Patrick Lemeur —Vincent Beck

Corrigé de l'examen d'Algèbre

Exercice 1 — Questions rapides / de cours.

a) On va montrer que $\mathrm{M} \overset{\text{A-mod.}}{\simeq} \mathrm{A}$ ou $\mathrm{M} = \{0\}$. On suppose $\mathrm{M} \neq \{0\}$ et on choisit une famille $(x_1, \dots x_s) \in \operatorname{Frac} \mathrm{A}$ telle que $\mathrm{M} = \langle x_1, \dots, x_s \rangle$. On peut supposer que $x_i \neq 0$. On pose alors $x_i = p_i/q_i$ avec $p_i, q_i \in \mathrm{A} \smallsetminus \{0\}$ (et p_i et q_i premier entre eux). On a donc

$$\mathrm{M} = \mathrm{A}p_1/q_1 + \cdots + \mathrm{A}p_s/q_s = \frac{1}{q_1 \cdots q_s} \left(\sum_{i=1}^{s} \mathrm{A}\ p_i \prod_{j=1, j\neq i}^{s} q_j \right)$$

En posant
$$p = \operatorname{pgcd} \left(p_i \prod_{j=1, j\neq i}^{s} q_j, \quad i = 1, \dots, s \right),$$

on obtient, par principalité de l'anneau A, $\mathrm{M} = \mathrm{A}p/q_1 \cdots q_s$. On en déduit que M est monogène et donc de la forme $\mathrm{A}/\langle d \rangle$ où d est l'idéal annulateur d'un générateur de M. Par ailleurs, pour $x \in \mathrm{K}$, on a $ax = 0 \implies a = 0$ puisque K est intègre. L'annulateur (dans A) d'un élément non nul de K est donc réduit à 0. Ainsi, comme $\mathrm{M} \neq \{0\}$, on a $p/q_1 \cdots q_s \neq 0$ et donc l'annulateur d'un générateur de M est réduit à 0. Ainsi $\mathrm{M} \overset{\text{A-mod.}}{\simeq} \mathrm{A}$.

b) M est de torsion si et seulement si M est de dimension finie sur k (le fait que k soit algébriquement clos n'intervient pas). En effet, le théorème de classification des modules de type fini sur l'anneau principal $k[\mathrm{X}]$ donne

$$\mathrm{M} \overset{k[\mathrm{X}]\text{-mod.}}{\simeq} k[\mathrm{X}]^n \oplus k[\mathrm{X}]/\mathrm{P}_1 \oplus \cdots \oplus k[\mathrm{X}]/\mathrm{P}_s \qquad \text{avec} \quad \mathrm{P}_1 \mid \mathrm{P}_2 \mid \cdots \mid \mathrm{P}_s \quad \text{et} \quad \deg \mathrm{P}_1 \geqslant 1$$

Par ailleurs, M est de torsion si et seulement si $n = 0$. Comme $\dim_k k[\mathrm{X}] = \infty$ et $\dim_k k[\mathrm{X}]/\mathrm{P} = \deg \mathrm{P}$, on obtient le résultat souhaité.

c) On considère le $k[\mathrm{X}]$-module (E, f). La condition « E engendré comme k-espace vectoriel par $\left\{ f^i(x),\ i \geqslant 0 \right\}$ » est synonyme de « x engendre le $k[\mathrm{X}]$-module (E, f) ». Il s'agit donc de décrire l'ensemble des sous-$k[\mathrm{X}]$-modules d'un module monogène M. Deux cas se présentent : M est donc isomorphe à $k[\mathrm{X}]$ ou M est isomorphe à $k[\mathrm{X}]/\mathrm{P}$ avec $\deg \mathrm{P} \geqslant 0$. Dans le premier cas, le sous-$k[\mathrm{X}]$-module de $k[\mathrm{X}]$ sont les idéaux de $k[\mathrm{X}]$ et donc de la forme $\mathrm{Q}k[\mathrm{X}]$ avec $\mathrm{Q} \in k[\mathrm{X}]$. De plus, $\mathrm{Q}k[\mathrm{X}] = \mathrm{R}k[\mathrm{X}]$ si et seulement si Q et R diffèrent d'un élément de k. Les sous-modules de (E, f) sont donc les $\{\mathrm{Q}(f)\mathrm{R}(f)(x), \quad \mathrm{R} \in k[\mathrm{X}]\}$ pour $\mathrm{Q} \in k[\mathrm{X}]$ unitaire ou $\mathrm{Q} = 0$. Dans le deuxième cas, le sous-$k[\mathrm{X}]$-module de $k[\mathrm{X}]/\mathrm{P}$ sont en bijection avec les sous-$k[\mathrm{X}]$-modules de $k[\mathrm{X}]$ contenant P c'est-à-dire les idéaux de $k[\mathrm{X}]$ contenant P ou encore les idéaux de la forme $\mathrm{Q}k[\mathrm{X}]$ avec $\mathrm{Q} \mid \mathrm{P}$. Les sous-modules de (E, f) sont donc les $\{\mathrm{Q}(f)\mathrm{R}(f)(x), \mathrm{R} \in k[\mathrm{X}]\}$ pour $\mathrm{Q} \in k[\mathrm{X}]$, Q unitaire et $\mathrm{Q} \mid \mathrm{P}$.

