.

$$\begin{tikzcd}
 & \mathrm{P} \in k[\mathrm{X}] \arrow[dl] \arrow[dr] & \\
\text{où sont les racines ?} \arrow[d] & & \text{combien ai-je de racines ?} \arrow[d] \\
\text{polynômes scindés} \arrow[d] & & \text{racines multiples} \arrow[d] \\
\text{extension normale} \arrow[dr] & & \text{extension séparable} \arrow[dl] \\
 & \text{extension galoisienne} &
\end{tikzcd}$$

Corps de rupture

Corps de rupture : problématique

Le polynôme $\mathrm{X}^2+1 \in \mathbb{R}[\mathrm{X}]$ n'a pas de racine dans $\mathbb{R}$. Pour remédier à ce problème, on crée le corps $\mathbb{C} := \mathbb{R}[\mathrm{X}]/(\mathrm{X}^2+1)$. Sur $\mathbb{C}$, le polynôme T^2+1 a une racine qui est la classe de X.

Soit $\mathrm{P} \in k[\mathrm{X}]$ un polynôme. Peut-on trouver un corps (une extension de k) dans lequel P a une racine ? Dans quelle mesure, une telle extension est-elle unique ?

Si P n'est pas irréductible, on écrit $\mathrm{P} = \mathrm{P}_1\mathrm{P}_2$ avec $\mathrm{P}_1, \mathrm{P}_2$ non inversible. Il suffit de trouver une racine de P_1 ou de P_2. Ainsi, en continuant la factorisation, il suffit de trouver des racines aux polynômes irréductibles sur k. Cette même factorisation en irréductibles montre que si P n'est pas irréductible, il n'y a aucune chance d'obtenir une quelconque propriété d'unicité du corps dans lequel P a une racine. Par exemple, sur $\mathbb{R}$, avec $\mathrm{P} = \mathrm{X}(\mathrm{X}^2+1)$, $\mathbb{R}$ et $\mathbb{C}$ sont deux corps dans lesquels P admet une racine. De même, si on n'impose pas un propriété de minimalité de l'extension cherchée, aucune chance d'avoir unicité : les extensions $\mathbb{Q}(\sqrt{2})$ et $\mathbb{C}$ contiennent des racines de $\mathrm{P} = \mathrm{X}^2 - 2$.

Corps de rupture : solution

Définition 138 — Corps de rupture. Soit $\mathrm{P} \in k[\mathrm{X}]$ un polynôme **irréductible**. Un **corps de rupture sur** k pour P est un triplet (K, i, a) où (K, i) est une extension de k et $a \in \mathrm{K}$ vérifiant $\mathrm{P}(a) = 0$ et $\mathrm{K} = k(a)$.

Proposition 139 — Existence, unicité et propriété universelle. Soit $\mathrm{P} \in k[\mathrm{X}]$ un polynôme **irréductible**. Il existe un corps de rupture pour P : $k[\mathrm{X}]/\mathrm{P}$ en est un.

Par ailleurs, soit (K, i, a) un corps de rupture pour P et considérons (L, j) une extension de k et $b \in \mathrm{L}$ vérifiant $\mathrm{P}(b) = 0$. Il existe un unique morphisme d'extensions σ de (K, i) dans (L, j) vérifiant $\sigma(a) = b$.

Soit (K, i, a) et (L, j, b) deux corps de rupture pour P. Il existe un unique isomorphisme d'extensions σ de (K, i) dans (L, j) vérifiant $\sigma(a) = b$.

Le degré d'un corps de rupture est donc bien défini et c'est le degré du polynôme. Un corps de rupture de P est isomorphe à $k[\mathrm{X}]/\mathrm{P}$.

Preuve. $k[\mathrm{X}]/\mathrm{P}$ **est un corps de rupture.** On note $\pi : k[\mathrm{X}] \to k[\mathrm{X}]/(\mathrm{P})$ la surjection canonique et $j : k \to k[\mathrm{X}]$ l'injection usuelle. Le morphisme $\pi \circ j : k \to k[\mathrm{X}]/\mathrm{P}$ munit $k[\mathrm{X}]/(\mathrm{P})$ d'une structure de k-algèbre. Cette k-algèbre est engendrée par $x := \pi(\mathrm{X})$ (puisque $k[\mathrm{X}]$ est déjà engendré par X). De plus, si on pose $\mathrm{A} = k[\mathrm{X}]/(\mathrm{P})$ et $\mathrm{P} \in \mathrm{A}[\mathrm{T}]$, alors x est une racine de P dans A. En effet, on a $\mathrm{P}(x) = \mathrm{P}(\pi(\mathrm{X})) = \pi(\mathrm{P}(\mathrm{X})) = 0$. La deuxième relation résultant du fait que π est un morphisme de k-algèbres : si $\mathrm{P} = \lambda_0 + \lambda_1\mathrm{T} + \cdots + \lambda_n\mathrm{T}^n$ alors

$$\begin{aligned}
\pi(\mathrm{P}(\mathrm{X})) &= \pi(\lambda_0) + \pi(\lambda_1\mathrm{X}) + \cdots + \pi(\lambda_n\mathrm{X}^n) \\
&= \lambda_0\pi(1) + \lambda_1\pi(\mathrm{X}) + \cdots + \lambda_n\pi(\mathrm{X})^n
\end{aligned}$$

$k[X]/P$ **est un corps.** La seule chose qu'il reste à montrer est que $k[X]/(P)$ est bien un corps. Soit $\pi(Q)$ non nul dans $k[X]/(P)$. On a donc $P \nmid Q$. Mais P est **irréductible** (il faut bien que cette hypothèse serve), donc P et Q sont premiers entre eux. Ainsi il existe $U, V \in k[X]$ tel que $UP+QV = 1$. En appliquant π, on obtient $\pi(U)\pi(P) + \pi(V)\pi(Q) = 1$ et donc $\pi(V)\pi(Q) = 1$ c'est-à-dire que $\pi(Q)$ est inversible dans $k[X]/(P)$.

Remarque 140 – au passage.... L'un des intérêts de l'identité de Bézout est de pouvoir inverser dans des quotients...

Propriété universelle des corps de fractions. Comme $K = k(a)$ est la k-extension engendrée par a, s'il existe un morphisme σ d'extensions de K dans L tel que $\sigma(a) = b$ alors il n'y en a pas d'autres (σ et σ' coïncideraient sur une famille génératrice). Il reste à montrer l'existence de σ. Comme $K = k(a) = k[a]$ (puisque a est algébrique sur k), tout élément de K s'écrit sous la forme $Q(a)$ pour un certain $Q \in k[T]$. Si σ existe, on a alors si $Q = \lambda_0 + \lambda_1 T + \cdots + \lambda_n T^n$:

$$\begin{aligned}\sigma(Q(a)) &= \sigma(\lambda_0) + \sigma(\lambda_1 a) + \cdots + \sigma(\lambda_n a^n) \\ &= \lambda_0 + \lambda_1\sigma(a) + \cdots + \lambda_n\sigma(a)^n \\ &= Q(\sigma(a)) = Q(b)\end{aligned} \qquad \star$$

On **doit** donc poser $\sigma(Q(a)) = Q(b)$. Le problème est qu'on peut avoir $Q(a) = R(a)$ avec $Q \neq R$. A-t-on alors bien $Q(b) = R(b)$?

σ est bien défini. Si $Q(a) = R(a)$ alors $Q - R$ annule a. Ainsi $Q - R$ est divisible par le polynôme minimal π_a de a. Mais P est irréductible et annule a, il est donc proportionnel à π_a. On a donc $P \mid Q-R$: il existe $U \in k[T]$ tel que $PU = Q - R$. En évaluant en b, on a alors $0 = P(b)U(b) = Q(b) - R(b)$ et σ est bien défini.

« Unicité » du corps de rupture. D'après la propriété universelle des corps de rupture appliquée à K et L, il existe $\varphi : K \to L$ et $\psi : L \to K$ deux morphismes d'extensions vérifiant $\varphi(a) = b$ et $\psi(b) = a$. Ainsi $\psi \circ \varphi : K \to K$ et $\varphi \circ \psi : L \to L$ deux morphismes d'extensions et ils vérifient $\psi \circ \varphi(a) = a$ et $\varphi \circ \psi(b) = b$. Mais $\mathrm{id}_K : K \to K$ et $\mathrm{id}_L : L \to L$ sont deux morphismes d'extensions vérifiant $\mathrm{id}_K(a) = a$ et $\mathrm{id}_L(b) = b$. L'unicité dans la propriété universelle des corps de rupture assure que $\psi \circ \varphi = \mathrm{id}_K$ et $\varphi \circ \psi = \mathrm{id}_L$. ■

Exemples

Considérons le polynôme $X^3 - 2$ sur $\mathbb{Q}$. Il est bien irréductible. On connaît 4 « versions » du corps de rupture de $X^3 - 2$ sur $\mathbb{Q}$.

(*i*) Le classique $\mathbb{Q}[X]/(X^3-2)$ dont l'élément distingué est x l'image de X par la surjection canonique.
(*ii*) $\mathbb{Q}(\sqrt[3]{2})$ dont l'élément distingué est $\sqrt[3]{2}$.
(*iii*) $\mathbb{Q}(j\sqrt[3]{2})$ dont l'élément distingué est $j\sqrt[3]{2}$.
(*iv*) $\mathbb{Q}(j^2\sqrt[3]{2})$ dont l'élément distingué est $j\sqrt[3]{2}$.

Ces 4 corps sont bien sûr isomorphes et même plus précisément, on peut trouver par exemple un isomorphisme du premier sur le deuxième qui envoie x sur $\sqrt[3]{2}$.

Corps de rupture : exercices

Exercice 35 Soient k un corps et K une extension de k de la forme $K = k(a)$ avec a algébrique sur K. Montrer que K est un corps de rupture pour le polynôme minimal de a. En déduire qu'une extension finie de k est un corps de rupture si et seulement si elle est monogène.

Soit L une extension de k. Montrer que l'application

$$\begin{cases} \mathrm{Hom}_{k-\mathsf{alg.}}(K, L) \longrightarrow \{x \in L, \quad P(x) = 0\} \\ \qquad \sigma \qquad\qquad \longmapsto \sigma(a) \end{cases}$$

est une bijection.

Exercice 36 Quel est « le » corps de rupture de X^2+1 sur $\mathbb{R}$, $\mathbb{Q}$, $\mathbb{C}$, $\mathbb{Q}(i)$, $\mathbb{Q}(\sqrt{2})$? Les questions posées ont-elles un sens ?

Corps de décomposition.

Corps de décomposition : problématique.

Étant donné un polynôme P à coefficients dans k, on sait construire une extension de k dans lequel P a une racine.

On cherche maintenant à agrandir encore le corps pour scinder le polynôme P : existe-t-il une extension de k dans laquelle P est scindé. Dans quelle mesure une telle extension est-elle unique ?

Bien entendu, une extension d'une extension dans laquelle P est scindé est encore une extension dans laquelle P est scindé. Ainsi, on ne peut espérer de résultats d'unicité qu'en demandant des propriétés de minimalité sur l'extension dans laquelle P est scindé.

Corps de décomposition : solution

Définition 141 – Corps de décomposition. Soit $\mathrm{P} \in k[\mathrm{X}]$ un polynôme. Un **corps de décomposition de P sur** k est une extension (K, i) dans laquelle P est scindé (P est produit de polynômes de degré 1) et $\mathrm{K} = k(x_1, \ldots, x_n)$ où $x_1, \ldots, x_n$ sont les racines de P dans K.

Définition 142 – Corps de décomposition. soit $(\mathrm{P}_i)_{i\in \mathrm{I}}$ une famille d'éléments de $k[\mathrm{X}]$. Un **corps de décomposition de la famille** $(\mathrm{P}_i)_i$ **sur** k est une extension (K, i) dans laquelle tous les P_i sont scindés et K est engendrée (en tant que k-extension) par les racines de tous les P_i (notées $x_1^{(i)}, \ldots, x_{\ell_i}^{(i)}$) : $\mathrm{K} = k(x_j^{(i)},\ j = 1, \ldots, \ell_i,\ i \in \mathrm{I})$

Existence et unicité du corps de décomposition. **Proposition 143** Pour tout $\mathrm{P} \in k[\mathrm{X}]$, il existe un corps de décomposition de P sur k.

Si (K, i) est un corps de décomposition de P sur k et (L, j) une extension de k dans laquelle P est scindé alors il existe un morphisme d'extensions $\sigma : \mathrm{K} \to \mathrm{L}$

Si (K, i) et (K', j) sont deux corps de décomposition de P sur k, il existe $\sigma : \mathrm{K} \to \mathrm{K}'$ un isomorphisme d'extensions de (K, i) dans (K', j).

Preuve. Idée de la preuve de l'existence on rajoute une racine x par un corps de rupture, puis on recommence avec $\mathrm{P}/(\mathrm{X} - x) \in k(x)$ et ainsi de suite, on construit ainsi un corps dans lequel P est scindé. Il n'y a plus qu'à considérer la sous-extension engendrée par les racines.

Preuve de l'existence. On va montrer le résultat par récurrence sur $n = \deg \mathrm{P}$. On fait l'hypothèse de récurrence suivante H_n : pour tout k, pour tout $\mathrm{P} \in k[\mathrm{X}]$ de degré inférieur ou égal à n, il existe un corps de décomposition de P sur k.

Si $n = 0$ alors $\mathrm{K} = k$ convient. Supposons H_n vraie et considérons $\deg \mathrm{P} = n + 1$.

Si P n'est pas irréductible, on peut écrire $\mathrm{P} = \mathrm{P}_1\mathrm{P}_2$ avec $\deg \mathrm{P}_1 < n + 1$ et $\deg \mathrm{P}_2 < n + 1$. On considère alors (grâce à l'hypothèse de récurrence) K le corps de décomposition de P_1 sur k et L le corps de décomposition de P_2 sur K : on a P_1 qui est scindé dans K et $\mathrm{K} = k(x_1, \ldots, x_s)$ où les x_i sont les racines de P_1 dans K : et P_2 qui est scindé dans L et $\mathrm{L} = \mathrm{K}(y_1, \ldots, y_r)$ où les y_i sont les racines de P_2 dans L.

On a alors P_1 qui est évidemment scindé dans L et donc P est scindé dans L et les racines de P sont $x_1, \ldots, x_s, y_1, \ldots, y_r$. De plus, $\mathrm{L} = k(x_1, \ldots, x_s)(y_1, \ldots, y_r) = k(x_1, \ldots, x_s, y_1, \ldots, y_r)$: L est un corps de décomposition de P sur k.

Si P est irréductible, on considère $k(x)$ un corps de rupture de P sur k. Dans $k(x)[\mathrm{X}]$, on a $\mathrm{X} - x \mid \mathrm{P}$ et on écrit $\mathrm{P} = (\mathrm{X} - x)\mathrm{Q}$ avec $\mathrm{Q} \in k(x)[\mathrm{X}]$. On a $\deg \mathrm{Q} = n$.

On considère alors K le corps de décomposition de Q sur $k(x)$ (grâce à l'hypothèse de récurrence) : Q est scindé dans K et $\mathrm{K} = k(x)(x_1, \ldots, x_s) = k(x, x_1, \ldots, x_s)$ où $x_1, \ldots, x_s$ sont les racines de Q dans K.

Ainsi P est scindé dans K, ses racines sont $x, x_1, \ldots, x_s$: K est un corps de décomposition de P sur k.

Construction de morphismes.

On va montrer le résultat par récurrence sur $n = \deg \mathrm{P}$. On fait l'hypothèse de récurrence suivante H_n : pour tout k, pour tout $\mathrm{P} \in k[\mathrm{X}]$ de degré inférieur ou égal à n, pour tout (K, i) corps de décomposition de P sur k et pour toute extension (L, j) de k dans laquelle P est scindée, il existe $\sigma : \mathrm{K} \to \mathrm{L}$ morphisme d'extensions.

Pour $n = 0$, on a $\mathrm{K} = k$ et $\sigma = j$ convient. Supposons H_n vraie et considérons $\deg \mathrm{P} = n + 1$.

Si P n'est pas irréductible, on peut écrire $\mathrm{P} = \mathrm{P}_1\mathrm{P}_2$ avec $\deg \mathrm{P}_1 < n+1$ et $\deg \mathrm{P}_2 < n+1$. Comme P est scindé dans K, on a alors P_1 et P_2 qui sont scindés dans K. On note alors $x_1, \ldots, x_s, y_1, \ldots, y_r$ les racines de P où $x_1, \ldots, x_s$ sont les racines de P_1 et $y_1, \ldots, y_r$ les racines de P_2.

On pose $K' = k(x_1, \ldots, x_s)$, c'est un corps de décomposition de P_1 sur k. On note alors $i = i'' \circ i'$ où $i' : k \to K'$ et $i'' : K' \to K$. Comme P_1 est aussi scindé dans L, l'hypothèse de récurrence assure qu'il existe $\sigma' : K' \to L$ un morphisme d'extensions : $\sigma' \circ i' = j$. En particulier, L est une extension de K'.

Par ailleurs, on a $K = k(x_1, \ldots, x_s, y_1, \ldots, y_r) = K'(y_1, \ldots, y_r)$ et P_2 est scindé dans K : ainsi K est un corps de décomposition de P_2 sur K'. Comme P_2 est scindé dans L, il existe $\sigma : K \to L$ tel que $\sigma \circ i'' = \sigma'$. En composant par i', on obtient bien $\sigma \circ i = j$.

On suppose que P est irréductible. On note $x_1, \ldots, x_s$ les racines de P dans K. On pose $K' = k(x_1)$ qui est un corps de rupture de P sur k. On note $i = i'' \circ i'$ avec $i' : k \to k(x_1)$ et $i'' : k(x_1) \to K$.

Comme P est scindé dans L, il a en particulier une racine x. D'après la propriété universelle du corps de rupture, il existe $\sigma' : k(x_1) \to L$ morphisme d'extensions tel que $\sigma'(x_1) = x$. En particulier, $\sigma' \circ i' = j$ et L est une extension de $k(x_1)$.

Par ailleurs, on a $K = k(x_1)(x_2, \ldots, x_s)$. En posant $P = (X - x_1)Q$ avec $Q \in k(x_1)[X]$, on a Q qui est scindé dans K et $x_2, \ldots, x_s$ qui sont les racines de Q dans K. Ainsi K est un corps de décomposition de Q sur $k(x_1)$. De plus, Q est évidemment scindé dans L et donc, d'après l'hypothèse de récurrence, il existe $\sigma : K \to L$ tel que $\sigma \circ i'' = \sigma'$.

Isomorphisme entre deux corps de rupture.

Soient K, K' deux corps de décomposition de P sur k.

Comme P est scindé dans K' et K corps de décomposition de P sur k, il existe $\sigma : K \to K'$ morphisme d'extensions qui est donc injectif. En particulier $[K' : k] \geqslant [K : k]$.

De même, comme P est scindé dans K et K' corps de décomposition de P sur k, il existe $\sigma' : K' \to K$ morphisme d'extensions. Donc $[K : k] \geqslant [K' : k]$.

Ainsi $[K : k] = [K' : k]$. Comme K est de dimension finie sur k (puisqu'engendrée par un nombre fini d'éléments algébriques), on en déduit que σ est un isomorphisme. ■

Attention ! Il n'y a absolument pas unicité du morphisme σ construit, sinon il n'y aurait pas de théorie de Galois.

Exemples

Exemple 144 — $X^3 - 2$ sur $\mathbb{Q}$. Le polynôme $X^3 - 2 \in \mathbb{Q}[X]$ a pour corps de décomposition sur $\mathbb{Q}$: $\mathbb{Q}(\sqrt[3]{2}, j\sqrt[3]{2}, j^2\sqrt[3]{2}) = \mathbb{Q}(\sqrt[3]{2}, j)$ qui est de degré 6 sur $\mathbb{Q}$.

En effet, $X^3 - 2$ est irréductible sur $\mathbb{Q}$ donc $[\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = 3$. De plus, $j \notin \mathbb{Q}(\sqrt[3]{2}) \subset \mathbb{R}$ et $j^2 + j + 1 = 0$. Donc $[\mathbb{Q}(\sqrt[3]{2}, j) : \mathbb{Q}(\sqrt[3]{2})] = 2$.

Ainsi $\mathbb{Q}(\sqrt[3]{2}, j)$ contient trois corps de rupture de $X^3 - 2$ sur $\mathbb{Q}$.

Exemple 145 — Polynôme de degré 2. Soient $P = X^2 + aX + b \in k[X]$ un polynôme irréductible de degré 2. Un corps de rupture K de P est un corps de décomposition de P. En effet, K est bien évidemment engendré par les racines de P dans K puisqu'il est engendré par l'une d'elles. Il suffit donc de montrer que P est scindé dans K. Mais si x est une racine de P dans K alors $a - x$ est aussi dans K et est l'autre racine de P.