d) Soient E un k-espace vectoriel de dimension finie et $u \in \operatorname{End}_k(\mathrm{E})$. Les propriétés suivantes sont équivalentes.

(i) Tous les invariants de similitudes de u sont de degré 1.
(ii) Le polynôme minimal π_u de u est de degré 1.
(iii) L'endomorphisme u est une homothétie.
(iv) L'endomorphisme u a $\dim \mathrm{E}$ invariants de similitude.
(v) L'endomorphisme u a $\dim \mathrm{E}$ invariants de similitude tous égaux à π_u

L'implication $(i) \Rightarrow (ii)$ résulte du fait que π_u est l'un des invariants de similitude. L'implication $(ii) \Rightarrow (i)$ résulte du fait que tous les invariants de similitude divisent le polynôme minimal.

Montrons $(ii) \Rightarrow (iii)$. On a $\pi_u = \mathrm{X} - \lambda$ avec $\lambda \in \mathbb{C}$. Comme $u - \lambda \mathrm{id} = \pi_u(u) = 0$, u est l'homothétie de rapport λ. Montrons $(iii) \Rightarrow (ii)$. Si $u = \lambda \mathrm{id}$ alors $\mathrm{X} - \lambda$ est un polynôme annulateur de u. Comme il est irréductible sur k, c'est le polynôme minimal de u qui est donc de degré 1.

Comme un invariant de similitude est un polynôme de degré supérieur ou égal à 1 et que la somme des degrés des invariants de similitude est $\dim \mathrm{E}$, on en déduit $(iv) \Rightarrow (i)$ et $(i) \Rightarrow (iv)$.

On a $(v) \Rightarrow (iv)$. Montrons enfin $(ii) \Rightarrow (v)$. Comme tous les invariants de similitude divisent π_u et qu'ils sont de degré supérieur ou égal à 1, ils sont tous égaux à π_u. De plus, comme la somme des degrés des invariants de similitude est $\dim \mathrm{E}$, on en déduit qu'il y a $\dim \mathrm{E}$ invariants de similitude tous égaux à π_u.

Si $\dim \mathrm{E} = 2$ alors soit u est une homothétie et les invariants de similitude sont (π_u, π_u). Sinon, π_u est de degré 2 et comme $\pi_u \mid \chi_u$ et $\deg \chi_u = 2$, on a $\pi_u = \chi_u$. Comme, de plus, le produit des invariants de similitude est le polynôme caractéristique, on obtient que les invariants de similitude sont $\pi_u = \chi_u$.