Corps de décomposition : exercices.

Exercice 37 Reprendre la démonstration de l'existence du corps du rupture pour montrer que le degré du corps d'un polynôme de degré n divise $n!$.

Exercice 38 — Une autre propriété d'unicité pour les corps de décomposition. Soit $P \in k[X]$ et K une extension de k dans laquelle P est scindé. Montrer qu'il existe un unique sous-corps de K qui est un corps de décomposition de P sur k.

A-t-on un résultat analogue pour les corps de rupture ?

Corps algébriquement clos

Proposition 146 Soit k un corps. Les propositions suivantes sont équivalentes

(i) Tout polynôme non constant à coefficients dans k admet une racine dans k

(ii) Les éléments irréductibles de $k[X]$ sont les polynômes de degré 1

(iii) Tout polynôme non constant est produit de polynômes de degré 1

(iv) Si (K, i) est une extension algébrique de k alors i est un isomorphisme.

Un corps vérifiant ces propriétés est dit **algébriquement clos**. Par exemple, $\mathbb{C}$ est algébriquement clos.

Définition 147 Soit k un corps. Une **clôture algébrique de** k est une extension (K, i) de k où K est algébriquement clos et (K, i) est algébrique sur k. $\mathbb{C}$ est une clôture algébrique de $\mathbb{R}$ mais pas de $\mathbb{Q}$.

Preuve. $(i) \Rightarrow (ii)$. Si P est irréductible alors P est non constant donc il admet une racine a. Donc P est divisible par $\mathrm{X} - a$. Par irréductibilité de P, on a $\mathrm{P} = \lambda(\mathrm{X} - a)$ qui est de degré 1.

$(ii) \Rightarrow (iii)$. C'est la factorialité de $k[\mathrm{X}]$.

$(iii) \Rightarrow (i)$. C'est évident

$(ii) \Rightarrow (iv)$. On note x un élément de K. Son polynôme minimal est irréductible sur k et donc de degré 1. Ainsi $x \in \mathrm{K}$.

$(iv) \Rightarrow (ii)$. Soit P irréductible, l'extension $k[\mathrm{X}]/(\mathrm{P})$ est algébrique, donc de degré 1. Ainsi $\deg \mathrm{P} = 1$.

Clôture algébrique

Proposition 148 Soient K un corps algébriquement clos et k un sous-corps de K. La fermeture algébrique L de k dans K est une clôture algébrique de k.

Par exemple, $\overline{\mathbb{Q}} = \{x \in \mathbb{C}, \quad x \text{ algébrique sur } \mathbb{Q}\}$ est une clôture algébrique de $\mathbb{Q}$ et $\mathbb{C}$ n'est pas une clôture algébrique de $\mathbb{Q}$.

Preuve. L est évidemment algébrique sur k. Il s'agit de montrer que L est algébriquement clos.

Soit $\mathrm{P} \in \mathrm{L}[\mathrm{X}]$ non constant. Comme K est algébriquement clos, P a une racine x dans K. Ainsi x est algébrique sur L et donc sur k par transitivité. Finalement $x \in \mathrm{L}$ puisque L est la fermeture algébrique de k dans K. Tout polynôme non constant a donc une racine dans L.

Plongement dans un corps algébriquement clos.

Lemme 149 — Théorème de plongement. Soient (K, i) une extension **algébrique** de k et (K', j) une extension algébriquement close de k. Alors il existe un morphisme de (K, i) dans (K', j).

Preuve. On considère l'ensemble

$$\mathrm{C} = \{(\mathrm{L}, \sigma), \quad \mathrm{L} \text{ sous-extension de K et } \sigma : \mathrm{L} \to \mathrm{K}' \text{ morphisme d'extensions}\}$$

que l'on ordonne en posant $(\mathrm{L}, \sigma) \leqslant (\mathrm{L}', \sigma')$ si $\mathrm{L} \subset \mathrm{L}'$ et $\sigma'_{|\mathrm{L}} = \sigma$ (vérifier que c'est bien un ensemble ordonné).

C est un ensemble inductif : tout sous-ensemble totalement ordonné admet un majorant. En effet si $\mathrm{Y} = (\mathrm{L}_i, \sigma_i), i \in \mathrm{I}$ est un sous-ensemble totalement ordonné. On pose $\mathrm{L} = \cup_i \mathrm{L}_i$. C'est bien une sous-extension (grâce au fait que la relation d'ordre est totale sur Y). On pose alors $\sigma(x) = \sigma_i(x)$ si $x \in \mathrm{L}_i$ (σ est bien défini grâce au fait que la relation d'ordre est totale sur Y). Alors (L, σ) est bien un majorant de la famille des (L_i, σ_i).

Le lemme de Zorn assure qu'il existe (L, σ) maximal pour l'ordre. Montrons que $\mathrm{L} = \mathrm{K}$ et on aura construit le morphisme souhaité.

Sinon, il existe $x \in \mathrm{K} \setminus \mathrm{L}$ qui est donc algébrique sur L. Soit P son polynôme minimal. Comme K′ est une extension de L (via σ) et que K′ est algébriquement clos, P a une racine dans K′. Il existe donc $\sigma' : \mathrm{L}(x) \to \mathrm{K}$ un morphisme de L-extensions (PU des corps de rupture) qui est donc un morphisme de k-extensions. Cela contredit la maximalité de L.

Clôtures algébriques isomorphes.

Corollaire 150 Soient (K, i) et (K', j) deux clôtures algébriques de k. Alors les extensions (K, i) et (K', j) sont isomorphes.

Preuve. Comme K est algébrique sur k et K′ algébriquement close, il existe $\sigma : \mathrm{K} \to \mathrm{K}'$ morphisme d'extensions. De même, il existe $\sigma' : \mathrm{K}' \to \mathrm{K}$ morphisme d'extensions. Ils sont bien sûr tous les deux injectifs.

On a alors $\sigma' \circ \sigma : \mathrm{K} \to \mathrm{K}$ qui est un endomorphisme de l'extension algébrique K. Si nous montrons que $\sigma' \circ \sigma$ est un automorphisme, on obtient que σ' est surjectif et donc un isomorphisme.

Il s'agit donc de montrer qu'un endomorphisme τ d'une extension algébrique L est forcément un automorphisme. τ est évidemment injectif. Il s'agit de montrer sa surjectivité. Soit $x \in \mathrm{L}$ et π_x son polynôme minimal sur k. On note $\mathrm{X} = \{x_1 = x, \ldots, x_r\}$ l'ensemble des racines de π_x dans L (c'est évidemment un ensemble fini). Or τ envoie X dans lui-même (calcul $\star$) de façon injective. Comme X est fini, τ est une bijection sur X et x est dans l'image de τ.

Existence des clôtures algébriques

Proposition 151 — Théorème de Steinitz. Tout corps admet une clôture algébrique.

Corollaire 152 Soit k un corps et $(\mathrm{P}_i)_{i\in\mathrm{I}}$ une famille de polynôme de $k[\mathrm{X}]$. Alors la famille $(\mathrm{P}_i)_{i\in\mathrm{I}}$ admet un corps de décomposition.

Preuve. Il suffit de considérer la k-extension engendrée par les racines de tous les P_i dans une clôture algébrique de k.

Preuve du théorème de Steinitz

Preuve. On commence par construire K_1 une extension de $k = \mathrm{K}_0$ dans laquelle tout polynôme non constant à coefficients dans k a une racine. On recommence cette même construction à partir de K_1 et on obtient K_2 et ainsi de suite : on construit K_{n+1} à partir de K_n de telle sorte que tout polynôme non constant à coefficients dans K_n ait une racine dans K_{n+1}.

On pose alors $\mathrm{K} = \cup_n \mathrm{K}_n$ qui est bien un corps contenant k puisque les K_n forment une suite croissante.

L'extension K est algébriquement close. En effet, si $\mathrm{P} \in \mathrm{K}[\mathrm{X}]$ non constant alors il existe n tel que $\mathrm{P} \in \mathrm{K}_n[\mathrm{X}]$ et P a donc une racine dans $\mathrm{K}_{n+1} \subset \mathrm{K}$.

On considère alors l'ensemble des éléments algébriques sur k de K pour obtenir une clôture algébrique de k.

Construction de K_1.

On considère $\mathscr{P}$ la famille des polynômes non constant à coefficients dans k. Pour chaque $\mathrm{P} \in \mathscr{P}$, on considère une indéterminée X_P et on construit l'anneau de polynômes à une infinité d'indéterminées : $\mathrm{A} := k[\mathrm{X}_\mathrm{P}, \mathrm{P} \in \mathscr{P}]$.

On considère alors l'idéal $\mathrm{I} := \langle \mathrm{P}(\mathrm{X}_\mathrm{P}), \mathrm{P} \in \mathscr{P} \rangle$. Montrons que cet idéal n'est pas A tout entier.

Si c'était le cas, il existerait $\mathrm{Q}_1, \ldots, \mathrm{Q}_n$ tel que

$$\mathrm{Q}_1\mathrm{P}_1(\mathrm{X}_{\mathrm{P}_1}) + \cdots + \mathrm{Q}_n\mathrm{P}_n(\mathrm{X}_{\mathrm{P}_n}) = 1\,.$$

On considère alors L le corps de décomposition de $\mathrm{P}_1 \cdots \mathrm{P}_n$ et le morphisme φ de k-algèbres de A dans L donné par $\varphi(\mathrm{X}_{\mathrm{P}_i}) = x_i$ où x_i est une racine de P_i dans L et $\varphi(\mathrm{X}_\mathrm{P}) = 0$ pour $\mathrm{P} \neq \mathrm{P}_i$. On obtient une contradiction.

Ainsi I est contenu dans un idéal maximal $\mathfrak{m}$. Alors $\mathrm{A}/\mathfrak{m}$ est une extension de k et la classe de X_P dans le quotient est une racine de P... ■

Exercices.

Exercice 39 Démontrer le théorème de prolongement sans utiliser le lemme de Zorn lorsque $[\mathrm{K} : k] < +\infty$.

Exercice 40 Soient k un corps et (K, i) une extension algébrique de k. Montrer que k et K ont même clôture algébrique.

Exercice 41 — Une autre vision des corps de décomposition. À l'aide du théorème de Steinitz, démontrer le théorème d'existence et d'unicité des corps de décomposition d'un polynôme.

Soit k un corps et $(\mathrm{P}_i)_{i\in\mathrm{I}}$ une famille de polynôme de $k[\mathrm{X}]$. Démontrer que si L est une extension dans laquelle tous les P_i sont scindés et si K est un corps de décomposition des $(\mathrm{P}_i)_{i\in\mathrm{I}}$ alors il existe $\sigma : \mathrm{K} \to \mathrm{L}$ un morphisme d'extensions (adapter la preuve du théorème de plongement). Démontrer que deux corps de décompositions de la famille $(\mathrm{P}_i)_i$ sont isomorphes (adapter la preuve de l'isomorphisme des clôtures algébriques).

2.9 Multiplicité des racines.

Définition 153 Soit k un corps et $\mathrm{P} \in k[\mathrm{X}]$. On a définit la multiplicité d'une racine a de P dans le cours sur les anneaux factoriels comme la multiplicité de $(\mathrm{X}-a)$ dans P c'est-à-dire le plus grand entier n tel que $(\mathrm{X}-a)^n \mid \mathrm{P}$.

On dit que a est une racine simple si sa multiplicité est 1 et une racine multiple si sa multiplicité est supérieure ou égale à 2.

MULTIPLICITÉ ET DÉRIVATION.

Proposition 154 Soit k un corps et $\mathrm{P} \in k[\mathrm{X}]$. Les proposition suivantes sont équivalentes :

(i) P et P′ sont premiers entre eux dans $k[\mathrm{X}]$.
(ii) Il existe une extension K de k tel que P et P′ sont premiers entre eux dans K[X].
(iii) Pour toute extension K de k, P et P′ sont premiers entre eux dans K[X].
(iv) Pour toute extension K de k, P et P′ sont sans racine commune dans K.
(v) P n'a que des racines simples dans toute extension K de k.
(vi) Il existe une extension K de k dans laquelle P est scindé à racines simples.
(vii) P est à racines simples dans son corps de décomposition.
($viii$) P est à racines simples dans une extension algébriquement close de k.

Un premier lemme.

Lemme 155 – Le pgcd est indépendant du corps. Soit k un corps, $\mathrm{P}, \mathrm{Q} \in k[\mathrm{X}]$ et K une extension de k. On note R_k (resp. R_K) le pgcd unitaire de P et Q considérés comme polynômes à coefficients dans k (resp. K). On a $\mathrm{R}_k = \mathrm{R}_\mathrm{K}$.

Preuve. *Première démo.* On applique l'algorithme d'Euclide pour le calcul du pgcd dans K[X]. Tous les calculs ont lieu en fait dans $k[\mathrm{X}]$, ainsi, on est en fait en train d'effectuer l'algorithme d'Euclide dans $k[\mathrm{X}]$. On a ainsi $\mathrm{R}_k = \mathrm{R}_\mathrm{K}$.

Deuxième démo. On a R_k divise P et Q dans $k[\mathrm{X}]$ donc dans K[X]. Ainsi $\mathrm{R}_k \mid \mathrm{R}_\mathrm{K}$ dans K[X]. Inversement, grâce à la relation de Bézout, on peut écrire $\mathrm{R}_k = \mathrm{UP} + \mathrm{VQ}$ avec $\mathrm{U}, \mathrm{V} \in k[\mathrm{X}]$. Mais on a $\mathrm{P} = \mathrm{R}_\mathrm{K}\mathrm{S}$ et $\mathrm{Q} = \mathrm{R}_\mathrm{K}\mathrm{T}$ avec $\mathrm{S}, \mathrm{T} \in \mathrm{K}[\mathrm{X}]$, on a donc $\mathrm{R}_k = \mathrm{R}_\mathrm{K}(\mathrm{US} + \mathrm{VT})$ et $\mathrm{R}_\mathrm{K} \mid \mathrm{R}_k$ dans K[X] et donc $\mathrm{R}_\mathrm{K} = \mathrm{R}_k$ (puisqu'ils sont tous les deux unitaires).

Un deuxième lemme.

Lemme 156 – Racine multiple $\Longrightarrow$ racine commune. Soit $\mathrm{P} \in k[\mathrm{X}]$ ayant une racine multiple a de multiplicité m. Alors $(\mathrm{X}-a)^{m-1} \mid \mathrm{pgcd}(\mathrm{P}, \mathrm{P}')$. En particulier, a est une racine commune de P et P′.

Preuve. On a $\mathrm{P} = (\mathrm{X}-a)^m\mathrm{Q}$ avec $m \geqslant 2$ et $\mathrm{Q}(a) \neq 0$. On a alors $\mathrm{P}' = m(\mathrm{X}-a)^{m-1}\mathrm{Q} + (\mathrm{X}-a)^m\mathrm{Q}' = (\mathrm{X}-a)^{m-1}(m\mathrm{Q} + (\mathrm{X}-a)\mathrm{Q}')$.

Remarque 157 En caractéristique p et si $p \mid m$, on a même $(\mathrm{X}-a)^m \mid \mathrm{pgcd}(\mathrm{P}, \mathrm{P}')$ et le degré de multiplicité de a ne diminue pas dans la dérivée.

Un troisième (et dernier ?) lemme.

Lemme 158 – racine commune $\Longrightarrow$ racine multiple. Si a est une racine commune de P et P′ alors a est une racine multiple de P.

Preuve. Soit $m \geqslant 1$ la multiplicité de a dans P. On écrit $\mathrm{P} = (\mathrm{X}-a)^m\mathrm{Q}$ avec $\mathrm{Q}(a) \neq 0$. On a alors $\mathrm{P}' = (\mathrm{X}-a)^{m-1}(m\mathrm{Q} + (\mathrm{X}-a)\mathrm{Q}')$. Si $m = 1$, on en déduit que $\mathrm{P}' = (\mathrm{Q} + (\mathrm{X}-a)\mathrm{Q}')$. En particulier, $\mathrm{P}'(a) = \mathrm{Q}(a) \neq 0$. NON.

Preuve de la proposition.

Preuve. (i) $\Leftrightarrow$ (ii) et (ii) $\Leftrightarrow$ (iii). C'est le premier lemme. (iv) $\Rightarrow$ (v). C'est le deuxième lemme.
(iii) $\Rightarrow$ (iv). Si a est une racine commune de P et P′ dans K alors $(\mathrm{X}-a)$ divise $\mathrm{pgcd}(\mathrm{P}, \mathrm{P}')$.
(v) $\Rightarrow$ ($viii$). C'est juste le fait qu'il existe une extension algébriquement close de k.
($viii$) $\Rightarrow$ (vii). Une extension algébriquement close de k contient toujours un corps de décomposition de $\mathrm{P} \in k[\mathrm{X}]$.

$(vii) \Rightarrow (vi)$. Le corps de décomposition convient

$(vi) \Rightarrow (ii)$. On écrit $\mathrm{P} = \prod_{j=1}^{r} (\mathrm{X} - a_j)$ avec $a_j \in \mathrm{K}$ et $a_i \neq a_j$ si $i \neq j$. Un diviseur de P est alors de la forme $\prod_{j \in \mathrm{I}} (\mathrm{X} - a_j)$ où I est une partie de $\{1, \ldots, r\}$. En particulier, $\mathrm{pgcd}(\mathrm{P}, \mathrm{P}')$ est de cette forme-là pour un certain I, si I n'est pas vide alors pour $j \in \mathrm{I}$, a_j est une racine commune à P et P'.

Le troisième lemme assure que c'est impossible puisque P est à racine simple. Ainsi I est vide et $\mathrm{pgcd}(\mathrm{P}, \mathrm{P}') = 1$.

MULTIPLICITÉ ET POLYNÔMES IRRÉDUCTIBLES

Définition 159 Soit k un corps et $\mathrm{P} \in k[\mathrm{X}]$. Un polynôme **irréductible** vérifiant les propriétés équivalentes de la proposition est appelé polynôme **séparable**.

Proposition 160 Soit k un corps et $\mathrm{P} \in k[\mathrm{X}]$ irréductible. Les propriétés suivantes sont équivalentes

(i) P est séparable

(ii) Il existe une extension de k dans laquelle P admet une racine simple

(iii) $\mathrm{P}' \neq 0$

(iv) $\mathrm{car}\, k = 0$ ou ($\mathrm{car}\, k = p$ et $\mathrm{P} \notin k[\mathrm{X}^p]$).

Preuve. $(i) \Rightarrow (ii)$. C'est la proposition précédente.
$(iv) \Leftrightarrow (iii)$. On écrit $\mathrm{P} = a_0 + a_1\mathrm{X} + \cdots + a_n\mathrm{X}^n$. Si $\mathrm{P}' = 0$, on a $ia_i = 0$ pour tout $i \in \mathbb{N}$. En particulier, si $\mathrm{car}\, k = 0$, on obtient $a_i = 0$ pour tout $i \neq 0$ et donc P est constant (NON car P est irréductible). Si $\mathrm{car}\, k = p$, on obtient que $a_i = 0$ pour tout i tel que $p \mid i$: on peut écrire $\mathrm{P} = a_0 + a_p\mathrm{X}^p + a_{2p}\mathrm{X}^{2p} + \cdots + a_{\ell p}\mathrm{X}^{\ell p}$. Ainsi $\mathrm{P} \in k[\mathrm{X}^p]$.
$(iii) \Leftrightarrow (i)$. Comme P est irréductible, les diviseurs de P sont 1 ou P. On a $\mathrm{pgcd}(\mathrm{P}, \mathrm{P}') = 1$ ou $\mathrm{pgcd}(\mathrm{P}, \mathrm{P}') = \mathrm{P}$. Comme $\deg \mathrm{P}' < \deg \mathrm{P}$, on a $\mathrm{pgcd}(\mathrm{P}, \mathrm{P}') = \mathrm{P}$ si et seulement si $\mathrm{P}' = 0$.
$(ii) \Rightarrow (i)$. Comme P est irréductible, les diviseurs de P sont 1 ou P. On a $\mathrm{pgcd}(\mathrm{P}, \mathrm{P}') = 1$ ou $\mathrm{pgcd}(\mathrm{P}, \mathrm{P}') = \mathrm{P}$. Mais a n'est pas racine de P' donc $\mathrm{X} - a \nmid \mathrm{P}'$ et donc $\mathrm{P} \nmid \mathrm{P}'$ et $\mathrm{pgcd}(\mathrm{P}, \mathrm{P}') \neq \mathrm{P}$.