Si $\dim \mathrm{E} = 3$ alors soit u est une homothétie et les invariants de similitude sont (π_u, π_u, π_u). Sinon, $\deg \pi_u \in \{2, 3\}$. On suppose $\deg \pi_u = 2$. Si $\mathrm{P}_2, \dots, \mathrm{P}_s$ sont les autres invariants de similitude, on a

$$\deg \mathrm{P}_2 + \cdots + \deg \mathrm{P}_s = 3 - 2 = 1 \quad \text{avec} \quad \deg \mathrm{P}_i \geqslant 1 \qquad \text{et} \qquad \pi_u \mathrm{P}_2 \cdots \mathrm{P}_s = \chi_u$$

On en déduit que $s = 2$ et $\mathrm{P}_2 = \chi_u/\pi_u$. Les invariants de similitudes sont donc $(\pi_u, \chi_u/\pi_u)$. Enfin si $\deg \pi_u = 3$ alors comme $\pi_u \mid \chi_u$ et $\deg \chi_u = 3$, on a $\pi_u = \chi_u$. Comme, de plus, le produit des invariants de similitude est le polynôme caractéristique, on obtient que les invariants de similitude sont $\pi_u = \chi_u$.

e) On note $\mathrm{Sp}(\mathrm{M}) = \{\lambda_1, \dots, \lambda_r\}$ avec $\lambda_i \neq \lambda_j$ si $i \neq j$ le spectre de M. On considère alors $n_{1,i} \geqslant \cdots \geqslant n_{s_i,i} \geqslant 1$ la suite des tailles des blocs de Jordan de M associés à la valeur propre λ_i. On pose $s = \max(s_i,\ i \in [\![1\,,\, r]\!])$ et si $s_i < s$, on pose $n_{j,i} = 0$ pour $s_i + 1 \leqslant j \leqslant s$ (on complète les listes par des 0). On a donc

$$(k^n, \mathrm{M}) \overset{k[\mathrm{X}]\text{-mod.}}{\simeq} \bigoplus_{i=1}^{r} \bigoplus_{j=1}^{s_i} k[\mathrm{X}]/\langle (\mathrm{X} - \lambda_i)^{n_{j,i}} \rangle$$

Par le théorème chinois, on en déduit que les invariants de similitude sont

$$\mathrm{P}_1 = (\mathrm{X} - \lambda_1)^{n_{1,1}} \cdots (\mathrm{X} - \lambda_r)^{n_{1,r}}, \dots, \mathrm{P}_i = (\mathrm{X} - \lambda_1)^{n_{i,1}} \cdots (\mathrm{X} - \lambda_r)^{n_{i,r}}, \dots, \mathrm{P}_s = (\mathrm{X} - \lambda_1)^{n_{s,1}} \cdots (\mathrm{X} - \lambda_r)^{n_{s,r}}\,.$$

f) Le groupe de galois de P s'identifie, par permutation des racines, à un sous-groupe de $\mathfrak{S}_4$. Or un sous-groupe d'ordre 8 de P est un 2-sylow de $\mathfrak{S}_4$. Ils sont donc tous conjugués dans $\mathfrak{S}_4$ et en particulier tous isomorphes et isomorphe au groupe diédral D_4 qui n'est pas $\mathbb{H}_8$.

Si on ne sait pas que les sous-groupes de Sylow de $\mathfrak{S}_4$ sont D_4, on doit savoir que le groupe des doubles-transpositions est distingué dans $\mathfrak{S}_4$ et d'ordre 4. Il est donc contenu dans tous les 2-Sylow. En particulier, un 2-Sylow contient au moins trois éléments d'ordre 2. Comme $\mathbb{H}_8$ contient un seul élément d'ordre 2, on obtient la contradiction souhaité.

Exercice 2 — Caractère linéaire.

a) Le fait que $\widehat{\mathrm{G}}$ soit un groupe résulte simplement de la commutativité de $\mathbb{C}^\times$. D'une manière générale, si X est un ensemble et G' un groupe alors l'ensemble $\mathscr{F}(\mathrm{X}, \mathrm{G}')$ des applications de X dans G' est un groupe pour la loi $\cdot$ donnée par $(f \cdot f')(x) = f(x)f'(x)$. L'élément neutre pour cette loi est la fonction constante égale à l'élément neutre de G' et l'inverse de f est la fonction $x \mapsto f(x)^{-1}$ (qu'on note f^{-1}). Si X est un groupe G, il n'est pas vrai en général que l'ensemble $\mathrm{Hom}_{\mathrm{Gr}}(\mathrm{G}, \mathrm{G}')$ est un sous-groupe du groupe $\mathscr{F}(\mathrm{X}, \mathrm{G}')$. C'est par contre vrai si G' est commutatif (comme c'est le cas ici avec $\mathrm{G}' = \mathbb{C}^\times$ et $\mathrm{X} = \mathrm{G}$). En effet, pour $g, g' \in \mathrm{G}$ et $\varphi, \varphi' \in \widehat{\mathrm{G}}$, on a alors