2.10 Corps finis

Soit k un corps fini (c'est-à-dire de cardinal fini). Sa caractéristique est nécessairement un nombre premier p (sinon, il « contiendrait $\mathbb{Q}$ » est serait de cardinal infini). Ainsi k est une extension de $\mathbb{F}_p$. Comme les éléments de k forment une famille génératrice de k sur $\mathbb{F}_p$, $1 \leqslant n = [k : \mathbb{F}_p] < +\infty$.

On en déduit que k est un espace vectoriel de dimension finie sur $\mathbb{F}_p$. Ainsi $|k| = p^n$.

Pour tout p et tout $n \in \mathbb{N}^*$, existe-t-il un corps de cardinal p^n ? Peut-on décrire à isomorphisme près tous les corps de cardinal p^n ?

EXISTENCE ET UNICITÉ

Proposition 161 — Existence et unicité des corps finis. Soit p un nombre premier et $n \in \mathbb{N}^*$.

Il existe un corps de cardinal p^n, c'est un corps de décomposition de $\mathrm{X}^{p^n} - \mathrm{X}$ sur $\mathbb{F}_p$. Deux corps de cardinal p^n sont isomorphes.

Pour désigner « le » corps à p^n éléments, on utilise la notation $\mathbb{F}_{p^n}$.

Attention, $\mathbb{F}_{p^n} \neq \mathbb{Z}/p^n\mathbb{Z}$.

Preuve. Preuve : unicité Soit K un corps à p^n éléments. Un élément x non nul de K vérifie $x^{p^n-1} = 1$ d'après le théorème de Lagrange dans le groupe $\mathrm{K}^\times$ qui est d'ordre $p^n - 1$. Ainsi x est racine de $\mathrm{X}^{p^n} - \mathrm{X}$. Par ailleurs, 0 est évidemment racine de $\mathrm{X}^{p^n} - \mathrm{X}$. Ainsi tous les éléments de K sont racines de $\mathrm{X}^{p^n} - \mathrm{X}$. Le polynôme $\mathrm{X}^{p^n} - \mathrm{X}$ a donc p^n racines distinctes. Il est donc scindé dans K et K est évidemment engendré par les racines de $\mathrm{X}^{p^n} - \mathrm{X}$ sur $\mathbb{F}_p$. Ainsi K est un corps de décomposition de $\mathrm{X}^{p^n} - \mathrm{X}$ sur $\mathbb{F}_p$. On en déduit le fait que deux corps à p^n éléments sont isomorphes (puisque deux corps de décomposition d'un même polynôme sont isomorphes).

Preuve : existence Soit K un corps de décomposition de $\mathrm{X}^{p^n} - \mathrm{X}$ sur $\mathbb{F}_p$. On va montrer que les racines de $\mathrm{X}^{p^n} - \mathrm{X}$ forment un sous-corps de K et donc que K est exactement l'ensemble des racines de $\mathrm{X}^{p^n} - \mathrm{X}$.

$0, 1$ sont évidemment racines de $X^{p^n} - X$. Si x, y sont racines de $X^{p^n} - X$. On a alors $(x-y)^{p^n} = x^{p^n} - y^{p^n}$ (par le morphisme de Frobenius itéré n fois) et donc $(x-y)^{p^n} = x - y$. De même, on a $(xy)^{p^n} = x^{p^n} y^{p^n} = xy$.

Les racines de $X^{p^n} - X$ forment donc un sous-corps de K. Mais K est le corps de décomposition de $X^{p^n} - X$ donc K est l'ensemble des racines de $X^{p^n} - X$.

Ainsi K a au plus p^n éléments. Pour conclure que K a exactement p^n élément et assurer l'existence d'un corps à p^n éléments, il reste à montrer que $X^{p^n} - X$ qui est scindé dans K est à racines simples dans K. On a $(X^{p^n} - X)' = p^n X^{p^n - 1} - 1 = -1$ qui est évidemment premier avec $X^{p^n} - X$.

Un exemple d'isomorphisme

Exercice 42 Montrer que $\mathbb{F}_2[X]/\langle X^3 + X + 1\rangle$ et $\mathbb{F}_2[X]/\langle X^3 + X^2 + 1\rangle$ sont des corps, qu'ils sont isomorphes et donner un isomorphisme explicite entre ces deux corps.

GROUPE MULTIPLICATIF D'UN CORPS FINI

Lemme 162 Soient k un corps (commutatif) et G un sous-groupe fini de $k^\times$ alors G est cyclique.

Corollaire 163 Si k est un corps fini alors $k^\times$ est cyclique.

Corollaire 164 Les corps finis sont des corps de rupture sur $\mathbb{F}_p$.

Preuve. Soit K un corps fini et x un générateur de $K^\times$. On a alors $\mathbb{F}_p(x) \subset K$. Mais bien sûr comme x est un générateur de $K^\times$, on a $K^\times \subset \mathbb{F}_p(x)$ et $0 \in \mathbb{F}_p(x)$. Donc $K = \mathbb{F}_p(x)$.

On en déduit que K est le corps de rupture du polynôme minimal P de x sur $\mathbb{F}_p$. En particulier, $K \simeq \mathbb{F}_p[X]/P$.

Corollaire 165 Pour tout $n \in \mathbb{N}^*$, il existe un polynôme irréductible de degré n sur $\mathbb{F}_p$.

Preuve. D'après ce qui précède, on a $\mathbb{F}_{p^n} \simeq \mathbb{F}_p[X]/P$ où P est irréductible sur $\mathbb{F}_p$. En comparant les dimensions sur $\mathbb{F}_p$, on obtient $n = \deg P$.

CARRÉ DANS LES CORPS FINIS

Proposition 166 Soit k un corps à p^n éléments (avec p premier et $n \in \mathbb{N}^*$). On note

$$k^{\times 2} = \left\{x \in k^\times,\ \exists y \in k,\ x = y^2\right\}$$

Si $p = 2$ alors $k^{\times 2} = k^\times$.

Si $p \neq 2$ alors $k^{\times 2}$ est un sous-groupe d'indice 2 de $k^\times$ et $x \in k^{\times 2}$ si et seulement si $x^{(p^n-1)/2} = 1$. En particulier, -1 est un carré dans k si et seulement si $p^n = 1[4]$.

Preuve. Preuve 1 : Lagrange + un polynôme n'a pas plus de racines que son degré. On considère le morphisme de groupes

$$\square : \begin{cases} k^\times \longrightarrow k^\times \\ x \longmapsto x^2 \end{cases}$$

Par définition, l'image est $k^{\times 2}$. Comme $\operatorname{Im}\square \overset{\text{gr.}}{\simeq} k^\times/\operatorname{Ker}\square$, il suffit de déterminer le cardinal de $\operatorname{Ker}\square$ pour obtenir le nombre d'éléments de $k^{\times 2}$.

Preuve 1 :

Calculons $\operatorname{Ker}\square$: on cherche à déterminer les éléments tels que $x^2 = 1$.

Si $p = 2$ alors, par le morphisme de Frobenius, on a $x^2 = 1 \iff (x-1)^2 = 0 \iff x = 1$. Ainsi $\square$ est injectif et donc surjectif.

Si p est impair, on a alors $-1 \neq 1$ qui sont racines de $X^2 - 1$. Or ce polynôme a au plus deux racines dans k. Ainsi $\operatorname{Ker}\square = \{-1, 1\}$. Et on a donc $(p^n - 1)/2$ carrés dans $k^\times$.

Montrons maintenant la caractérisation de l'ensemble des carrés dans k. Si $x = y^2$ est un carré, on a alors $x^{(p^n-1)/2} = y^{p^n-1}$. En appliquant le théorème de Lagrange dans $k^\times$, on obtient que $y^{p^n-1} = 1$ et donc x est racine de $X^{(p^n-1)/2} - 1$ (on peut aussi montrer cette propriété de la façon suivante : l'ensemble des carrés est un sous-groupe de $k^\times$ de cardinal $(p^n - 1)/2$ et on applique le théorème de Lagrange à ce groupe).

Inversement, le polynôme $X^{(p^n-1)/2}-1$ a $(p^n-1)/2$ racines distinctes qui sont les carrés. Comme il est de degré $(p^n-1)/2$, il n'en a pas d'autres.

Ainsi -1 est un carré dans k si et seulement si $-1^{(p^n-1)/2}=1$ c'est-à-dire $(p^n-1)/2$ est pair c'est-à-dire $p^n=1[4]$.

Preuve 2 : groupe cyclique.

Lemme 167 Soit G un groupe cyclique de cardinal ℓ noté additivement et $m\in\mathbb{N}$. Le morphisme de groupes

$$[\times m]\colon \begin{cases} G \longrightarrow G \\ x \longmapsto mx \end{cases}$$

a pour image $\operatorname{Im}[\times m]=\operatorname{Im}[\times \operatorname{pgcd}(\ell,m)]=\operatorname{Ker}[\times \ell/\operatorname{pgcd}(\ell,m)]$ dont le cardinal est $\ell/\operatorname{pgcd}(\ell,m)$; et pour noyau $\operatorname{Ker}[\times m]=\operatorname{Ker}[\times \operatorname{pgcd}(\ell,m)]=\operatorname{Im}[\times \ell/\operatorname{pgcd}(\ell,m)]$ dont le cardinal est $\operatorname{pgcd}(\ell,m)$.

Preuve. Preuve du lemme On écrit une relation de Bézout : $mu+\ell v=\operatorname{pgcd}(m,\ell)$ et $\operatorname{pgcd}(m,\ell)d=m$. On a alors $y=mx=\operatorname{pgcd}(m,\ell)dx\in\operatorname{Im}[\times\operatorname{pgcd}(m,\ell)]$. Si $y=\operatorname{pgcd}(m,\ell)x$ alors $y=(mu+\ell v)x=m(ux)+v\ell x$ et $\ell x=0$ par le théorème de Lagrange. Ainsi $y=m(ux)\in\operatorname{Im}[\times m]$.

Si $y=\operatorname{pgcd}(m,\ell)x$ alors $\ell/\operatorname{pgcd}(m,\ell)y=\ell x=0$. Inversement, supposons $\ell/\operatorname{pgcd}(\ell,m)y=0$. On considère un générateur g de G. On écrit $y=rg$. On a alors $r\ell/\operatorname{pgcd}(\ell,m)g=0$ et donc $\ell\mid r\ell/\operatorname{pgcd}(\ell,m)$. Ainsi il existe t tel que $\ell t=r\ell/\operatorname{pgcd}(\ell,m)$ et donc $r=t\operatorname{pgcd}(\ell,m)$. Finalement, $y=\operatorname{pgcd}(\ell,m)(tg)$.

Si $mx=0$ alors $umx+v\ell x=0$ et donc $\operatorname{pgcd}(m,\ell)x=0$. Inversement, si $\operatorname{pgcd}(m,\ell)x=0$ alors $mx=d\operatorname{pgcd}(m,\ell)x=0$.

Si $y\in\operatorname{Im}[\times\operatorname{pgcd}(\ell,m)]$ alors $y=\operatorname{pgcd}(\ell,m)x=\operatorname{pgcd}(ell,m)sg$. Inversement, si $y\in\langle\operatorname{pgcd}(\ell,m)g\rangle$ alors $y=r\operatorname{pgcd}(\ell,m)g\in\operatorname{Im}[\times\operatorname{pgcd}(\ell,m)]$.

Et donc $\operatorname{Im}[\times\operatorname{pgcd}(\ell,m)]=\langle\operatorname{pgcd}(\ell,m)g\rangle$ qui a pour cardinal $\ell/\operatorname{pgcd}(\ell,m)$.

Preuve. Preuve 2.

Il n'y a plus qu'à appliquer le lemme au groupe cyclique $k^\times$ d'ordre p^n-1 et $m=2$. On a $\operatorname{pgcd}(p^n-1,2)=1$ si $p=2$ et $\operatorname{pgcd}(p^n-1,2)=2$ sinon.

Retour sur l'arithmétique

Exercice 43 Soient p un nombre premier impair, $n\in\mathbb{N}^*$ et $k=\mathbb{F}_{p^n}$. On considère $a,b\in k^\times$. Montrer que, pour tout $c\in k$, l'équation $ax^2+by^2=c$ d'inconnues (x,y) admet au moins une solution.

Application 168 Il existe une infinité de nombre premiers congrus à 1 modulo 4.

Preuve. Supposons qu'il n'en existe qu'un nombre fini $X=\{p_1,\dots,p_r\}$. On pose $N=(2p_1\cdots p_r)^2+1$. Soit p un diviseur premier de N. On a $p\notin X$ sinon $p\mid 1$. Par ailleurs, en réduisant modulo p l'égalité définissant N, on obtient $-1=(2p_1\cdots p_r)^2[p]$. En particulier, -1 est un carré modulo p et p est congru à 1 modulo 4 c'est-à-dire $p\in X$. NON.

SOUS-CORPS D'UN CORPS FINI

Proposition 169 – Sous-corps d'un corps fini. Soient p un nombre premier, $n\in\mathbb{N}^*$ et $k=\mathbb{F}_{p^n}$.

Soit k' un sous-corps de k alors $|k'|=p^m$ avec $m\mid n$. Inversement, pour tout $m\mid n$, k admet un unique sous-corps de cardinal $\mathbb{F}_{p^m}$.

De façon précise, le corps à p^m éléments contenu dans k est $k'=\left\{x\in k, x^{p^m}=x\right\}$.

Preuve. Si $k'\subset k$ alors k' est fini et a pour caractéristique p et donc $|k'|=p^m$. De plus, k peut être muni d'une structure de k'-espace vectoriel. En particulier, en choisissant une base de k en tant que k'-espace vectoriel, on a un isomorphisme de $k'^s \overset{k'\text{-ev.}}{\simeq} k$. Ainsi, en calculant le cardinal, on obtient $(p^m)^s=p^n$ et donc $ms=n$.

D'après ce qu'on a vu dans le théorème d'existence des corps finis, s'il existe un sous-corps k' de k de cardinal p^m alors k' est un corps de décomposition sur $\mathbb{F}_p$ de $X^{p^m}-X$ et est exactement formé des racines de ce polynôme. Il y a donc au plus un seul sous-corps de k à p^m éléments.

Pour conclure, il suffit maintenant de montrer que k contient un corps de décomposition de $X^{p^m}-X$ sur $\mathbb{F}_p$ ou de façon équivalente que $X^{p^m}-X$ est scindé dans k. Évidemment, il suffit de montrer que $X^{p^m-1}-1$ est scindé sur $\mathbb{F}_p$.

Mais $n = ms$ et donc $p^n - 1 = (p^m)^s - 1$ et donc $p^n - 1 = (p^m - 1)(1 + p^m + \cdots + p^{(s-1)m}) = (p^m - 1)r$.

$$\mathrm{X}^{p^n-1} - 1 = (\mathrm{X}^{p^m-1})^r - 1 = (\mathrm{X}^{p^m-1} - 1)(1 + \cdots + \mathrm{X}^{(r-1)(p^m-1)})$$

Ainsi, $(\mathrm{X}^{p^m-1} - 1)$ divise $\mathrm{X}^{p^n-1} - 1$ qui divise $\mathrm{X}^{p^n} - \mathrm{X}$ qui est scindé dans k. Donc $\mathrm{X}^{p^m} - \mathrm{X}$ est scindé dans k.

Exemples

Exemple 170 $\mathbb{F}_4$ n'est pas un sous-corps de $\mathbb{F}_8$ mais c'est un sous-corps de $\mathbb{F}_{16}$.

$\mathbb{F}_{64}$ a 4 sous-corps : $\mathbb{F}_{64}$, $\mathbb{F}_8$, $\mathbb{F}_4$, $\mathbb{F}_2$.

Remarque 171 Pour montrer que $\mathrm{X}^{p^m-1} - 1$ est scindé dans k, on aurait pu aussi invoquer le fait que $k^\times$ est un groupe cyclique et lemme sur le groupe cyclique démontré plus haut. En effet, $p^m - 1 \mid p^n - 1$ et donc les racines de $\mathrm{X}^{p^m-1} - 1$ qui sont les éléments de $\mathrm{Ker}\,[\times p^m - 1]$ sont au nombres de $\mathrm{pgcd}(p^m - 1, p^n - 1) = p^m - 1$.

AUTOMORPHISME D'UN CORPS FINI

Proposition 172 — Automorphisme. Soient p un nombre premier, $n \in \mathbb{N}^*$ et $k = \mathbb{F}_{p^n}$.

Les automorphismes du corps k forment un groupe cyclique d'ordre n engendré par le morphisme de Frobenius F.

Preuve. Le morphisme de Frobenius de k est injectif puisque c'est un morphisme d'anneaux qui part d'un corps. Comme k est fini, il est surjectif et donc c'est un automorphisme de k.

En particulier, tout élément de k est une puissance p^{e}. On retrouve le résultat de la proposition précédente lorsque $p = 2$.

Par ailleurs, on a vu que pour tout $x \in k$, on a $x^{p^n} = x$. Ainsi $\mathrm{F}^{\circ n} = \mathrm{id}_k$. Le groupe engendré par F est donc d'ordre au plus n. Par ailleurs, si $\mathrm{F}^{\circ d} = \mathrm{id}_k$, on a $x^{p^d} = x$ pour tout $x \in k$ ce qui implique par cardinalité que $p^d \geqslant |k| = p^n$ et donc $d \geqslant n$. Le groupe engendré par le Frobenius est donc bien d'ordre n.

Il reste à montrer qu'il n'y a pas d'autre automorphisme que les $\mathrm{F}^{\circ i}$ pour $0 \leqslant i \neq n - 1$.

On choisit x tel que $k = \mathbb{F}_p(x)$.

POLYNÔME IRRÉDUCTIBLE ET CORPS FINIS

Proposition 173 Soient p un nombre premier et $n \in \mathbb{N}^*$. On a la factorisation

$$\mathrm{X}^{p^n} - \mathrm{X} = \prod_{d \mid n} \prod_{\mathrm{P} \in \mu_d(p)} \mathrm{P}$$

où $\mu_d(p)$ désigne l'ensemble des polynômes **unitaires** de degré d irréductibles sur $\mathbb{F}_p$.

Preuve. On considère la factorisation de $\mathrm{X}^{p^n} - \mathrm{X}$ en irréductibles dans $\mathbb{F}_p[\mathrm{X}]$. On remarque que la multiplicité de chacun des facteurs irréductibles est un puisque $(\mathrm{X}^{p^n} - \mathrm{X})' = -1$ est premier avec $\mathrm{X}^{p^n} - \mathrm{X}$.

On considère à présent Q un facteur irréductible de $\mathrm{X}^{p^n} - \mathrm{X}$. Comme $\mathrm{X}^{p^n} - \mathrm{X}$ est scindé dans $k = \mathbb{F}_{p^n}$, Q est aussi scindé dans k, en particulier, il a une racine x dans $\mathbb{F}_{p^n}$. Ainsi $\mathbb{F}_p[\mathrm{X}]/\mathrm{Q}$ s'identifie au sous-corps $\mathbb{F}_p(x)$ de k. Avec le lemme précédent, on en déduit que $\deg \mathrm{Q}$ divise n.

Inversement, si Q est un polynôme irréductible sur $\mathbb{F}_p$ de degré d divisant n. Alors $\mathbb{F}_p[\mathrm{X}]/\mathrm{Q}$ est un corps à p^d éléments qui s'identifie à un sous-corps de $\mathbb{F}_{p^n}$. En particulier, Q a une racine dans FF_{p^n} et Q divise $\mathrm{X}^{p^n} - \mathrm{X}$.

Nombre de polynômes irréductibles

Proposition 174 Soit p un nombre premier et $m_d(p)$ le nombre de polynômes **unitaires** de degré d irréductibles sur $\mathbb{F}_p$. On a

$$p^n = \sum_{d \mid n} d m_d(p) \qquad \text{et} \qquad n m_n(p) = \sum_{d \mid n} \mu(n/d) p^d$$

Preuve. Il suffit de calculer le degré dans la relation donnée par le lemme précédent et d'appliquer la formule d'inversion de Möbius.

Corollaire 175 Pour tout n, il existe un polynôme irréductible de degré n sur $\mathbb{F}_p$.

Preuve. On a $\mu_n(p) \geqslant \dfrac{p^n - \dfrac{p^{n/2+1}-1}{p-1}}{n} \geqslant \dfrac{1}{n}(1+p^n-p^{n/2+1})$.

Comme $n/2+1 > n$ si et seulement si $n < 2$, on obtient que $\mu_n(p) > 0$ pour $n \geqslant 2$. Pour $n = 1$, le résultat est évident.

3 Séries formelles et polynômes

Fonctions à valeurs dans...

Soit X un ensemble et $(\mathrm{A}, +_\mathrm{A}, \cdot_\mathrm{A})$ un anneau (commutatif unitaire). On considère l'ensemble $\mathscr{F}(\mathrm{X},\mathrm{A})$ des (toutes les) fonctions de X dans A.