$$(\varphi \cdot \varphi')(gg') = \varphi(gg')\varphi'(gg') = \varphi(g)\varphi(g')\varphi'(g)\varphi'(g') = \varphi(g)\varphi'(g)\varphi(g')\varphi'(g') = (\varphi \cdot \varphi')(g)(\varphi \cdot \varphi')(g')\,.$$

et $$\varphi^{-1}(gg') = \varphi(gg')^{-1} = (\varphi(g)\varphi(g'))^{-1} = \varphi(g')^{-1}\varphi(g)^{-1} = \varphi(g)^{-1}\varphi(g')^{-1} = \varphi^{-1}(g)\varphi^{-1}(g')\,.$$

De plus, $\widehat{\mathrm{G}} \neq \varnothing$ puisque la fonction constante égale à 1 est le morphisme de groupes trivial qui est donc dans $\widehat{\mathrm{G}}$. Ainsi $\widehat{\mathrm{G}}$ est un sous-groupe de $\mathscr{F}(\mathrm{G}, \mathbb{C}^\times)$.

Pour completer ce qui précède, on a en fait G est commutatif si et seulement si $\mathrm{End}_{\mathrm{Gr}}(\mathrm{G})$ est un sous-groupe de $\mathscr{F}(\mathrm{G}, \mathrm{G})$. En effet, $(\mathrm{id} \cdot \mathrm{id}) = g \mapsto g^2$. Or, pour $g, g' \in \mathrm{G}$, on a, par simplification par g à gauche et g' à droite

$$(gg')^2 = g^2 g'^2 \qquad \Longleftrightarrow \qquad g'g = gg'.$$

b) Soit $\varphi \in \widehat{\mathfrak{S}_n}$. Montrons que φ est le caractère trivial ($\varphi(\sigma) = 1$ pour tout $\sigma \in \mathfrak{S}$) ou la signature. Comme deux transpositions sont conjugués (ce sont deux cycles de même longueurs) et $\mathbb{C}^\times$ est commutatif, toutes les transpositions ont la même image par φ. Comme une transposition est d'ordre 2, l'image par φ d'une transposition est d'ordre 1 ou 2 et donc 1 ou -1. Ainsi soit toutes les transpositions ont pour image 1 et auquel cas, comme les transpositions engendrent $\mathfrak{S}_n$, φ est le caractère trivial. Sinon toutes les transpositions ont pour image -1 et φ et la signature coïncident sur une partie génératrice et donc partout.

c) Soient G un groupe et n un entier. L'application

$$\Phi\colon \begin{cases} \mathrm{Hom}_{\mathrm{Gr}}(\mathbb{Z}/n\mathbb{Z}, \mathrm{G}) \longrightarrow \mathrm{G} \\ \qquad \varphi \qquad\qquad \longmapsto \varphi(1) \end{cases}$$

est injective et d'image $\mathrm{G}_n = \{x \in \mathrm{G}, \quad x^n = 1_{\mathrm{G}}\}$. En effet, comme 1 engendre le groupe $\mathbb{Z}/n\mathbb{Z}$, l'application Φ est injective. Comme $n1 = 0$ (dans $\mathbb{Z}/n\mathbb{Z}$), on a $\varphi(n1) = \varphi(1)^n = \varphi(0) = 1_{\mathrm{G}}$. Ainsi Φ est bien à valeurs dans G_n. Enfin, pour $x \in \mathrm{G}_n$, on peut définir l'application

$$\psi\colon \begin{cases} \mathbb{Z} \longrightarrow \mathrm{G} \\ k \longmapsto x^k \end{cases}$$

c'est un morphisme de groupes (par « définition » de la notation x^k) qui contient n et donc $n\mathbb{Z}$ dans son noyau puisque $x \in \mathrm{G}_n$. Ainsi ψ passe au quotient par $n\mathbb{Z}$ et fournit le morphisme de groupes

$$\varphi\colon \begin{cases} \mathbb{Z}/n\mathbb{Z} \longrightarrow \mathrm{G} \\ \overline{k} \quad \longmapsto x^k\,. \end{cases}$$