À partir de celle de A, on peut définir une loi de groupe abélien sur $\mathscr{F}(\mathrm{X},\mathrm{A})$ en posant pour $f, g \in \mathscr{F}(\mathrm{X},\mathrm{A})$ et $x \in \mathrm{X}$,

$$(f+g)(x) = f(x) +_\mathrm{A} g(x)\,.$$

L'élément neutre est la fonction constante égale à $0_\mathrm{A} : x \mapsto 0_\mathrm{A}$. L'opposée de f est la fonction $x \mapsto -_\mathrm{A} f(x)$.

On peut aussi définir la multiplication de f par un élément $a \in \mathrm{A}$ via

$$af : x \mapsto af(x)\,.$$

Remarque 176 — Notation. Il est souvent de noter la fonction $f : x \mapsto f(x)$ comme une famille d'éléments indexée par X. Par exemple, la famille $(a_x)_{x\in\mathrm{X}}$ désigne la fonction donnée par $x \mapsto a_x$.

Multiplication

Grâce à la multiplication dans A, on peut aussi définir une multiplication sur l'ensemble des fonctions : pour $f, g \in \mathscr{F}(\mathrm{X},\mathrm{A})$ et $x \in \mathrm{X}$,

$$(fg)(x) = f(x) \cdot_\mathrm{A} g(x)\,.$$

L'élément neutre est la fonction constante égale à $1_\mathrm{A} : x \mapsto 1_\mathrm{A}$.

On construit ainsi une structure d'anneau sur $\mathscr{F}(\mathrm{X},\mathrm{A})$.

Dans ce cadre, la fonction af est aussi le produit de la fonction constante $x \mapsto a$ par la fonction f.

Que se passe-t-il lorsque X est plus riche ?

Lorsqu'on peut additionner des éléments de X, on peut définir un autre produit sur $\mathscr{F}(\mathrm{X},\mathrm{A})$ et ainsi une autre structure d'anneau sur $\mathscr{F}(\mathrm{X},\mathrm{A})$.

Le cas qui va nous intéresser est celui de l'ensemble $\mathrm{X} = \mathbb{N}^n$ muni de la loi d'addition composante par composante. Cet ensemble à la propriété remarquable que, pour tout $x \in \mathbb{N}^n$, l'ensemble $\mathrm{S}_x = \{(s,t) \in (\mathbb{N}^n)^2, \quad s+t = x\}$ est fini.

3.1 Séries formelles

Définition 177 — Série formelle. Soit A un anneau commutatif unitaire et $n \in \mathbb{N}$. L'anneau des **séries formelles à n indéterminées à coefficients dans** A est noté $\mathrm{A}[\![\mathrm{X}_1,\ldots,\mathrm{X}_n]\!]$. L'ensemble sous-jacent à $\mathrm{A}[\![\mathrm{X}_1,\ldots,\mathrm{X}_n]\!]$ est l'ensemble $\mathscr{F}(\mathbb{N}^n,\mathrm{A})$ des fonctions de $\mathbb{N}^n$ dans A ou encore l'ensemble des familles d'éléments de A indexés par $\mathbb{N}^n$: un élément typique de $\mathrm{A}[\![\mathrm{X}_1,\ldots,\mathrm{X}_n]\!]$ est de la forme $a = (a_{i_1,\ldots,i_n})_{(i_1,\ldots,i_n)\in\mathbb{N}^n}$ où $a_{i_1,\ldots,i_n} \in \mathrm{A}$.

La somme de $a = (a_{i_1,\ldots,i_n})_{(i_1,\ldots,i_n)\in\mathbb{N}^n}$ et $b = (b_{i_1,\ldots,i_n})_{(i_1,\ldots,i_n)\in\mathbb{N}^n}$ est définie terme à terme par $c = a+b$ où $c_{i_1,\ldots,i_n} = a_{i_1,\ldots,i_n} + b_{i_1,\ldots,i_n}$ pour tout $(i_1,\ldots,i_n) \in \mathbb{N}^n$.

La question du produit

Le produit (qui est évidemment commutatif) de a et b est défini par $c = ab$ où

$$c_{i_1,\ldots,i_n} = \sum_{\substack{((j_1,\ldots,j_n),(k_1,\ldots,k_n)) \\ (j_1,\ldots,j_n)+(k_1,\ldots,k_n)=(i_1,\ldots,i_n)}} a_{j_1,\ldots,j_n} b_{k_1,\ldots,k_n}$$

Exercice 44 Ce produit est bien défini (la somme est finie), associatif, commutatif et distributif par rapport à $+$.

Il a un élément neutre : l'élément $a = (a_{i_1,\dots,i_n})_{(i_1,\dots,i_n)\in\mathbb{N}^n}$ donné par $a_{0,\dots,0} = 1_{\mathrm{A}}$ et $a_{i_1,\dots,i_n} = 0$ sinon.

Ainsi $\mathrm{A}[\![\mathrm{X}_1,\dots,\mathrm{X}_n]\!]$ est bien un anneau commutatif unitaire.

Morphismes d'anneaux

Proposition 178 On dispose d'un morphisme d'anneaux de A dans $\mathrm{A}[\![\mathrm{X}_1,\dots,\mathrm{X}_n]\!]$ donné par $a \mapsto i(a)$ où $i(a)_{0,\dots,0} = a$ et $i(a)_{i_1,\dots,i_n} = 0$ sinon.

On dispose d'un morphisme d'anneaux de $\mathrm{A}[\![\mathrm{X}_1,\dots,\mathrm{X}_n]\!]$ dans A donné par $a \mapsto a_{0,\dots,0}$.

Preuve. Le seul couple $(j,k) \in (\mathbb{N}^n)^2$ tel que $j+k=0$ est $(0,0)$.

Si $i \in \mathbb{N}^n$ et $i \neq 0$, alors pour $(j,k) \in (\mathbb{N}^n)^2$ vérifiant $j+k=i$, on a $j \neq 0$ ou $k \neq 0$.

Notation

Définition 179 — Les indéterminées. Pour $i \in \{1,2,\dots,n\}$, on définit $\mathrm{X}_i \in \mathrm{A}[\![\mathrm{X}_1,\dots,\mathrm{X}_n]\!]$ par $(\mathrm{X}_i)_{0,\dots,1,\dots,0} = 1$ et $(\mathrm{X}_i)_{i_1,\dots,i_n} = 0$ sinon.

Exercice 45 Montrer que ${\mathrm{X}_i}^j$ est donnée par $({\mathrm{X}_i}^j)_{0,\dots,j,\dots,0} = 1$ et $({\mathrm{X}_i}^j)_{i_1,\dots,i_n} = 0$ sinon.

Montrer que $c := {\mathrm{X}_1}^{i_1}\cdots{\mathrm{X}_n}^{i_n}$ est donnée par $c_{i_1,\dots,i_n} = 1$ et $c_{j_1,\dots,j_n} = 0$ sinon.

Puis que $d := a{\mathrm{X}_1}^{i_1}\cdots{\mathrm{X}_n}^{i_n}$ est donnée par $d_{i_1,\dots,i_n} = a$ et $d_{j_1,\dots,j_n} = 0$ sinon.

Comprendre alors le sens de la **notation** d'un élément de $\mathrm{A}[\![\mathrm{X}_1,\dots,\mathrm{X}_n]\!]$ sous la forme

$$a = \sum_{(i_1,\dots,i_n)\in\mathbb{N}^n} a_{i_1,\dots,i_n}{\mathrm{X}_1}^{i_1}\cdots{\mathrm{X}_n}^{i_n}.$$

Quelques exercices

Exercice 46 Montrer que si A est intègre alors $\mathrm{A}[\![\mathrm{X}_1,\dots,\mathrm{X}_n]\!]$ l'est aussi (on pourra introduire un ordre total compatible avec l'addition sur $\mathbb{N}^n$ (par exemple l'ordre lexicographique) et considérer les coefficients de plus bas degré).

Exercice 47 Montrer que $\mathrm{A}[\![\mathrm{X}_1,\dots,\mathrm{X}_n]\!] \overset{\text{Ann.}}{\simeq} \mathrm{A}[\![\mathrm{X}_1,\dots,\mathrm{X}_k]\!][\![\mathrm{Y}_1,\dots,\mathrm{Y}_{n-k}]\!]$.

Montrer que dans $\mathrm{A}[\![\mathrm{X}]\!]$, l'élément $1-\mathrm{X}$ est inversible et calculer son inverse.

En déduire qu'un élément $a \in \mathrm{A}[\![\mathrm{X}_1,\dots,\mathrm{X}_n]\!]$ est inversible si et seulement si $a_{0,\dots,0}$ est inversible.

3.2 Polynômes

Définition 180 — Polynômes. L'ensemble des séries formelles dont le nombre de coefficients non nuls est fini est un sous-anneau de $\mathrm{A}[\![\mathrm{X}_1,\dots,\mathrm{X}_n]\!]$ notée $\mathrm{A}[\mathrm{X}_1,\dots,\mathrm{X}_n]$ et appelée l'algèbre des polynômes à n indéterminées à coefficients dans A.

L'écriture

$$a = \sum_{(i_1,\dots,i_n)\in\mathbb{N}^n} a_{i_1,\dots,i_n}{\mathrm{X}_1}^{i_1}\cdots{\mathrm{X}_n}^{i_n}.$$

est alors une somme finie.

Définition 181 — Graduation. On dit que $\mathrm{P} \in \mathrm{A}[\mathrm{X}_1,\dots,\mathrm{X}_n]$ est un **polynôme homogène de degré** m si $a_{i_1,\dots,i_n} = 0$ dès que $i_1+\cdots+i_n \neq m$.

Tout polynôme $\mathrm{P} \in \mathrm{A}[\mathrm{X}_1,\dots,\mathrm{X}_n]$ se décompose de façon unique en $\mathrm{P} = \mathrm{P}_0 + \mathrm{P}_1 + \cdots + \mathrm{P}_m$ où P_i est homogène de degré i, $\mathrm{P}_m \neq 0$. On dit que m est le **degré total** de P.

Le cas d'un corps

Lorsque $\mathrm{A} = k$ est un corps, la famille $({\mathrm{X}_1}^{i_1}\cdots{\mathrm{X}_n}^{i_n})_{(i_1,\dots,i_n)}$ est une base du k-espace vectoriel $k[\mathrm{X}_1,\dots,\mathrm{X}_n]$.

On a la décomposition

$$k[\mathrm{X}_1,\dots,\mathrm{X}_n] = \bigoplus_{i\in\mathbb{N}} \mathrm{H}_i$$

où H_i désigne l'ensemble des polynômes homogènes de degré i qui forme un sous-espace vectoriel dont une base $({\mathrm{X}_1}^{i_1}\cdots{\mathrm{X}_n}^{i_n})_{(i_1,\dots,i_n),i_1+\cdots+i_n=i}$.

La dimension de H_i est $\binom{n+i-1}{n-1}$

Propriété de l'anneau des polynômes

Exercice 48 Soit A un anneau commutatif unitaire.

a) Montrer à l'aide de la définition que $\mathrm{A}[\mathrm{X}_1,\dots,\mathrm{X}_n] = \mathrm{A}[\mathrm{X}_1,\dots,\mathrm{X}_k][\mathrm{X}_{k+1},\dots,\mathrm{X}_n]$.

Dans les questions **b** à **d**, on considère le polynôme $\mathrm{P} = a_0 + a_1\mathrm{X} + \cdots + a_n\mathrm{X}^n \in \mathrm{A}[\mathrm{X}]$.

b) Montrer que P est nilpotent si et seulement si pour tout i, a_i est nilpotent.

c) Montrer que P est inversible si et seulement si a_0 est inversible et $a_1,\dots,a_n$ nilpotent (on pourra démontrer que dans un anneau commutatif, si u est inversible et x nilpotent alors $u+x$ est inversible).

d) Montrer que si P est un diviseur de 0 alors il existe $a \in \mathrm{A} \smallsetminus \{0\}$ tel que $a\mathrm{P} = 0$.

e) En déduire les éléments nilpotents, inversibles et diviseurs de zéros de $\mathrm{A}[\mathrm{X}_1,\dots,\mathrm{X}_n]$.

PROPRIÉTÉ UNIVERSELLE DES POLYNÔMES

Proposition 182 — Propriété universelle des polynômes. Soit B un anneau **commutatif**, $\rho : \mathrm{A} \to \mathrm{B}$ un morphisme d'anneaux unitaires et $b_1,\dots,b_n \in \mathrm{B}$.

Il existe un unique morphisme d'anneaux φ de $\mathrm{A}[\mathrm{X}_1,\dots,\mathrm{X}_n]$ dans B tel que $\varphi \circ i = \rho$ et $\varphi(\mathrm{X}_j) = b_j$ pour tout j.

Il est donné par

$$\varphi\left(\sum_{(i_1,\dots,i_n)\in\mathbb{N}^n} a_{i_1,\dots,i_n}\mathrm{X}_1{}^{i_1}\cdots\mathrm{X}_n{}^{i_n}\right) = \sum_{(i_1,\dots,i_n)\in\mathbb{N}^n} \rho(a_{i_1,\dots,i_n})b_1{}^{i_1}\cdots b_n{}^{i_n}$$

φ est appelé le *morphisme d'évaluation en les b_i*.

Exercice 49 Que se passe-t-il si on ne suppose plus B commutative ?

Applications

Application 183 Il n'existe pas d'éléments $\mathrm{U},\mathrm{V},\mathrm{W}$ de l'anneau $\mathbb{Z}[\mathrm{X}_1,\mathrm{X}_2,\mathrm{X}_3,\mathrm{Y}_1,\mathrm{Y}_2,\mathrm{Y}_3]$ vérifiant

$$\mathrm{U}^2+\mathrm{V}^2+\mathrm{W}^2 = (\mathrm{X}_1{}^2+\mathrm{X}_2{}^2+\mathrm{X}_3{}^2)(\mathrm{Y}_1{}^2+\mathrm{Y}_2{}^2+\mathrm{Y}_3{}^2)$$

En effet, sinon, en évaluant en $\mathrm{X}_1 \mapsto 1, \mathrm{X}_2 \mapsto 1, \mathrm{X}_3 \mapsto 1, \mathrm{Y}_1 = 1, \mathrm{Y}_2 = 2, \mathrm{Y}_3 = 0$, on obtient que 15 est somme de 3 carrés d'entiers. NON.

Corollaire 184 Soit A un anneau intègre infini (par exemple un corps infini). Le morphisme d'anneaux

$$\begin{cases} \mathrm{A}[\mathrm{X}_1,\dots,\mathrm{X}_n] \longrightarrow \mathscr{F}(\mathrm{A}^n,\mathrm{A}) \\ \qquad \mathrm{P} \qquad\quad \longmapsto ((a_1,\dots,a_n)\mapsto \mathrm{P}(a_1,\dots,a_n)) \end{cases}$$

est injectif.

Preuve. Si $n=1$ alors, on a vu que $\mathrm{P} \neq 0$ avait au plus $\deg \mathrm{P}$ racines.

On raisonne par récurrence et on prend P qui vérifie $\mathrm{P}(a_1,\dots,a_n) = 0$ pour tout $(a_1,\dots,a_n) \in \mathrm{A}^n$.

On écrit $\mathrm{P} = \sum_{i=0}^{\ell} \mathrm{P}_i\mathrm{X}_n{}^i$ avec $\mathrm{P}_i \in \mathrm{A}[\mathrm{X}_1,\dots,\mathrm{X}_{n-1}]$. On fixe $(a_1,\dots,a_{n-1}) \in \mathrm{A}^{n-1}$. On a alors $\mathrm{Q}(\mathrm{X}_n) := \mathrm{P}(a_1,\dots,a_{n-1},\mathrm{X}_n) = \sum_{i=0}^{\ell} \mathrm{P}_i(a_1,\dots,a_{n-1})\mathrm{X}_n{}^i \in \mathrm{A}[\mathrm{X}_n]$.

Par hypothèse $\mathrm{Q}(a) = 0$ pour tout $a \in \mathrm{A}$. Le cas $n=1$ assure alors que $\mathrm{P}_i(a_1,\dots,a_{n-1}) = 0$ pour tout i. L'hypothèse de récurrence assure alors que $\mathrm{P}_i = 0$ pour tout i et donc $\mathrm{P} = 0$

Un réservoir d'identité

Application 185 Soit A un anneau commutatif et $\mathrm{U},\mathrm{V} \in \mathrm{M}_n(\mathrm{A})$. On a $\det(\mathrm{UV}) = \det(\mathrm{U})\det(\mathrm{V})$ et aussi $\mathrm{com}(\mathrm{U})\mathrm{com}(\mathrm{V}) = \mathrm{com}(\mathrm{UV})$ et encore $\chi_{\mathrm{U}}(\mathrm{U}) = 0$ ou encore $\chi_{\mathrm{UV}} = \chi_{\mathrm{VU}}$ et ${}^t\mathrm{Com}(\mathrm{U})\,\mathrm{U} = \mathrm{U}\,{}^t\mathrm{Com}(\mathrm{U}) = \det(\mathrm{U})\mathrm{id}$.

Une caractérisation des anneaux polynômes

Exercice 50 Soit C un anneau commutatif unitaire vérifiant les propositions suivantes

1. Il existe $\lambda : A \to C$ un morphisme d'anneaux (unitaires)
2. Il existe $c_1, \ldots, c_n \in C$ tel que pour tout B anneau commutatif unitaire, tout $\rho : A \to B$ et tout $b_1, \ldots, b_n \in B$, il existe un unique morphisme d'anneaux unitaires $\varphi : C \to B$ tel que $\varphi(c_i) = b_i$ et $\varphi \circ \lambda = \rho$.

Alors C est isomorphe à $A[X_1, \ldots, X_n]$. Plus précisément, il existe un isomorphisme φ vérifiant $\varphi \circ i = \lambda$ et $\varphi(X_i) = c_i$.

Corollaire 186 On a $A[X_1, \ldots, X_n] = A[X_1, \ldots, X_{n-1}][X_n]$.

3.3 Polynômes symétriques

Définition 187 – Polynôme symétrique. Soit A un anneau. Pour tout $\sigma \in \mathfrak{S}_n$, il existe un unique automorphisme φ_σ d'anneaux de $A[X_1, \ldots, X_n]$ tel que $\varphi_\sigma(X_i) = X_{\sigma(i)}$ et $\varphi \circ i = i$. Un polynôme $P \in A[X_1, \ldots, X_n]$ est dit *symétrique* si $\varphi_\sigma(P) = P$ pour tout $\sigma \in \mathfrak{S}_n$. On note $A[X_1, \ldots, X_n]^{\mathfrak{S}_n}$ le sous-anneau de $A[X_1, \ldots, X_n]$ engendré par A et les polynômes symétriques.

Définition 188 – Polynôme symétrique élémentaires. On définit $\Sigma_k(X_1, \ldots, X_n) \in A[X_1, \ldots, X_n]^{\mathfrak{S}_n}$ comme le coefficient en Y^{n-k} dans

$$(Y + X_1) \cdots (Y + X_n).$$

On a

$$\Sigma_k(X_1, \ldots, X_n) = \sum_{1 \leqslant i_1 < \cdots < i_k \leqslant n} X_{i_1} \cdots X_{i_k}.$$

Théorème

Théorème 189 Le morphisme d'évaluation en les Σ_k

$$\begin{cases} A[Y_1, \ldots, Y_n] & \longrightarrow A[X_1, \ldots, X_n] \\ \quad Q & \longmapsto Q(\Sigma_1, \ldots, \Sigma_n) \end{cases}.$$

est un morphisme injectif dont l'image est $A[X_1, \ldots, X_n]^{\mathfrak{S}_n}$.

Applications

Définition 190 – Fraction rationnelle symétrique. Soit k un corps. Pour tout $\sigma \in \mathfrak{S}_n$, il existe un unique automorphisme φ_σ de k-algèbre de $k(X_1, \ldots, X_n)$ tel que $\varphi_\sigma(X_i) = X_{\sigma(i)}$. Une fraction rationnelle $P \in k(X_1, \ldots, X_n)$ est dite *symétrique* si $\varphi_\sigma(P) = P$ pour tout $\sigma \in \mathfrak{S}_n$. On note $k(X_1, \ldots, X_n)^{\mathfrak{S}_n}$ la sous-algèbre de $k(X_1, \ldots, X_n)$ formée des polynômes symétriques.

Proposition 191 On a $k(X_1, \ldots, X_n)^{\mathfrak{S}_n} = k(\Sigma_1, \ldots, \Sigma_n)$.

Un exemple Soit $X^4 + aX^3 + bX^2 + cX + d = (X - a_1)(X - a_2)(X - a_3)(X - a_4)$. Déterminer les coefficients du polynôme dont les racines sont $\theta_1 = (a_1 + a_2)(a_3 + a_4)$,$\theta_2 = (a_1 + a_3)(a_2 + a_4)$ et $\theta_3 = (a_1 + a_4)(a_2 + a_3)$.

Un autre exemple

Proposition 192 Soit k un corps et $P = a_0 + a_1X + \cdots + a_nX^n \in k[X]$ (non scindé avec $a_n \neq 0$). Soit K un corps de décomposition de P sur K et $P = \prod_{i=1}^{n} (X - \alpha_i)$ une décomposition de P en irréductible dans K[X].

Si $P \in k[X_1, \ldots, X_n]$ est un polynôme symétrique alors $P(\alpha_1, \ldots, \alpha_n) \in k$.

Preuve. En effet, on peut écrire $P = Q(\Sigma_1, \ldots, \Sigma_n)$ avec $Q \in k[Y_1, \ldots, Y_n]$ et on a $\Sigma_i(\alpha_1, \ldots, \alpha_n) = (-1)^i a_{n-i}/a_n \in k$ et donc $P(\alpha_1, \ldots, \alpha_n) = Q(-a_{n-1}/a_n, \ldots, (-1)^n a_0/a_n) \in k$.

3.4 $\mathbb{C}$ est algébriquement clos

Le corps $\mathbb{R}$ vérifie les deux propriétés suivantes : le théorème des valeurs intermédiaires, tout nombre positif est un carré. Cela assure que le corps $\mathbb{C} := \mathbb{R}[X]/(X^2 + 1)$ est algébriquement clos.

Preuve. Soit $\mathrm{P} \in \mathbb{C}[\mathrm{X}]$ non constant. On veut montrer que P a une racine dans $\mathbb{C}$. On peut se ramener au cas où $\mathrm{P} \in \mathbb{R}[\mathrm{X}]$, en considérant le polynôme $\mathrm{Q} = \mathrm{P}\overline{\mathrm{P}} \in \mathbb{R}[\mathrm{X}]$. Si Q a une racine z alors, soit $\mathrm{P}(z) = 0$. OK. Soit $\overline{\mathrm{P}}(z) = 0$ mais on a alors en calculant le conjugué, $\mathrm{P}(\overline{z}) = 0$. OK.

On raisonne par récurrence sur la plus grande puissance ν de 2 qui divise $\deg \mathrm{Q}$. Si $\nu = 0$ alors $\deg \mathrm{Q}$ est impair et Q a une racine réelle donc complexe d'après le théorème des valeurs intermédiaires.

Suite de la preuve On suppose que le résultat est vrai pour $\nu = n$.

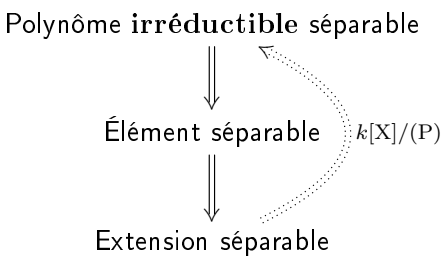
On note x_i les racines de Q dans un corps de décomposition k de P sur $\mathbb{C}$. On veut montrer que l'un des x_i est dans $\mathbb{C}$.

On fixe $c \in \mathbb{R}$. On considère alors le polynôme $\mathrm{R}_c \in k[\mathrm{X}]$ ayant les $\deg \mathrm{Q}(\deg \mathrm{Q} - 1)/2$ racines suivantes $x_i + x_j + cx_ix_j$ $(i < j)$. Les coefficients de R_c sont des polynômes symétriques en les x_i. Ainsi $\mathrm{R}_c \in \mathbb{R}[\mathrm{X}]$ et la plus grande puissance de 2 divisant $\deg \mathrm{R}_c$ est $n - 1$. Ainsi (hypothèse de récurrence) R_c a une racine complexe.

Comme $\mathbb{R}$ est infini, il existe $c \neq c'$ et $i < j$ tel que $x_i + x_j + cx_ix_j \in \mathbb{C}$. $x_i + x_j + c'x_ix_j \in \mathbb{C}$.

On en déduit que $a = x_i + x_j \in \mathbb{C}$ et $b = x_ix_j \in \mathbb{C}$. Ainsi x_i et x_j sont racines de $\mathrm{R} = \mathrm{X}^2 - a\mathrm{X} + b \in \mathbb{C}[\mathrm{X}]$. Or $\mathrm{R} = (\mathrm{X} - a/2)^2 + b - a^2/4$. Pour montrer que x_i et x_j sont dans $\mathbb{C}$, il suffit donc de montrer que tout nombre complexe est un carré. En reprenant la démonstration du fait que si z^2 était constructible alors z l'était (qui repose sur le fait que tout nombre réel positif est un carré), on obtient le résultat souhaité.

4 Théorie de Galois



Le cas des extensions séparables finies

$\updownarrow$

Nombre de prolongements à valeurs dans une extension algébriquement close

4.1 Changement de corps

Soit K une extension du corps k et $\mathrm{U}, \mathrm{V} \in k[\mathrm{X}]$ avec $\mathrm{V} \neq 0$.

On considère $\mathrm{U} = \mathrm{V}\mathrm{Q}_k + \mathrm{R}_k$ la division euclidienne de U par V dans $k[\mathrm{X}]$ c'est-à-dire $\mathrm{Q}_k, \mathrm{R}_k \in k[\mathrm{X}]$ et $\deg \mathrm{R}_k < \deg \mathrm{V}$.

De même, on considère $\mathrm{U} = \mathrm{V}\mathrm{Q}_\mathrm{K} + \mathrm{R}_\mathrm{K}$ la division euclidienne de U par V dans $k[\mathrm{X}]$ c'est-à-dire $\mathrm{Q}_\mathrm{K}, \mathrm{R}_\mathrm{K} \in \mathrm{K}[\mathrm{X}]$ et $\deg \mathrm{R}_\mathrm{K} < \deg \mathrm{V}$.

Par unicité de la division euclidienne dans $\mathrm{K}[\mathrm{X}]$, on obtient $\mathrm{Q}_k = \mathrm{Q}_\mathrm{K}$ et $\mathrm{R}_k = \mathrm{R}_\mathrm{K}$.

Application 193

1. $\mathrm{V} \mid \mathrm{U}$ dans $k[\mathrm{X}]$ $\iff$ $\mathrm{V} \mid \mathrm{U}$ dans $\mathrm{K}[\mathrm{X}]$.
2. Le pgcd de U et V ne dépend pas du corps : si $\mathrm{P}_k = \mathrm{pgcd}(\mathrm{U}, \mathrm{V})$ dans $k[\mathrm{X}]$ et $\mathrm{P}_\mathrm{K} = \mathrm{pgcd}(\mathrm{U}, \mathrm{V})$ dans $\mathrm{K}[\mathrm{X}]$ alors il existe $\lambda \in \mathrm{K}^\times$ tel que $\mathrm{P}_\mathrm{K} = \lambda \mathrm{P}_k$.

4.2 Séparabilité

Polynôme séparable

Proposition 194 Soient k un corps, $\mathrm{P} \in k[\mathrm{X}]$ non constant. Dans la suite, Ω désigne une extension algébriquement close de k ; K un corps de décomposition de P sur k et L une extension de k. On a les équivalences suivantes

(i) $\mathrm{pgcd}(\mathrm{P}, \mathrm{P}') = 1$;

(ii) pour toute L, P et P′ sont sans racine commune ;

(*iii*) P et P′ n'ont pas de racine commune dans K ;
(*iv*) P et P′ n'ont pas de racine commune dans Ω ;
(*v*) pour toute L, P n'a que des racines simples dans L ;
(*vi*) P n'a que des racines simples dans K ;
(*vii*) P n'a que des racines simples dans Ω ;
(*viii*) il existe L telle que P se factorise en un produit de polynôme de degré 1 **deux à deux distincts** dans L[X] ;
(*ix*) P se factorise en un produit de polynôme de degré 1 **deux à deux distincts** dans K[X] ;
(*x*) P se factorise en un produit de polynôme de degré 1 **deux à deux distincts** dans Ω[X].

Définition 195 — Polynôme séparable. Soit $\mathrm{P} \in k[\mathrm{X}]$ un polynôme **irréductible**. On dit que P est **séparable** si P vérifie les conditions équivalentes de la proposition précédente.

De plus, si P est irréductible, elles sont aussi équivalentes à

(*xi*) $\mathrm{P}' \neq 0$
(*xii*) il existe une extension L de k tel que P ait une racine simple.

Preuve. On a $(x) \Rightarrow (xii)$.

$(xii) \Rightarrow (xi)$. Si a est une racine de P dans L, on a $\mathrm{P}'(a) \neq 0$ et donc $\mathrm{P}' \neq 0$.

$(xi) \Rightarrow (i)$. Comme P est irréductible, on a $\mathrm{pgcd}(\mathrm{P}, \mathrm{P}') \in \{1, \mathrm{P}\}$ et $\mathrm{pgcd}(\mathrm{P}, \mathrm{P}') = \mathrm{P}$ si et seulement si $\mathrm{P} \mid \mathrm{P}'$ si et seulement si $\mathrm{P}' = 0$ car $\deg \mathrm{P}' < \deg \mathrm{P}$.

Polynôme séparable et caractéristique

Remarque 196 — Polynôme irréductible et dérivation. Soit $\mathrm{P} \in k[\mathrm{X}]$ un polynôme irréductible. Alors $\mathrm{pgcd}(\mathrm{P}, \mathrm{P}') = 1$ ou alors $\mathrm{P}' = 0$. Ce deuxième cas ne peut intervenir qu'en caractéristique p et si en plus $k^{[p]} := \{x^p,\ x \in k\} \neq k$ (c'est-à-dire l'homorphisme de Frobenius de k n'est pas surjectif).

En effet, si $\mathrm{P} = \sum a_i \mathrm{X}^i$ est irréductible et vérifie $\mathrm{P}' = 0$ alors $\mathrm{P} = \mathrm{Q}(\mathrm{X}^p)$ avec $\mathrm{Q} = \sum a_{pi} \mathrm{X}^i$. Si $k^{[p]} = k$ alors on écrit $a_{pi} = b_i{}^p$ et on a $\mathrm{P} = \mathrm{R}(\mathrm{X})^p$ avec $\mathrm{R} = \sum b_i \mathrm{X}^i$ et P n'est pas irréductible.

Exemple 197 En caractéristique nulle, tout polynôme irréductible est séparable.

Soit k un corps fini alors tout polynôme irréductible sur k est séparable.

ÉLÉMENTS ET EXTENSIONS SÉPARABLES

Définition 198 — Élément séparable. Soient K une extension de k et $x \in \mathrm{K}$. On dit que x est **séparable** sur k si le polynôme minimal de x sur k est séparable. Un élément séparable est algébrique.

Définition 199 — Extension algébrique. Soit K une extension de k. On dit que K est une **extension séparable de** k si tout élément de K est séparable sur k. Une extension séparable est algébrique.

Remarque 200 — Lien polynôme séparable et extension séparable. Soient $\mathrm{P} \in k[\mathrm{X}]$ un polynôme irréductible. Alors $k[\mathrm{X}]/(\mathrm{P})$ séparable sur k si et seulement si P est séparable.

En effet, si $k[\mathrm{X}]/(\mathrm{P})$ est séparable sur k alors P qui est le polynôme minimal de x la classe de X est séparable.

Réciproquement, soit $y = \mathrm{Q}(x) \in k[\mathrm{X}]/(\mathrm{P})$. Il s'agit de montrer que le polynôme minimal de y est séparable. Pour cela, on a besoin d'autres caractérisations de la séparabilité...

Manipuler la séparabilité

Pb 1 On n'a pas montré que P séparable $\Longrightarrow k[\mathrm{X}]/(\mathrm{P})$ séparable.

Lemme 201 — Un premier critère. Soient k un corps, K une extension de k et $a \in \mathrm{K}$. On a alors les équivalences

(*i*) a est séparable sur k ;
(*ii*) a est racine simple du polynôme minimal P de a sur k ;
(*iii*) il existe $\mathrm{Q} \in k[\mathrm{X}]$ tel que a soit racine simple de Q

Preuve. $(i) \Rightarrow (iii)$. On prend $\mathrm{Q} = \mathrm{P}$.

$(iii) \Rightarrow (ii)$. On a $\mathrm{P} \mid \mathrm{Q}$ et donc a est racine simple de P (sinon $(\mathrm{X} - a)^2 \mid \mathrm{Q}$).

$(ii) \Rightarrow (i)$. C'est le critère (xii) de séparabilité

Application 202 — Transitivité de la séparabilité. Soient $k \hookrightarrow \mathrm{K}$ et $\mathrm{K} \hookrightarrow \mathrm{L}$ deux extensions de corps. Alors L séparable sur k si et seulement si L séparable sur K et K séparable sur k.

(⇒) K est évidemment séparable sur k. De plus, si $x \in \mathrm{L}$ alors le polynôme minimal de a sur k est à coefficient dans K et admet a comme racine. Donc x est séparable sur K.

Pb 2 Il faut démontrer la réciproque.

Dégré séparable

Proposition-Définition 203 — Degré séparable. Soit $i : k \hookrightarrow \mathrm{K}$ une extension **algébrique** et $j : k \hookrightarrow \Omega$ une extension algébriquement close de Ω. Alors $|\mathrm{Hom}_{k-\mathrm{alg.}}(\mathrm{K}, \Omega)|$ ne dépend ni de Ω ni de j. On définit alors **le degré séparable de** K **sur** k

$$[\mathrm{K} : k]_{\mathrm{s}} := |\mathrm{Hom}_{k-\mathrm{alg.}}(\mathrm{K}, \Omega)| \neq 0.$$

Preuve. Soit $\widetilde{\Omega}$ **la** clôture algébrique de k contenue dans Ω. On a $\mathrm{Hom}_{k-\mathrm{alg.}}(\mathrm{K}, \Omega) = \mathrm{Hom}_{k-\mathrm{alg.}}(\mathrm{K}, \widetilde{\Omega})$ car K est algébrique sur k. En effet, si $x \in \mathrm{K}$ est annulé par $\mathrm{P} \in k[\mathrm{X}]$ et $\sigma : \mathrm{K} \to \Omega$ un morphisme d'extensions alors $\sigma(x)$ est annulé par P.

Si $j' : k \to \Omega'$ est une extension algébriquement close, on a de même

$$\mathrm{Hom}_{k-\mathrm{alg.}}(\mathrm{K}, \Omega') = \mathrm{Hom}_{k-\mathrm{alg.}}(\mathrm{K}, \widetilde{\Omega}').$$

Enfin, comme $\widetilde{\Omega}$ et $\widetilde{\Omega}'$ sont des extensions k-isomorphes (disons via $\tau : \widetilde{\Omega} \to \widetilde{\Omega}'$), alors la composition à gauche par τ donne $\mathrm{Hom}_{k-\mathrm{alg.}}(\mathrm{K}, \widetilde{\Omega}) \overset{\text{bij.}}{\simeq} \mathrm{Hom}_{k-\mathrm{alg.}}(\mathrm{K}, \widetilde{\Omega}')$

Multiplicativité

Théorème 204 — Multiplicativité du degré séparable. Soient K une extension de k et L une extension de K. Alors on a

$$[\mathrm{L} : \mathrm{K}]_{\mathrm{s}}[\mathrm{K} : k]_{\mathrm{s}} = [\mathrm{L} : k]_{\mathrm{s}}.$$

Preuve. Soit $j : k \hookrightarrow \Omega$ une extension algébriquement close. Il existe $[\mathrm{K} : k]_{\mathrm{s}}$ morphismes d'extensions noté $\sigma_i : \mathrm{K} \to \Omega$ pour $i \in \mathrm{I}$.

On fixe i. Ainsi $\sigma_i : \mathrm{K} \hookrightarrow \Omega$ est une extension algébriquement close. Il existe exactement $[\mathrm{L} : \mathrm{K}]_{\mathrm{s}}$ morphismes d'extensions $\tau_{i\ell} : \mathrm{L} \to \Omega$.

$$\begin{tikzcd}
\mathrm{L} \arrow[rr, "\tau_{i\ell}"] & & \Omega \\
& \mathrm{K} \arrow[ul] \arrow[ur, "\sigma_i"'] & \\
& & k \arrow[ul] \arrow[uu, "j"']
\end{tikzcd}$$

De plus, si $\tau_{i\ell} = \tau_{i'\ell'}$ alors par restriction à K, on a $\sigma_i = \sigma_{i'}$ et donc $i = i'$ puis $\ell = \ell'$.

Enfin si $\tau : \mathrm{L} \hookrightarrow \Omega$ est un morphisme d'extensions alors $\tau_{|\mathrm{K}} : \mathrm{K} \hookrightarrow \Omega$ est un morphisme d'extension donc il existe i tel que $\tau_{|\mathrm{K}} = \sigma_i$. Puis il existe ℓ tel que $\tau = \tau_{i\ell}$.

Le cas des extension monogènes

Théorème 205 Soit $k(x)$ une extension algébrique monogène de k. Alors $[k(x) : k]_{\mathrm{s}}$ est le nombre de racines distinctes de P le polynôme minimal de x sur k dans Ω une extension algébriquement close de k

En particulier, on a $[k(x) : k]_{\mathrm{s}} \leqslant [k(x) : k] = \deg \mathrm{P}$.

De plus, on a les équivalences

(i) $[k(x) : k]_{\mathrm{s}} = [k(x) : k]$;

(ii) x est séparable sur k ;

(iii) P est séparable sur k ;

(iv) $k(x)$ est séparable sur k.

Preuve. Le premier point est une conséquence immédiate de la propriété universelle des corps de rupture. Le deuxième point est une conséquence immédiate du premier point.

On a $(i) \iff$ le nombre de racines distinctes de P est $\deg \mathrm{P} \iff$ les racines de P sont simples $\iff (iii) \iff (ii)$.

On a déjà vu $(iv) \Rightarrow (iii)$.

Le problème 1 : $(i) \Rightarrow (iv)$
$(i) \Rightarrow (iv)$. Soit $y \in k(x)$. On a

$$[k(x) : k] = [k(x) : k(y)][k(y) : k]$$

et

$$[k(x) : k]_{\mathrm{s}} = [k(x) : k(y)]_{\mathrm{s}}[k(y) : k]_{\mathrm{s}}\,.$$

Or $[k(x) : k(y)]_{\mathrm{s}} \leqslant [k(x) : k(y)]$ (puisque $k(x)$ est engendré sur $k(y)$ par x) et $[k(y) : k] \leqslant [k(y) : k]_{\mathrm{s}}$. On en déduit que $[k(y) : k]_{\mathrm{s}} = [k(y) : k]$ et y est séparable sur k.

Application 206 Soit K une extension **finie** de k alors $[\mathrm{K} : k]_{\mathrm{s}} \leqslant [\mathrm{K} : k]$. En particulier $[\mathrm{K} : k]_{\mathrm{s}} < +\infty$.

On écrit $\mathrm{K} = k(x_1, \ldots, x_n)$. On obtient le résultat par multiplicativité du degré séparable :

$$[\mathrm{K} : k]_{\mathrm{s}} = [\mathrm{K} : \mathrm{K}_{n-1}]_{\mathrm{s}} \cdots [\mathrm{K}_1 : k]_{\mathrm{s}} \leqslant [\mathrm{K} : \mathrm{K}_{n-1}] \cdots [\mathrm{K}_1 : k] = [\mathrm{K} : k]$$

Applications

Corollaire 207 — Une caractérisation de la séparabilité. Soit K une extension **finie** de k. Alors K est séparable sur k si et seulement si $[\mathrm{K} : k]_{\mathrm{s}} = [\mathrm{K} : k]$

Preuve. (⇐) Soit $x \in \mathrm{K}$. On a

$$[\mathrm{K} : k] = [\mathrm{K} : k(x)][k(x) : k]$$

et

$$[\mathrm{K} : k]_{\mathrm{s}} = [\mathrm{K} : k(x)]_{\mathrm{s}}[k(x) : k]_{\mathrm{s}}\,.$$

Or $[k(x) : k]_{\mathrm{s}} \leqslant [k(x) : k]$ et $[\mathrm{K} : k(x)] \leqslant [\mathrm{K} : k(x)]_{\mathrm{s}}$. On en déduit que $[k(x) : k]_{\mathrm{s}} = [k(x) : k]$ et x est séparable sur k.

(⇒) On écrit $\mathrm{K} = k(x_1, \ldots, x_n)$. Comme x_{i+1} est séparable sur $\mathrm{K}_i = k(x_1, \ldots, x_i)$, on obtient le résultat par multiplicativité du degré séparable : on a

$$[\mathrm{K} : k]_{\mathrm{s}} = [\mathrm{K} : \mathrm{K}_{n-1}]_{\mathrm{s}} \cdots [\mathrm{K}_1 : k]_{\mathrm{s}} = [\mathrm{K} : \mathrm{K}_{n-1}] \cdots [\mathrm{K}_1 : k] = [\mathrm{K} : k]$$

Le problème 2

Proposition 208 — Transitivité de la séparabilité. Soient $k \hookrightarrow \mathrm{K}$ et $\mathrm{K} \hookrightarrow \mathrm{L}$ deux extensions de corps. Alors L séparable sur k si et seulement si L séparable sur K et K séparable sur k.