où $\overline{k}$ désigne la classe de l'entier k modulo n. Comme $\varphi(1) = x$, on en déduit l'image de Φ est bien G_n. De plus, la bijection réciproque de l'application $\Phi : \mathrm{Hom}_{\mathrm{Gr}}(\mathbb{Z}/n\mathbb{Z}, \mathrm{G}) \to \mathrm{G}_n$ est donnée par

$$\begin{cases} \mathrm{G}_n \longrightarrow \mathrm{Hom}_{\mathrm{Gr}}(\mathbb{Z}/n\mathbb{Z}, \mathrm{G}) \\ x \longmapsto (\overline{k} \mapsto x^k) \end{cases}$$

Ainsi si x désigne un générateur de C_n, par composition avec l'isomorphisme de groupe donné par $x^k \mapsto \overline{k}$, on en déduit la bijection

$$\Psi\colon \begin{cases} \mathrm{Hom}_{\mathrm{Gr}}(\mathrm{C}_n, \mathrm{G}) \longrightarrow \mathrm{G}_n \\ \qquad \varphi \qquad\quad \longmapsto \varphi(x) \end{cases}$$

Comme $(\mathbb{C}^\times)_n = \{x \in \mathbb{C}^\times, \quad x^n = 1\} = \mathbb{U}_n$ le groupe des racines n^{e} de l'unité, on en déduit que l'application

$$\Psi\colon \begin{cases} \mathrm{Hom}_{\mathrm{Gr}}(\mathrm{C}_n, \mathbb{C}^\times) \longrightarrow \mathbb{U}_n \\ \qquad \varphi \qquad\quad \longmapsto \varphi(x) \end{cases}$$

est une bijection. De plus, Ψ est un morphisme de groupes. En effet,

$$\Psi(\varphi \cdot \varphi') = (\varphi \cdot \varphi')(x) = \varphi(x)\varphi'(x) = \Psi(\varphi(x))\Psi(\varphi'(x)).$$

Ainsi Ψ est un isomorphisme de groupes entre $\widehat{\mathrm{C}_n}$ et $\mathbb{U}_n$. Comme $\mathbb{U}_n \overset{\mathrm{Gr.}}{\simeq} \mathrm{C}_n$, on obtient l'isomorphisme voulu.

Remarque. L'isomorphisme construit dans cette question n'est pas du tout canonique. Il est du même type que celui entre un espace vectoriel de dimension finie et son dual (via le choix d'une base). Ici, on choisit de façon arbitraire un générateur de C_n.

d) Contrairement à la question précédente, l'isomorphisme qu'on va donner ici est un isomorphisme canonique. Commençons par quelques notations. On considère les morphismes de groupes canoniques $i_{\mathrm{G}} : \mathrm{G} \to \mathrm{G} \times \mathrm{H}$ et $i_{\mathrm{H}} : \mathrm{H} \to \mathrm{H} \times \mathrm{G}$ définis par $i_{\mathrm{G}}(g) = (g, 1_{\mathrm{H}})$ pour $g \in \mathrm{G}$ et $i_{\mathrm{H}}(h) = (1_{\mathrm{G}}, h)$ pour $h \in \mathrm{H}$. On note aussi $p_{\mathrm{G}} : \mathrm{G} \times \mathrm{H} \to \mathrm{G}$ et $p_{\mathrm{H}} : \mathrm{G} \times \mathrm{H} \to \mathrm{H}$ les morphismes de groupes canoniques donnés par $p_{\mathrm{G}}(g, h) = g$ et $p_{\mathrm{H}}(g, h) = h$ pour $(g, h) \in \mathrm{G} \times \mathrm{H}$.