Preuve. (⇒) On l'a déjà vu.
(⇐) Soit $x \in \mathrm{L}$ alors x annule $\mathrm{P} = \sum a_i \mathrm{X}^i \in \mathrm{K}[\mathrm{X}]$ séparable sur K. On en déduit que x est séparable sur $k(a_1, \ldots, a_n)$.

Par ailleurs $k(a_1, \ldots, a_n) \subset \mathrm{K}$ séparable sur k. Ainsi, on a

$$[k(a_1, \ldots, a_n) : k]_{\mathrm{s}} = [k(a_1, \ldots, a_n) : k]$$
$$[k(a_1, \ldots, a_n)(x) : k(a_1, \ldots, a_n)]_{\mathrm{s}} = [k(a_1, \ldots, a_n)(x) : k(a_1, \ldots, a_n)]$$

Finalement, on obtient

$$[k(a_1, \ldots, a_n, x) : k]_{\mathrm{s}} = [k(a_1, \ldots, a_n, x) : k]$$

et $k(a_1, \ldots, a_n, x)$ est séparable sur k. En particulier, x est séparable sur k.

Exercices

Exercice 51 — Famille génératrice et séparabilité. Soit K une extension de k.

(i) Montrer que l'ensemble des éléments de K séparables sur k est une sous-extension de K. Elle est notée K_{s} et appelée **fermeture séparable** de K sur k.

(ii) En déduire que K est séparable sur k si et seulement si K est engendré par des éléments séparables sur k.

(iii) Soit E et F deux sous-extensions de K. On suppose E est une extension séparable de k. Montrer que EF est une extension séparable de F.

Exercice 52 — Extension séparable infinie. Soit K une extension de k. Montrer que K est une extension séparable de k si et seulement si tout sous-extension finie de K est séparable.

Corps parfait

Proposition-Définition 209 — Corps parfait. Soit k un corps de caractéristique p. Si $p = 0$, on note $k^{[p]} := k$. Si p est premier, on note $k^{[p]} := \{x^p \in k,\ x \in k\}$. Soit Ω une clôture algébrique de k.

Les propositions suivantes sont équivalentes

(i) $k = k^{[p]}$;

(ii) tout élément irréductible de $k[\mathrm{X}]$ est séparable ;

(iii) tout extension algébrique de k est séparable ;

(iv) Ω est une extension séparable de k.

Un corps vérifiant ces conditions est appelé **corps parfait**.

Preuve. On a toujours $(ii) \Rightarrow (iii)$ et $(iii) \Rightarrow (iv)$.

$(iv) \Rightarrow (ii)$. Considérons P un polynôme irréductible. Comme Ω est algébriquement clos, il existe une racine x de P dans Ω et P est le polynôme minimal de x sur k. Comme Ω est séparable, on en déduit que P est séparable.

Un corps de caractéristique nulle vérifie immédiatement (i) et (ii).

Supposons $\operatorname{car} k = p$. On a vu que $k = k^{[p]}$ implique (ii).

$(ii) \Rightarrow (i)$

Lemme 210 Soient k un corps de caractéristique p avec p premier et $k \neq k^{[p]}$. Pour $a \in k \smallsetminus k^{[p]}$, le polynôme $\mathrm{P} = \mathrm{X}^{p^n} - a$ est irréductible. De plus, si $n \geqslant 1$, P n'est pas séparable.

Preuve. On suppose $n \geqslant 1$. Soit L un extension de k dans lequel P a une racine α. On a alors $\alpha^{p^n} = a$ et donc $\mathrm{P} = (\mathrm{X} - \alpha)^{p^n}$ dans $\mathrm{L}[\mathrm{X}]$. Si $\mathrm{P} = \mathrm{QR}$ est une factorisation de P dans $k[\mathrm{X}]$ alors $\mathrm{Q} = (\mathrm{X} - \alpha)^m$ avec $1 \leqslant m \leqslant p^n$. On écrit $m = p^r \ell$ avec $\ell \wedge p = 1$. On a donc $\mathrm{Q} = (\mathrm{X}^{p^r} - \alpha^{p^r})^\ell$. Le coefficient en $\mathrm{X}^{p^r(\ell-1)}$ de Q est alors $-\ell\alpha^{p^r} \in k$. Comme $\ell \wedge p = 1$, on en déduit que $\alpha^{p^r} \in k$. Si $r < n$ alors $a = b^p \in k^{[p]}$ avec $b = (\alpha^{p^r})^{p^{n-r-1}}$. Ainsi $m = p^n$ et P est irréductible.

$(ii) \Rightarrow (i)$. Si $k \neq k^{[p]}$ alors on a un polynôme irréductible non séparable.

Élément primitif

Question : Quand une extension algébrique est-elle engendrée par un seul élément ?

Définition 211 — Élément primitif. Soit K une extension monogène de k. On dit qu'un élément $x \in \mathrm{K}$ est **primitif** si $k(x) = \mathrm{K}$.

Proposition 212 — Une caractérisation. Soit K une extension finie de k. Alors K est une extension monogène si et seulement si K admet un nombre fini de sous-extension.

Preuve. Si k est fini alors K aussi et K admet à la fois un nombre fini de sous-corps et un élément primitif (il suffit de choisir un générateur du groupe multiplicatif $\mathrm{K}^\times$).

(⇒) On considère x un élément primitif de K sur k. Pour F une sous-extension de k, on note $\mathrm{P_F}$ le polynôme minimal de x sur F. Montrons que l'injectivité de l'application

$$\begin{cases} \{\text{Sous-extensions de K}\} \longrightarrow \{\text{Diviseurs unitaires de } \mathrm{P}_k\} \\ \qquad \mathrm{F} \qquad\qquad\qquad \longmapsto \mathrm{P_F}\,. \end{cases}$$

Fin de la preuve On fixe F une sous-extension de K et on pose $\mathrm{L} = k(a_0, \ldots, a_n) \subset \mathrm{F}$ où les a_i sont les coefficients de $\mathrm{P_F}$. On a alors $\mathrm{L} = \mathrm{F}$ car $[\mathrm{K} : \mathrm{F}] = [\mathrm{F}(x) : \mathrm{F}] = \deg \mathrm{P_F} = [\mathrm{L}(x) : \mathrm{L}] = [\mathrm{K} : \mathrm{L}]$ puisque $\mathrm{P_F}$ est irréductible sur F et donc sur L. Ainsi F est entièrement déterminé. Comme il n'y a qu'un nombre fini de diviseurs unitaires de P_k, on obtient le résultat souhaité.

(⇐) Prenons x qui n'est dans aucune des sous-extensions strictes de K. Alors $\mathrm{K} = k(x)$. Un tel x existe d'après le lemme suivant.

Lemme 213 — Réunion de sous-espaces vectoriels. Soient k un corps infini, E un k-espace vectoriel et $\mathrm{E}_1, \ldots, \mathrm{E}_n$ des sous-espaces vectoriels stricts de E. Alors

$$\bigcup_{i=1}^{n} \mathrm{E}_i \neq \mathrm{E}$$

Preuve. Raisonnons par récurrence sur n. Le résultat est vrai pour $n = 0$. Si

$$\mathrm{E}_n \subset \bigcup_{i=1}^{n-1} \mathrm{E}_i := \mathrm{F}_{n-1}$$

le résultat s'obtient grâce à l'hypothèse de récurrence. Sinon, il existe $x \in \mathrm{E}_n \smallsetminus \mathrm{F}_{n-1}$ et $y \in \mathrm{E} \smallsetminus \mathrm{E}_n$. On suppose de plus que $\mathrm{E} = \mathrm{F}_{n-1} \cup \mathrm{E}_n$. Pour $\lambda \in k$, on a alors $\lambda x + y \notin \mathrm{E}_n$ et donc $\lambda x + y \in \mathrm{F}_{n-1}$. Comme k est infini, il existe $\lambda \neq \mu$ et $i \in [\![1\,,\, n-1]\!]$ tel que $\lambda x + y \in \mathrm{E}_i$ et $\mu x + y \in \mathrm{E}_i$. On en déduit que $x \in \mathrm{E}_i$. NON.

Donnons une autre preuve de **(⇐)** On a $\mathrm{K} = k(x_1, \ldots, x_n)$. Comme k est infini et que K n'a qu'un nombre fini de sous-extensions, il existe $\lambda, \mu \in k$ avec $\lambda \neq \mu$ tels que $k(x_1 + \lambda x_2) = k(x_1 + \mu x_2)$. On en déduit que $x_2, x_1 \in k(x_1 + \lambda x_2)$. Ainsi $k(x_1, x_2, \ldots, x_n) = k(x_1 + \lambda x_2, x_3, \ldots, x_n)$.

Théorème de l'élément primitif

Proposition 214 Soit K une extension séparable et finie de k. Alors K est une extension monogène de k.

Preuve. On suppose k infini. Soit Ω une extension algébriquement close de k. Pour σ, τ deux morphismes de k-algèbres de K dans Ω, on considère la sous-extension de k donnée $\mathrm{K}_{\sigma,\tau} = \{x \in \mathrm{K}, \sigma(x) = \tau(x)\}$. Comme $[\mathrm{K} : k]_\mathrm{s}$ est fini, il existe $x \in \mathrm{K}$ tel que $\sigma(x) \neq \tau(x)$ pour tout $\sigma \neq \tau$. Le choix d'un tel x assure que $[k(x) : k]_\mathrm{s} \geqslant [\mathrm{K} : k]_\mathrm{s}$ puisque chacun des éléments de $\mathrm{Hom}_{k-\mathrm{alg}}(\mathrm{K}, \Omega)$ se restreint à $k(x)$ en un morphisme différent. De plus, on a $[k(x) : k]_\mathrm{s} \leqslant [\mathrm{K} : k]_\mathrm{s}$ puisque $k(x) \subset \mathrm{K}$.

Enfin, comme K est séparable, $k(x)$ l'est aussi et donc $[k(x) : k] = [k(x) : k]_\mathrm{s} = [\mathrm{K} : k]_\mathrm{s} = [\mathrm{K} : k]$. Finalement $\mathrm{K} = k(x)$.

Construction

Exemple 215 — Construction explicite d'éléments primitifs. Soient $\mathrm{K} = k(\alpha, \beta)$ une extension finie de corps avec β séparable sur k et Ω une extension algébriquement close de K. On note $\beta = \beta_1, \ldots, \beta_n$ les racines du polynôme minimal Q de β dans Ω et $\alpha = \alpha_1, \ldots, \alpha_m$ les racines du polynôme minimal P de α dans Ω. On considère $c \in k$ tel que

$$c \notin \left\{ \frac{\alpha - \alpha_j}{\beta_i - \beta}, \quad i \in [\![2\,,\, n]\!],\ j \in [\![1\,,\, m]\!] \right\} \cap k\,.$$

On a alors $k(\alpha, \beta) = k(\alpha + c\beta)$.

En effet, soit $\gamma = \alpha + c\beta$. Alors $\mathrm{P}(\gamma - c\mathrm{X}) \in k(\gamma)[\mathrm{X}]$ admet β comme racine mais aucun des β_i. Ainsi $\mathrm{X} - \beta = \mathrm{pgcd}(\mathrm{P}(\gamma - c\mathrm{X}), \mathrm{Q})$ puisque Q est séparable. Finalement $\beta \in k(\gamma)$ et comme $c \neq 0$, on a bien $k(\alpha, \beta) = k(\gamma)$.

4.3 Extension normale

Corps de décomposition : le retour

Définition 216 — Corps de décomposition d'une famille de polynôme. Soient k un corps et $\mathscr{F} = (\mathrm{P}_i)_{i \in \mathrm{I}}$ une famille d'éléments de $k[\mathrm{X}]$. *Un corps de décomposition* de la famille $\mathscr{F}$ est une extension K de k telle que tous les éléments de $\mathscr{F}$ sont scindés dans K et K est engendrée sur k par les racines des éléments de $\mathscr{F}$.

Remarque 217 — Une notion pas vraiment nouvelle. Si $\mathscr{F}$ a un seul élément alors c'est précisément la notion déjà vue.

Si $\mathscr{F} = (\mathrm{P}_1, \ldots, \mathrm{P}_n)$ est une famille finie alors un corps de décomposition pour $\mathscr{F}$ n'est rien d'autre qu'un corps de décomposition pour le polynôme $\mathrm{P} = \mathrm{P}_1 \cdots \mathrm{P}_n \in k[\mathrm{X}]$. Ainsi pour les familles finies, on est ramené à ce qu'on connaît déjà.

Corps de décomposition d'une famille

Proposition 218 — Existence et unicité du corps de décomposition. Soient k un corps et $\mathscr{F} = (\mathrm{P}_i)_{i \in \mathrm{I}}$ une famille d'éléments de $k[\mathrm{X}]$. Il existe un corps de décomposition pour la famille $\mathscr{F}$. Si K et K′ sont deux corps de décomposition pour la famille $\mathscr{F}$ alors ils sont k-isomorphes.

Plus généralement, si K est un corps de décomposition et L une extension de K dans laquelle tous les P_i sont scindés alors il existe un k-morphisme de K dans L.

Preuve. *Existence.* Considérons Ω une extension algébriquement close de k. Dans Ω, on pose K l'extension engendrée par les racines de l'ensemble des P_i. Comme Ω est algébriquement clos, les P_i sont scindés dans Ω et donc dans K et par définition K est bien sûr engendrée sur k par les racines des P_i.

Unicité. Considérons L une extension de k dans laquelle tous les P_i sont scindés et $j : \mathrm{L} \to \Omega$ une extension algébriquement close. Bien sûr, les P_i sont scindés sur $j(\mathrm{L})$. Il existe un k-morphisme $\sigma : \mathrm{K} \to \Omega$. Comme K est engendrée par les racines des P_i et que σ envoie une racine de P_i dans K sur une racine de P_i dans Ω , $\sigma(\mathrm{K})$ est contenue dans $j(\mathrm{L})$. Ainsi, on peut factoriser σ par j.

$$\begin{tikzcd}
\mathrm{K} \arrow[rr, dotted, "j^{-1}\circ\sigma"'] \arrow[rrr, bend left, "\sigma"] & & \mathrm{L} \arrow[r, "j"] & \Omega \\
& k \arrow[ul] \arrow[ur] & &
\end{tikzcd}$$

Si K et K′ sont deux corps de décompositions de $\mathscr{F}$ alors il existe un k-morphisme σ de K dans K′ et un K′ dans K (noté τ), on obtient ainsi un k-endomorphisme de K (c'est $\tau\sigma$) et un de K′ (c'est $\sigma\tau$) qui sont donc des automorphismes puisque K et K′ sont algébriques sur k. Ainsi τ et σ sont surjectifs.

EXTENSION NORMALE

Définition 219 — Extension normale. Soit K une extension algébrique de k. On dit que K est une *extension normale de k* si pour tout P polynôme irréductible sur k ayant une racine dans K alors P est scindé dans K.

Définition 220 — Extension séparable. Soit K une extension algébrique de k. On dit que K est une *extension séparable de k* si pour tout P polynôme irréductible sur k ayant une racine dans K alors P est à racines simples dans K.

Exercice 53 Montrer que k est une extension normale de k.

Si Ω est une clôture algébrique de k, montrer que Ω est une extension normale de k.

Si K est une extension de degré 2 de k, montrer que K est normale sur k.

$\mathbb{Q}(\sqrt[4]{2})$ n'est pas une extension normale de $\mathbb{Q}$. Mais $\mathrm{L}(\sqrt[4]{2})$ est une extension normale de $\mathrm{L} = \mathbb{Q}(i)$.

Caractérisation

Proposition 221 — Caractérisation des extensions normales. Soit K une extension algébrique de k. On désigne par L une extension de k, par Ω une extension algébriquement close de k, par M une k-extension contenant K, par $\widetilde{\Omega}$ une extension algébrique close contenant K et par σ, σ' des k-morphismes. Les morphismes σ et σ' désignent des morphismes d'extensions de k. On a alors les équivalences

- (i) K est une extension normale de k ;
- (ii) K est le corps de décomposition d'une famille $\mathscr{F}$ de $k[\mathrm{X}]$;
- (iii) Pour toute L et tout $\sigma, \sigma' : \mathrm{K} \to \mathrm{L}$, on a $\sigma(\mathrm{K}) = \sigma'(\mathrm{K})$;
- (iv) Pour tout $\sigma, \sigma' : \mathrm{K} \to \Omega$, on a $\sigma(\mathrm{K}) = \sigma'(\mathrm{K})$;
- (v) Pour toute M et tout $\sigma : \mathrm{K} \to \mathrm{M}$, on a $\sigma(\mathrm{K}) = \mathrm{K}$;
- (vi) Pour toute M et tout $\sigma : \mathrm{K} \to \mathrm{M}$, on a $\sigma(\mathrm{K}) \subset \mathrm{K}$;
- (vii) Pour tout $\sigma : \mathrm{K} \to \widetilde{\Omega}$, on a $\sigma(\mathrm{K}) = \mathrm{K}$
- $(viii)$ Pour tout $\sigma : \mathrm{K} \to \widetilde{\Omega}$, on a $\sigma(\mathrm{K}) \subset \mathrm{K}$

Preuve. $(v) \Leftrightarrow (vi)$ et $(vii) \Leftrightarrow (viii)$ résultent du fait que σ définit par restriction un endomorphisme d'une extension algébrique de k qui est donc un automorphisme.

De plus, on a évidemment $(v) \Rightarrow (vii)$ et $(iii) \Rightarrow (iv)$.

$(iv) \Rightarrow (iii)$. Considérons $\sigma, \sigma' : \mathrm{K} \to \mathrm{L}$. Comme K est algébrique sur k, σ et σ' sont à valeurs dans l'ensemble $\mathrm{L}' = \{x \in \mathrm{L}, x \text{ algébrique sur } k\}$. On en déduit que $\sigma, \sigma' : \mathrm{K} \to \mathrm{L}'$. Par ailleurs, comme L′ est algébrique sur k, il existe un morphisme de k-extensions $j : \mathrm{L}' \to \Omega$. On peut alors définir $j\sigma$ et $j\sigma'$ qui sont des morphismes de k-extensions de K dans Ω. On en déduit que $j\sigma(\mathrm{K}) = j\sigma'(\mathrm{K})$ et $\sigma(\mathrm{K}) = \sigma'(\mathrm{K})$ puisque j est injective.

$(vii) \Rightarrow (v)$. Considérons $\sigma : \mathrm{K} \to \mathrm{L}$ alors σ est à valeurs dans $\mathrm{M}' = \{x \in \mathrm{M}, x \text{ algébrique sur } k\}$. On en déduit que $\sigma : \mathrm{K} \to \mathrm{M}'$. Par ailleurs, comme M′ est algébrique sur k, on a $\mathrm{M}' \subset \widetilde{\Omega}$. On peut alors considérer σ comme un morphisme de k-extensions de K dans $\widetilde{\Omega}$. On en déduit que $\sigma(\mathrm{K}) = \mathrm{K}$.

$(i) \Rightarrow (ii)$. Considérons $\mathscr{F}$ la famille des polynômes irréductibles sur k ayant une racine dans K. Par hypothèse tous les polynômes sont scindés dans K et tout élément de K est racine d'un tel polynôme (son polynôme minimal) puisque K est algébrique. Ainsi K est bien engendré sur k par les racines des éléments de $\mathscr{F}$.
$(ii) \Rightarrow (iii)$. Comme K est engendré par les racines des éléments de $\mathscr{F}$, $\sigma(\mathrm{K})$ est engendré par les racines des éléments de $\mathscr{F}$ dans L. Ainsi $\sigma(\mathrm{K})$ est complètement déterminée.
$(iii) \Rightarrow (v)$. Il suffit de prendre $\sigma' = \mathrm{id}_{\mathrm{M}}$.
$(vii) \Rightarrow (i)$. Considérons $\mathrm{P} \in k[\mathrm{X}]$ un polynôme irréductible ayant une racine x dans K. On note $\{x = x_1, \ldots, x_n\}$ l'ensemble des racines de P dans $\widetilde{\Omega}$. La propriété universelle des corps de rupture assure que pour tout i, il existe un k-(iso)morphisme $\tau_i : k(x) \to k(x_i)$ envoyant x sur x_i. Comme $k(x_i) \subset \widetilde{\Omega}$ et que $\widetilde{\Omega}$ est algébriquement clos, chacun des τ_i se prolonge à K en $\sigma_i : \mathrm{K} \to \widetilde{\Omega}$. On a alors $\sigma_i(x) = x_i \in \mathrm{K}$ et P est scindé dans K.

Extension normale et automorphisme

Application 222 — Normalité et automorphisme. Soit K une extension algébrique de k, on a
$$|\mathrm{Aut}_k(\mathrm{K})| = |\mathrm{Hom}_{k-\mathrm{alg.}}(\mathrm{K}, \mathrm{K})| \leqslant [\mathrm{K} : k]_{\mathrm{s}}.$$

En effet, K est algébrique sur k, donc tout k-endomorphisme de K est un automorphisme de K. Par ailleurs, si Ω est une extension algébriquement close de k et $j : \mathrm{K} \to \Omega$ un morphisme de k-extensions alors les $j\sigma : \mathrm{K} \to \Omega$ pour $\sigma \in \mathrm{Aut}_k(\mathrm{K})$ forment une famille d'éléments deux à deux distincts (puisque j est injectif).

Le groupe $\mathrm{Aut}_k(\mathrm{K})$ est noté $\mathrm{Gal}(\mathrm{K}/k)$ ou $\mathrm{Gal}_k(\mathrm{K})$.

De plus, si K est une extension normale de k, on a
$$|\mathrm{Gal}(\mathrm{K}/k)| = [\mathrm{K} : k]_{\mathrm{s}}.$$

En effet, considérons $\widetilde{\Omega}$ une extension algébriquement close contenant K. Le critère (vii) de normalité assure que $\mathrm{Hom}_{k-\mathrm{alg.}}(\mathrm{K}, \widetilde{\Omega}) = \mathrm{Hom}_{k-\mathrm{alg.}}(\mathrm{K}, \mathrm{K})$.

Extension normale de dimension finie

Remarque 223 — Extension normale finie. Soit K une extension finie de k. Alors K est normale sur k si et seulement si K est le corps de décomposition d'un polynôme.

En effet, comme K est finie sur k, on peut écrire $\mathrm{K} = k(x_1, \ldots, x_n)$ et K est le corps de décomposition de $\mathrm{P} = \mathrm{P}_1 \cdots \mathrm{P}_n \in k[\mathrm{X}]$ où P_i est le polynôme minimal de x_i sur k. En effet, P est scindé puisque chacun des P_i l'est (puisque K est normale sur k) et K est bien engendré par les racines de P (puisqu'il l'est déjà par $x_1, \ldots, x_n$ qui sont des racines de P).

Extension galoisienne

Remarque 224 — Extension normale et séparable finie. Soit K une extension finie. de k Alors K est normale et séparable sur k si et seulement si K est le corps de décomposition d'un polynôme irréductible séparable.
(⇒) En effet, comme K est finie et séparable sur k, on peut écrire $\mathrm{K} = k(x)$ et K est le corps de décomposition de $\mathrm{P} \in k[\mathrm{X}]$ le polynôme minimal de x sur k. En effet, P est scindé (puisque K est normale sur k) et K est bien engendré par les racines de P (puisqu'il l'est déjà par x qui sont des racines de P).
(⇐) K est normale sur k puisque K est un corps de décomposition sur k et K est séparable sur k puisque K est engendré par des éléments séparable sur k (les racines du polynôme irréductible).

Exemples

Exemple 225 — Un exemple classique. L'extension $\mathbb{Q}(j, \sqrt[3]{2}) = \mathbb{Q}(\sqrt[3]{2}, j\sqrt[3]{2}, j^2\sqrt[3]{2})$ est normale : c'est le corps de décomposition de $\mathrm{X}^3 - 2$. Par contre, l'extension $\mathbb{Q}(\sqrt[3]{2})$ ne l'est pas : le polynôme $\mathrm{X}^3 - 2$ est irréductible sur $\mathbb{Q}$ mais n'a pas toutes ses racines dans $\mathbb{Q}(\sqrt[3]{2})$.

Ainsi une sous-extension d'une extension normale n'est pas nécessairement normale.

Exemple 226 — Normalité et transitivité. L'extension $\mathbb{Q}(\sqrt{2})$ est normale de $\mathbb{Q}$ puisqu'elle est de degré 2, de même, l'extension $\mathbb{Q}(\sqrt[4]{2})$ de $\mathbb{Q}(\sqrt{2})$ est normale. Mais l'extension $\mathbb{Q}(\sqrt[4]{2})$ de $\mathbb{Q}$ n'est pas normale puisque le polynôme $X^4 - 2$ irréductible sur $\mathbb{Q}$ n'a pas toutes ses racines dans $\mathbb{Q}(\sqrt[4]{2})$.

Ainsi la normalité n'est pas une propriété transitive.

Les restes de la transitivité

Remarque 227 Soient K une extension de k et L une extension de K. On suppose que l'extension L de k est normale. Alors L est une extension normale de K.

En effet, si L est le corps de décomposition sur k d'une famille $\mathscr{F}$ alors L est encore le corps de décomposition de $\mathscr{F}$ sur K.

4.4 Clôture normale

Définition 228 — Clôture normale. Soit K une extension de k. Une *clôture normale* de K est une extension N de K vérifiant les deux propriétés suivantes :

- N est normale sur k ;
- Si N′ est une sous-**K**-extension de N telle que N′ soit normale sur k alors $N' = N$.

Proposition 229 — Existence et unicité de la clôture normale. Soit K une extension algébrique de k. Alors K admet une clôture normale N.

De plus, si $\sigma : K \to M$ est un k-morphisme à valeurs dans M une extension **normale** de k. Alors il existe un **K**-morphisme de N dans M (c'est-à-dire un « prolongement » de σ à N).

$$\begin{tikzcd} N \arrow[rr, dotted] & & M \\ & K \arrow[ul] \arrow[ur, "\sigma"'] & \\ & k \arrow[u] \arrow[ul] & \end{tikzcd}$$

En particulier, deux clôtures normales de K sont K-isomorphes.

Preuve. *Existence.* Soit N un corps de décomposition de la famille $\mathscr{F}$ des polynômes irréductibles sur k ayant une racine dans K.

Montrons que N est une clôture normale de K sur k.

L'extension N de k est normale.

Montrons à présent que N est bien une extension de K. Comme deux corps de décomposition de $\mathscr{F}$ sont k-isomorphes, il suffit de trouver un corps de décomposition M de l'ensemble des polynômes irréductibles sur k qui est une extension de K. On aura alors $j : K \to M$ et par composition avec un k-isomorphisme $\sigma : M \to N$, on obtiendra que N est une extension de K.

On considère alors M le corps de décomposition de $\mathscr{F}$ formé de l'ensemble des racines des éléments de $\mathscr{F}$ dans une extension algébriquement close Ω de k. Comme Ω est algébriquement clos, il existe un k-morphisme τ de K dans Ω. De plus, si $x \in K$ alors le polynôme minimal P est dans $\mathscr{F}$ et donc $\tau(x) \in M$ est une racine de P dans Ω. Ainsi $\tau : K \to M$.

Considérons à présent N′ une sous-K-extension N qui est normale sur k. Pour tout $x \in K$, le polynôme minimal de $x \in K$ sur k admet une racine dans N′ (puisque N′ est une sous-K-extension) donc est scindé dans N′ (puisque $(N' : k)$ est normale). Ainsi N′ contient toutes les racines des éléments de $\mathscr{F}$ et donc $N \subset N'$ puisque N est engendrée par ces racines.

Montrons à présent qu'une clôture normale N est toujours un corps de décomposition sur K de la famille $\mathscr{F}$. Comme N est une extension de K, tout élément P de $\mathscr{F}$ a une racine dans N (l'image d'une racine de P dans K par le morphisme de K dans N est une racine de P dans N) donc est scindé dans N (puisque N est normale sur k). La sous-k-extension N_1 de N engendrée par les racines des éléments de $\mathscr{F}$ dans N est alors le corps de décomposition de $\mathscr{F}$ contenu dans N. En particulier, c'est une sous-K-extension de N qui est normale sur k et donc $N = N_1$ puisque N est une clôture normale.

Propriété de morphismes. Soit M une extension de K qui est normale sur k. On note $j : K \to \Omega$ une extension algébriquement close. Comme Ω est algébriquement clos, Ω est une K-extension de M et de N. On a

$$\begin{tikzcd} N \arrow[rr, "\sigma"] & & \Omega \\ & M \arrow[ur, "\tau"'] & \\ & K \arrow[ul] \arrow[u] & \end{tikzcd}$$

Tout élément de $\mathscr{F}$ admet une racine dans M (puisque c'est une K-extension) et donc est scindé dans M (puisque $(\mathrm{M} : k)$ est normale). Ainsi, tout élément de $\mathscr{F}$ est scindé dans M et donc dans $\tau(\mathrm{M})$.

Comme N est un corps de décomposition pour $\mathscr{F}$ sur k, N (resp. $\sigma(\mathrm{N})$) est engendré sur k par les racines des éléments de $\mathscr{F}$ dans N (resp. $\sigma(\mathrm{N})$). Or les racines des éléments de $\mathscr{F}$ sont dans $\tau(\mathrm{M})$. Ainsi $\sigma(\mathrm{N}) \subset \tau(\mathrm{M})$ et on peut considérer « $\tau^{-1}\sigma$ ».

Propriété de morphismes.

Soit M une extension de K qui est normale sur k. On note $j : \mathrm{K} \to \Omega$ une extension algébriquement close. Comme Ω est algébriquement clos, Ω est une K-extension de M et de N. On a

$$\begin{tikzcd}
\mathrm{N} \arrow[rr, dotted, "\sigma"] \arrow[rrr, bend left, "\sigma"] & & \mathrm{M} \arrow[r, "\tau"] & \Omega \\
& \mathrm{K} \arrow[ul, "\tau^{-1}\sigma"] \arrow[ur] & &
\end{tikzcd}$$

Tout élément de $\mathscr{F}$ admet une racine dans M (puisque c'est une K-extension) et donc est scindé dans M (puisque $(\mathrm{M} : k)$ est normale). Ainsi, tout élément de $\mathscr{F}$ est scindé dans M et donc dans $\tau(\mathrm{M})$.

Comme N est un corps de décomposition pour $\mathscr{F}$ sur k, N (resp. $\sigma(\mathrm{N})$) est engendré sur k par les racines des éléments de $\mathscr{F}$ dans N (resp. $\sigma(\mathrm{N})$). Or les racines des éléments de $\mathscr{F}$ sont dans $\tau(\mathrm{M})$. Ainsi $\sigma(\mathrm{N}) \subset \tau(\mathrm{M})$ et on peut considérer « $\tau^{-1}\sigma$ ».

Unicité.

Si N et N′ sont deux clôtures normales de K alors il existe un K-morphisme σ de N dans N′ et un de N′ dans N (noté τ), on obtient ainsi un K-endomorphisme de N (c'est $\tau\sigma$) et un de N′ (c'est $\sigma\tau$) qui sont donc des automorphismes puisque N et N′ sont algébriques sur K. Ainsi τ et σ sont surjectifs.

Remarque 230 — Autre preuve. Démontrer la « propriété de morphismes » et « l'unicité » en démontrant qu'une extension normale est un corps de décomposition de $\mathscr{F}$ sur K (et pas seulement sur k).

4.5 Théorème de correspondance de Galois

Problématique

Soit K une extension de k. On cherche à comprendre la structure d'extension de K et pour cela à déterminer toutes les sous-k-extensions de K. Même si $[\mathrm{K} : k] < +\infty$, K peut avoir une infinité de sous-extension : en effet, on a vu que pour une extension finie, le nombre de sous-extension est finie si et seulement l'extension est monogène ; de plus on a vu qu'une extension séparable est toujours toujours monogène. Ainsi, il est raisonnable de ne considérer que les extensions séparables.

Par ailleurs, une façon de produire des sous-extensions de K est de considérer les sous-extensions de la forme

$$\mathrm{K}^{\mathrm{H}} = \{x \in \mathrm{K}, \qquad \forall\, \sigma \in \mathrm{H}, \quad \sigma(x) = x\}$$

où H est une sous-groupe de $\mathrm{G} = \mathrm{Gal}(\mathrm{K}/k) = \mathrm{Aut}_k(\mathrm{K})$.

Pour avoir une chance de décrire toutes les sous-extensions de K par cette méthode, il faut que G soit aussi gros que possible c'est-à-dire que $|\mathrm{G}| = [\mathrm{K} : k]_{\mathrm{s}}$ et on a vu que cette condition signifiait que K était une extension normale de k (au moins si $[\mathrm{K} : k]_{\mathrm{s}}$ était finie). En effet, pour $j : \mathrm{K} \to \Omega$, l'application

$$\begin{cases} \mathrm{G} \longrightarrow \mathrm{Hom}_{k-\mathrm{ext.}}(\mathrm{K}, \Omega) \\ \sigma \longmapsto j \circ \sigma \end{cases}$$

est injective.

Finalement, les extensions qui vont nous intéresser sont les extensions à la fois normale et séparable.

Définition 231 — Extension galoisienne. Soit K une extension de k. On dit que K est une *extension galoisienne* de k si K est une extension normale et séparable de k.

Extension galoisienne

Proposition 232 — Caractérisation des extensions galoisiennes. Soit K une extension algébrique de k. On note $\mathrm{G} = \mathrm{Gal}(\mathrm{K}/k)$. Les propositions suivantes sont équivalentes

(*i*) K est une extension galoisienne de k

(*ii*) $\mathrm{K}^{\mathrm{G}} = k$

(*iii*) Tout polynôme irréductible sur k ayant une racine dans K est scindé à racine simple dans K

(*iv*) Pour tout $x \in \mathrm{K}$, le polynôme minimal de x sur k se factorise dans $\mathrm{K}[\mathrm{X}]$ en produit de polynômes distincts de degré 1

(*v*) K est le corps de décomposition d'une famille $\mathscr{F}$ formée de polynômes $\mathrm{P} \in k[\mathrm{X}]$ vérifiant $\mathrm{pgcd}(\mathrm{P}, \mathrm{P}') = 1$.

De plus si $[\mathrm{K} : k] < +\infty$, les conditions précédentes sont équivalentes à

(*vi*) $|\mathrm{G}| = [\mathrm{K} : k]$.

Preuve. $(iii) \Leftrightarrow (iv)$. Un polynôme irréductible sur k ayant une racine dans K est proportionnel au polynôme minimal de cette racine. Inversement, le polynôme minimal de $x \in \mathrm{K}$ est irréductible sur K et admet une racine dans K.
$(i) \Rightarrow (v)$. K est normal sur k donc K est le corps de décomposition de la famille des polynômes irréductibles sur k ayant une racine dans K ou ce qui revient au même de la familles des polynômes minimaux sur k des éléments de K. Comme K est séparable sur k ces polynômes sont séparables et donc $\mathrm{pgcd}(\mathrm{P}, \mathrm{P}') = 1$.
$(v) \Rightarrow (i)$. K est normale puisque c'est un corps de décomposition. De plus, K est engendrée sur k par les racines des éléments de $\mathscr{F}$. Or le polynôme minimal d'une racine d'un élément de $\mathscr{F}$ est séparable car il divise un élément de $\mathscr{F}$ et que les éléments de $\mathscr{F}$ sont à racines simples dans une extension suffisamment grande. Ainsi K est engendrée sur k par des éléments séparables et donc K est séparable sur k.
$(i) \Rightarrow (iii)$. Tout polynôme irréductible P sur k ayant une racine dans K est scindé puisque K est normale. Comme P est le polynôme minimal d'une de ces racines dans K et que K est séparable sur k alors P est séparable et donc à racines simples dans K.
$(iii) \Rightarrow (i)$. Tout polynôme irréductible sur k ayant une racine dans K étant scindé dans K, l'extension K est normale sur k. De plus le polynôme minimal d'un élément $x \in \mathrm{K}$ est irréductible sur k et a une racine dans K donc est à racines simples dans K et il est donc séparable. Ainsi K est séparable sur k.
$(i) \Rightarrow (ii)$. On a bien sûr $k \subset \mathrm{K}^{\mathrm{G}}$ puisque tous les éléments de G sont k-linéaires. On fixe à présent une extension algébriquement close Ω de K contenant K. Si $x \in \mathrm{K} \smallsetminus k$ le polynôme minimal de x sur K est de degré supérieur ou égal à 2 et admet donc une racine y distincte de x puisque x est séparable sur k. Il existe alors un (unique) k-morphisme $\tau : k(x) \to \Omega$ tel que $\tau(x) = y$. Ce morphisme se prolonge en un morphisme $\sigma : \mathrm{K} \to \Omega$. De plus, comme K est normale sur k, on a $\sigma(\mathrm{K}) = \mathrm{K}$ et $\sigma \in \mathrm{Gal}(\mathrm{K}/k)$. Ainsi, si $x \notin k$ alors il existe $\sigma \in \mathrm{Gal}(\mathrm{K}/k)$ tel que $\sigma(x) = y \neq x$.
$(ii) \Rightarrow (iv)$. Soit $x \in \mathrm{K}$ et P le polynôme minimal de x sur k. On note $x = y_1, \ldots, y_\ell$ les racines distinctes de P dans K et $\mathrm{Q} = (\mathrm{X} - y_1) \cdots (\mathrm{X} - y_\ell)$. Pour tout $\sigma \in \mathrm{G}$, il existe j tel que $\sigma(y_i) = y_j$ (σ envoie les racines de P sur les racines de P). On en déduit que $\mathrm{Q} \in \mathrm{K}^{\mathrm{G}}[\mathrm{X}]$ et donc $\mathrm{Q} \in k[\mathrm{X}]$. Comme $\mathrm{Q} \mid \mathrm{P}$ et $\mathrm{P} \in k[\mathrm{X}]$ est irréductible, on en déduit que $\mathrm{P} = \mathrm{Q}$ est scindé à racines simples dans K.

Le cas des extensions finies. Pour une extension finie, on a $|\mathrm{G}| \leqslant [\mathrm{K} : k]_{\mathrm{s}} \leqslant [\mathrm{K} : k]$. De plus, on a $|\mathrm{G}| = [\mathrm{K} : k]_{\mathrm{s}}$ si et seulement si K est normale (puisque $[\mathrm{K} : k]_{\mathrm{s}}$ est fini) et $[\mathrm{K} : k]_{\mathrm{s}} = [\mathrm{K} : k]$ si et seulement si l'extension $k \to \mathrm{K}$ est séparable.

Remarque 233 – Extension finie galoisienne. Soit K une extension finie de k. On a déjà vu que L'extension K est galoisienne sur k si et seulement si K est le corps de décomposition d'un polynôme irréductible séparable sur k.

THÉORÈME DE CORRESPONDANCE

Soit K une extension algébrique de k. On note $\mathscr{E}$ l'ensemble des sous-k-extensions de K et $\mathscr{G}$ l'ensemble des sous-groupes de $\mathrm{G} = \mathrm{Gal}(\mathrm{K}/k)$.

Si $\mathrm{H} \in \mathscr{G}$, on a vu que $\mathrm{K}^{\mathrm{H}} := \{x \in \mathrm{K}, \quad \forall \sigma \in \mathrm{H}, \quad \sigma(x) = x\}$ est une sous-extension de K. On définit ainsi une application $\Phi : \mathrm{H} \in \mathscr{G} \mapsto \mathrm{K}^{\mathrm{H}} \in \mathscr{E}$.

Inversement, si $\mathrm{E} \in \mathscr{E}$ l'ensemble des $\sigma \in \mathrm{G}$ tel que $\sigma(x) = x$ pour tout $x \in \mathrm{E}$ est un sous-groupe de G qui n'est autre que $\mathrm{Gal}(\mathrm{K}/\mathrm{E})$. On définit ainsi une application $\Gamma : \mathrm{E} \in \mathscr{E} \mapsto \mathrm{Gal}(\mathrm{K}/\mathrm{E}) \in \mathscr{G}$.

Dans la suite, on va étudier ces applications. Par exemple, on a déjà vu que $\Phi(\mathrm{G}) = k$ si et seulement si K est galoisienne.

ATTENTION !!! Si $k \subset \mathrm{E} \subset \mathrm{K}$ est une suite d'extension, on a $\mathrm{Gal}(\mathrm{K}/\mathrm{E}) \leqslant \mathrm{Gal}(\mathrm{K}/k)$ mais on

n'a pas $\mathrm{Gal}(\mathrm{E}/k) \subset \mathrm{Gal}(\mathrm{K}/k)$. On verra que dans certains cas, $\mathrm{Gal}(\mathrm{E}/k)$ est un quotient de $\mathrm{Gal}(\mathrm{K}/k)$.

Premières propriétés

Proposition 234 Soient $\mathrm{E}, \mathrm{E}_1, \mathrm{E}_2 \in \mathscr{E}$ et $\mathrm{H}, \mathrm{H}_1, \mathrm{H}_2 \in \mathscr{G}$, on a alors les propriétés suivantes

(*i*) si $\mathrm{E}_1 \subset \mathrm{E}_2$ alors $\Gamma(\mathrm{E}_2) \subset \Gamma(\mathrm{E}_1)$
(*ii*) si $\mathrm{H}_1 \subset \mathrm{H}_2$ alors $\Phi(\mathrm{H}_2) \subset \Phi(\mathrm{H}_1)$
(*iii*) $\mathrm{E} \subset \Phi(\Gamma(\mathrm{E}))$
(*iv*) $\mathrm{H} \subset \Gamma(\Phi(\mathrm{H}))$
(*v*) $\Phi \circ \Gamma \circ \Phi = \Phi$ et $\Gamma \circ \Phi \circ \Gamma = \Gamma$
(*vi*) Pour $\sigma \in \mathrm{G}$, on a

$$\Gamma(\sigma(\mathrm{E})) = \sigma\Gamma(\mathrm{E})\sigma^{-1} \qquad \text{et} \qquad \Phi(\sigma\mathrm{H}\sigma^{-1}) = \sigma(\Phi(\mathrm{H})).$$

Preuve. (*i*) Un élément qui vaut l'identité sur E_2 vaut l'identité sur E_1.

(*ii*) Un élément qui est fixe par tous les éléments de H_2 est fixe par tous les éléments de H_1.

(*iii*) Un élément de E est fixe par tous les éléments du groupe de Galois de K sur E.

(*iv*) Un élément de H laisse fixe tous les éléments de K^{H} et donc est dans le groupe de Galois de K sur K^{H}.

(*v*) On a $\Phi(\mathrm{H}) \subset \Phi \circ \Gamma(\Phi(\mathrm{H}))$ d'après (*iii*). De plus, on a $\mathrm{H} \subset \Gamma(\Phi(\mathrm{H}))$ d'après (*iv*) et donc $\Phi(\Gamma(\Phi(\mathrm{H})) \subset \Phi(\mathrm{H})$ d'après (*ii*).

On a $\Gamma(\mathrm{E}) \subset \Gamma \circ \Phi(\Gamma(\mathrm{E}))$ d'après (*iv*). De plus, on a $\mathrm{E} \subset \Phi(\Gamma(\mathrm{E}))$ d'après (*iii*) et donc $\Gamma(\Phi(\Gamma(\mathrm{E})) \subset \Gamma(\mathrm{E})$ d'après (*i*).

(*vi*) On a $g \in \Gamma(\sigma(\mathrm{E}))$ si et seulement si $g\sigma(x) = \sigma(x)$ pour tout $x \in \mathrm{E}$ si et seulement si $\sigma^{-1}g\sigma(x) = x$ pour tout $x \in \mathrm{E}$ si et seulement si $\sigma^{-1}g\sigma \in \Gamma(\mathrm{E})$.

On a $x \in \Phi(\sigma\mathrm{H}\sigma^{-1})$ si et seulement si $\sigma h\sigma^{-1}(x) = x$ pour tout $h \in \mathrm{H}$ si et seulement si $h\sigma^{-1}(x) = \sigma^{-1}(x)$ pour tout $h \in \mathrm{H}$ si et seulement si $\sigma^{-1}(x) \in \mathrm{K}^{\mathrm{H}}$.

Caractérisation de l'image

Proposition 235 Soit $\mathrm{E} \in \mathscr{E}$. On a équivalence entre

(*i*) E est dans l'image de Φ
(*ii*) $\Phi(\Gamma(\mathrm{E})) = \mathrm{E}$
(*iii*) K est une extension galoisienne de E

Proposition 236 Soit $\mathrm{H} \in \mathscr{G}$. On a équivalence entre

(*i*) H est dans l'image de Γ
(*ii*) $\Gamma(\Phi(\mathrm{H})) = \mathrm{H}$

Corollaire 237 — Bijection. Γ et Φ induisent par restriction des bijections inverses l'une de l'autre entre l'image l'image de Φ et l'image de Γ.

Preuve. Si $\Phi(\Gamma(\mathrm{E})) = \mathrm{E}$ alors E est dans l'image de Φ. Si $\mathrm{E} = \Phi(\mathrm{H})$, on a bien $\mathrm{E} = \Phi(\mathrm{H}) = \Phi\Gamma(\Phi(\mathrm{H})) = \Phi(\Gamma(\mathrm{E}))$. On a $\Phi(\Gamma(\mathrm{E})) = \mathrm{K}^{\mathrm{Gal}(\mathrm{K}/\mathrm{E})}$. Ainsi $\mathrm{E} = \Phi(\Gamma(\mathrm{E}))$ si et seulement si $\mathrm{K}^{\mathrm{Gal}(\mathrm{K}/\mathrm{E})} = \mathrm{E}$ si et seulement si K est une extension galoisienne de E (car K est une extension algébrique de E).

Si $\mathrm{H} = \Gamma(\Phi(\mathrm{H}))$ alors H est dans l'image de Γ. Si $\mathrm{H} = \Gamma(\mathrm{E})$ alors $\mathrm{H} = \Gamma(\mathrm{E}) = \Gamma\Phi\Gamma(\mathrm{E}) = \Gamma\Phi(\mathrm{H})$.

Remarque 238 — Le cas d'une extension galoisienne. On suppose que K est galoisienne sur k. Alors toute extension E est dans l'image de Φ. En effet, K est galoisienne sur E par transitivité de la séparabilité et « ce qu'il reste de la transitivité pour les extensions normales ».

Problème : trouver une caractérisation de l'image de Γ. Besoin d'un ingrédient supplémentaire : la topologie de Krull

Lemme d'Artin

Proposition 239 — Lemme d'Artin. Soit L un corps et H un sous-groupe **fini** du groupe des automorphismes de L. Alors L est une extension galoisienne de L^{H} de degré $|\mathrm{H}|$ et de groupe de galois H.

Preuve. Soit $x \in \mathrm{L}$. On note $\{x_1 = x, x_2, \ldots, x_\ell\} = \{hx,\ h \in \mathrm{G}\}$ l'orbite de x sous l'action du groupe H avec $x_i \neq x_j$ si $i \neq j$. Le polynôme $\mathrm{Q(X)} = (\mathrm{X} - x_1) \cdots (\mathrm{X} - x_\ell) \in \mathrm{L^H[X]}$ est à racines simples et annule x. Ainsi x est algébrique et même séparable sur $\mathrm{L^H}$ et L est séparable sur $\mathrm{L^H}$.

Par ailleurs, si P est le polynôme minimal de x sur $\mathrm{L^H}$ et $h \in \mathrm{H}$. On a $\mathrm{P}(hx) = h(\mathrm{P}(x)) = 0$. Ainsi les x_i sont aussi racines de P et donc $\mathrm{Q} \mid \mathrm{P}$. Comme P est irréductible, on a $\mathrm{Q} = \mathrm{P}$. Le polynôme minimal de x est donc scindé dans L et L est une extension normale de $\mathrm{L^H}$.

L'extension L est bien galoisienne de $\mathrm{L^H}$.

Montrons à présent que $[\mathrm{L} : \mathrm{L^H}] \leqslant |\mathrm{H}|$. On a vu que c'est le cas pour toute sous-$\mathrm{L^H}$-extension monogène de L : $[\mathrm{L^H}(x) : \mathrm{L^H}] \leqslant |\mathrm{H}|$ pour tout $x \in \mathrm{L}$. Si $[\mathrm{L} : \mathrm{L^H}] < +\infty$ alors $[\mathrm{L} : \mathrm{L^H}] < |\mathrm{H}|$ car L est monogène car séparable et finie sur $\mathrm{L^H}$. Si $[\mathrm{L} : \mathrm{L^H}] = +\infty$, il existe $|\mathrm{H}| + 1$ éléments linéairement $\mathrm{L^H}$-indépendants dans L. L'extension engendrée par ces éléments est alors finie (puisque algébrique et de type fini) et séparable sur $\mathrm{L^H}$ donc monogène. Ainsi son degré sur $\mathrm{L^H}$ est majoré par $|\mathrm{H}|$ ce qui est absurde.

On a alors $[\mathrm{L} : \mathrm{L^H}] \leqslant |\mathrm{H}| \leqslant |\mathrm{Gal(L/L^H)}| \leqslant [\mathrm{L} : \mathrm{L^H}]$. La deuxième inégalité résulte du fait que $\mathrm{H} \subset \mathrm{Gal(L/L^H)}$, la troisième inégalité du fait que $[\mathrm{L} : \mathrm{L^H}]$ est fini. On en déduit alors que $\mathrm{H} = \mathrm{Gal(L/L^H)}$ et $|\mathrm{H}| = [\mathrm{L} : \mathrm{L^H}]$.

Corollaire 240 Tout sous-groupe fini H de $\mathrm{Gal}(\mathrm{K}/k)$ est dans l'image de Γ : en effet, d'après le lemme d'Artin, $\mathrm{H} = \mathrm{Gal(K/K^H)}$.

Le théorème de correspondance de Galois

Théorème 241 Soit K une extension galoisienne **finie** de k. Les applications Φ et Γ définissent des bijections réciproques l'une de l'autre entre l'ensemble $\mathscr{E}$ des sous-k-extensions de K et l'ensemble $\mathscr{G}$ des sous-groupes de $\mathrm{G} = \mathrm{Gal}(\mathrm{K}/k)$.

Dans cette bijection le degré sur k et l'indice se correspondent : si $\mathrm{E} = \mathrm{K^H}$ ou $\mathrm{H} = \mathrm{Gal(K/E)}$, on a $|\mathrm{H}| = [\mathrm{K} : \mathrm{K^H}]$ et $|\mathrm{G}| = [\mathrm{K} : \mathrm{K^G}] = [\mathrm{K} : k]$. Ainsi par multiplicativité, on a $(\mathrm{G} : \mathrm{H}) = [\mathrm{K^H} : k]$.

Preuve. On a vu que tout sous-extension E de K est telle que K est galoisienne sur k et est donc dans l'image de Φ. De plus, comme G est fini, tout sous-groupe de G est dans l'image de Γ. Enfin Φ et Γ sont des bijections réciproques l'une de l'autre entre l'image de Γ et l'image de Φ.

Proposition 242 – Complément à la correspondance. Soit K une extension galoisienne **finie** de k de groupe G. On considère H un sous-groupe de G et E une sous-k-extension de K qui se correspondent dans la bijection précédente c'est-à-dire $\mathrm{H} = \mathrm{Gal(K/E)}$ et $\mathrm{E} = \mathrm{K^H}$.

On a les équivalences

(*i*) H est distingué dans G
(*ii*) E est normale sur k
(*iii*) E est galoisienne sur k
(*iv*) $\sigma(\mathrm{E}) = \mathrm{E}$ pour tout $\sigma \in \mathrm{G}$

Dans ce cas, le groupe de Galois $\mathrm{Gal}(\mathrm{E}/k)$ s'identifie par l'application restriction à G/H.

Preuve. (*ii*) $\Leftrightarrow$ (*iii*). Comme E est séparable sur k (puisque K l'est), E est normale sur k si et seulement si E est galoisienne sur k.
(*i*) $\Leftrightarrow$ (*iv*). Comme Φ et Γ sont des bijections inverses l'une de l'autre « compatible avec l'action de G », on a $\sigma(\mathrm{E}) = \mathrm{E}$ pour tout $\sigma \in \mathrm{G}$ si et seulement si $\mathrm{H} = \Phi(\mathrm{E}) = \Phi(\sigma(\mathrm{E})) = \sigma\Phi(\mathrm{E})\sigma^{-1} = \sigma\mathrm{H}\sigma^{-1}$ pour tout $\sigma \in \mathrm{G}$.
(*iii*) $\Rightarrow$ (*i*). Si E galoisienne sur k alors on peut définir le morphisme de groupe

$$r : \begin{cases} \mathrm{Gal}(\mathrm{K}/k) \longrightarrow \mathrm{Gal}(\mathrm{E}/k) \\ \quad \sigma \qquad \longmapsto \sigma_{|\mathrm{E}} \end{cases}$$

En effet, $\sigma(\mathrm{E}) = \mathrm{E}$ car E est normale sur k. Le noyau de r est $\mathrm{H} = \mathrm{Gal(K/E)}$ qui est donc distingué dans G.
(*iv*) $\Rightarrow$ (*iii*). Par hypothèse le morphisme r est bien défini et de noyau H. On en déduit que G/H s'identifie à un sous-groupe de $\mathrm{Gal}(\mathrm{E}/k)$. Ainsi $|\mathrm{G/H}| = [\mathrm{E} : k] \leqslant |\mathrm{Gal}(\mathrm{E}/k)|$. Comme $|\mathrm{Gal}(\mathrm{E}/k)| \leqslant [\mathrm{E} : k]$, on en déduit que $|\mathrm{Gal}(\mathrm{E}/k)| = [\mathrm{E} : k]$ et E est galoisienne.

Lorsque les propriétés sont vérifiées, on obtient par cardinalité que r est surjective et ainsi r définit par passage au quotient un isomorphisme entre G/H et $\mathrm{Gal}(\mathrm{E}/k)$.

Exercice 54 — Surjectivité de r. À l'aide du lemme du prolongement et de la normalité de E, donner une autre démonstration de la surjectivité de r.

Groupe de Galois et permutation

Soit $\mathrm{P} \in k[\mathrm{X}]$ un polynôme dont tous les facteurs irréductibles sont séparables. Le corps de décomposition de P sur k noté $\mathrm{D}_k(\mathrm{P})$ est alors une extension galoisienne de k et on note $\mathrm{Gal}_k(\mathrm{P}) := \mathrm{Gal}(\mathrm{D}_k(\mathrm{P})/k)$ le **groupe de Galois de** P.

Soient $\mathrm{Rac}(\mathrm{P}) = \{x_1, \ldots, x_n\}$ l'ensemble des racines de P. Pour $\sigma \in \mathrm{Gal}_k(\mathrm{P})$ et x_i une racine de P, on a $\mathrm{P}(\sigma(x_i)) = \sigma(\mathrm{P}(x_i)) = 0$. On peut ainsi définir une action de $\mathrm{Gal}_k(\mathrm{P})$ sur $\mathrm{Rac}(\mathrm{P})$ par

$$\begin{cases} \mathrm{Gal}_k(\mathrm{P}) \times \mathrm{Rac}(\mathrm{P}) \longrightarrow \mathrm{Rac}(\mathrm{P}) \\ \qquad (\sigma, x) \qquad\quad \longmapsto \sigma(x) \end{cases}$$

Le morphisme de groupe associé à cette action permet alors de définir un morphisme de groupes $\mathrm{Gal}_k(\mathrm{P})$ dans $\mathfrak{S}_n$. De plus, ce morphisme est injectif (c'est-à-dire l'action est fidèle) puisque $\mathrm{D}_k(\mathrm{P})$ est engendré par les x_i.

Ainsi $\mathrm{Gal}_k(\mathrm{P})$ s'identifie à un sous-groupe de $\mathfrak{S}_n$.

Action transitive et irréductibilité

Lemme 243 Soit $\mathrm{P} \in k[\mathrm{X}]$ un polynôme dont tous les facteurs irréductibles sont séparables. Le groupe $\mathrm{Gal}_k(\mathrm{P})$ agit transitivement sur les racines de P si et seulement si P est une puissance d'un irréductible.

Si P est une puissance d'un irréductible Q et x, y deux racines de P donc de Q dans $\mathrm{D}_k(\mathrm{P})$. Il existe un morphisme τ de $k(x)$ dans $\mathrm{D}_k(\mathrm{P})$ qui envoie x sur y. Comme le polynôme P est scindé dans $\mathrm{D}_k(\mathrm{P})$, on peut prolonger τ en un (auto)morphisme σ de $\mathrm{D}_k(\mathrm{P})$. Ainsi, il existe $\sigma \in \mathrm{Gal}_k(\mathrm{P})$ tel que $\sigma(x) = y$.

Si P n'est pas une puissance d'un irréductible, P admet deux facteurs irréductibles premiers entre eux P_1 et P_2 qui n'ont donc de racines communes dans aucune extension (en effet, il existe $\mathrm{U}, \mathrm{V} \in k[\mathrm{X}]$ tel que $\mathrm{UP}_1 + \mathrm{VP}_2 = 1$). Si x est une racine de P_1 et y une racine de P_2 dans $\mathrm{D}_k(\mathrm{P})$, un élément de $\mathrm{Gal}_k(\mathrm{P})$ enverra x sur une racine de P_1 et donc ne l'enverra jamais sur y.

Constructibilité : fin

Il restait à montrer que si p est un nombre premier de Fermat alors $\zeta := \exp(2i\pi/p)$ est constructible.

On a vu que $\mathbb{Q}(\zeta)$ est une extension de degré $p - 1 = 2^{2^n}$ de $\mathbb{Q}$.

On est en caractéristique 0 donc $\mathbb{Q}(\zeta)$ est séparable sur $\mathbb{Q}$.

Par ailleurs, pour $j \in [\![0, p-1]\!]$, les ζ^j sont des racines distinctes de $\mathrm{X}^p - 1$ qui est scindé dans $\mathbb{Q}$. Et $\mathbb{Q}(\zeta)$ est engendré sur $\mathbb{Q}$ par les racines de $\mathrm{X}^p - 1$. Finalement, $\mathbb{Q}(\zeta)$ est une extension normale de $\mathbb{Q}$.

On en déduit que $\mathbb{Q}(\zeta)$ est une extension galoisienne de $\mathbb{Q}$. Et donc $|\mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q})| = [\mathbb{Q}(\zeta) : \mathbb{Q}] = 2^{2^n}$. En particulier $\mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q})$ est un 2-groupe.

Lemme 244 Soit p un nombre premier et G un p-groupe (c'est-à-dire $|\mathrm{G}| = p^m$ pour $m \in \mathbb{N}$). Il existe une suite de sous-groupes $\{1\} = \mathrm{G}_0 \subset \mathrm{G}_1 \subset \cdots \subset \mathrm{G}_m = \mathrm{G}$ vérifiant $(\mathrm{G}_i : \mathrm{G}_{i-1}) = p$ pour $i \geqslant 1$.

Preuve. On raisonne par récurrence sur m. C'est évident si $m = 0$ et $m = 1$. On suppose $m \geqslant 2$ et on suppose le résultat vrai pour les groupes d'ordre p^n avec $n < m$.

Si G est abélien, on choisit $x \in \mathrm{G} \smallsetminus \{1\}$.

Si $\langle x \rangle = \mathrm{G}$ alors G est cyclique et le résultat est vrai d'après la structure des groupes cycliques.

Si $\langle x \rangle \neq \mathrm{G}$, on applique l'hypothèse de récurrence au groupe $\mathrm{G}/\langle x \rangle$ et on obtient ainsi en relevant le groupe du quotient dans G une suite $\mathrm{H}_0 = \langle x \rangle \subset \mathrm{H}_1 \subset \cdots \subset \mathrm{G}$. En appliquant l'hypothèse de récurrence à $\langle x \rangle$ on conclut.

Si G n'est pas abélien alors $1 \neq \mathrm{ZG} \neq \mathrm{G}$ (voir le lemme 245) et on applique l'hypothèse de récurrence à G/ZG puis à ZG.

Lemme 245 Soit p un nombre premier et G un p-groupe non trivial. Alors $\mathrm{ZG} \neq 1$.

Preuve. On applique l'équation aux classes c'est-à-dire on fait agir G sur lui-même par conjugaison. On obtient $|\mathrm{G}| = |\mathrm{ZG}| + \sum_{\mathrm{C} \in \mathscr{C}} |\mathrm{C}|$ où $\mathscr{C}$ désigne l'ensemble des classes de conjugaison non ponctuelle de G. On C est en bijection avec $\mathrm{G}/\mathrm{Z}_\mathrm{C}$ où $\mathrm{Z}_\mathrm{C} \neq \mathrm{G}$ est le centralisateur d'un élément de C. En particulier, $|\mathrm{C}|$ est divisible par p. On en déduit que $|\mathrm{ZG}|$ est divisible par p.

Conclusion : théorème de Gauss.
Il existe une suite de sous-groupe $\{1\} \subset \mathrm{G}_1 \subset \cdots \subset \mathrm{G}_{2^n} = \mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q})$ tel que $(\mathrm{G}_{i+1} : \mathrm{G}_i) = 2$.
En appliquant le théorème de correspondance de Galois, il obtient une suite d'extension $\mathrm{K}_{2^n} = \mathbb{Q} \subset \mathrm{K}_{2^n-1} \subset \cdots \subset \mathrm{K}_0 = \mathbb{Q}(\zeta)$ vérifiant $[\mathrm{K}_i : \mathrm{K}_{i+1}] = 2$. Ainsi ζ est constructible.