Soit $\chi \in \widehat{\mathrm{G} \times \mathrm{H}}$. Par composition, $\chi \circ i_{\mathrm{G}}$ et $\chi \circ i_{\mathrm{H}}$ sont des morphismes de groupes. On a construit une application

$$\Phi\colon \begin{cases} \widehat{\mathrm{G} \times \mathrm{H}} \longrightarrow \widehat{\mathrm{G}} \times \widehat{\mathrm{H}} \\ \quad \chi \quad \longmapsto (\chi \circ i_{\mathrm{G}}, \chi \circ i_{\mathrm{H}})\,. \end{cases}$$

La définition de la loi de groupe sur $\widehat{\mathrm{G} \times \mathrm{H}}$ et $\widehat{\mathrm{G}} \times \widehat{\mathrm{H}}$ assure que Φ est un morphisme de groupes. En effet, pour $\chi, \chi' \in \widehat{\mathrm{G} \times \mathrm{H}}$ et $(g, h) \in \mathrm{G} \times \mathrm{H}$, on a

$$[(\chi \cdot \chi') \circ i_{\mathrm{G}}](g) = \chi(g, 1_{\mathrm{H}})\chi'(g, 1_{\mathrm{H}}) = [(\chi \circ i_{\mathrm{G}}) \cdot (\chi' \circ i_{\mathrm{G}})](g)$$

et

$$[(\chi \cdot \chi') \circ i_{\mathrm{H}}](h) = \chi(1_{\mathrm{G}}, h)\chi'(1_{\mathrm{G}}, h) = [(\chi \circ i_{\mathrm{H}}) \cdot (\chi' \circ i_{\mathrm{H}})](h)\,.$$

On considère à présent $\chi_{\mathrm{G}} \in \widehat{\mathrm{G}}$ et $\chi_{\mathrm{H}} \in \widehat{\mathrm{H}}$. Par composition, on obtient que $\chi_{\mathrm{G}} \circ p_{\mathrm{G}} : \mathrm{G} \times \mathrm{H} \to \mathbb{C}^\times$ et $\chi_{\mathrm{H}} \circ p_{\mathrm{H}} : \mathrm{G} \times \mathrm{H} \to \mathbb{C}^\times$ sont des morphismes de groupes. Ainsi $\chi_{\mathrm{G}} \circ p_{\mathrm{G}} \in \widehat{\mathrm{G}}$ et $\chi_{\mathrm{H}} \circ p_{\mathrm{H}} \in \widehat{\mathrm{H}}$. On peut ainsi définir l'application

$$\Psi\colon \begin{cases} \widehat{\mathrm{G}} \times \widehat{\mathrm{H}} \longrightarrow \widehat{\mathrm{G} \times \mathrm{H}} \\ (\chi_{\mathrm{G}}, \chi_{\mathrm{H}}) \longmapsto (\chi_{\mathrm{G}} \circ p_{\mathrm{G}}) \cdot (\chi_{\mathrm{H}} \circ p_{\mathrm{H}})\,. \end{cases}$$

Par définition, on a donc $\Psi(\chi_{\mathrm{G}}, \chi_{\mathrm{H}})(g, h) = \chi_{\mathrm{G}}(g)\chi_{\mathrm{H}}(h)$ pour tout $(g, h) \in \mathrm{G} \times \mathrm{H}$.

On a clairement $\Phi \circ \Psi = \mathrm{id}_{\widehat{\mathrm{G}\times\mathrm{H}}}$ puisque $\Psi(\chi_{\mathrm{G}}, \chi_{\mathrm{H}})(g, 1_{\mathrm{H}}) = \chi_{\mathrm{G}}(g)$ et $\Psi(\chi_{\mathrm{G}}, \chi_{\mathrm{H}})(1_{\mathrm{G}}, h) = \chi_{\mathrm{H}}(h)$. De même, on a $\Psi \circ \Phi = \mathrm{id}_{\widehat{\mathrm{G}\times\mathrm{H}}}$ puisque, pour $(g, h) \in \mathrm{G} \times \mathrm{H}$, on a

$$\Psi \circ \Phi(\chi)(g, h) = \chi(g, 1_{\mathrm{H}})\chi(1_{\mathrm{G}}, h) = \chi((g, 1_{\mathrm{H}})(1_{\mathrm{G}}, h)) = \chi(g, h).$$

Ainsi Ψ est la bijection réciproque de Φ et donc un morphisme de groupes. Finalement, Φ et Ψ réalisent l'isomorphisme souhaité.

e) L'isomorphisme de la question **d** s'étend par récurrence en un isomorphisme

$$\widehat{\prod_{i=1}^{r} \mathrm{G}_i} \quad \longrightarrow \quad \prod_{i=1}^{r} \widehat{\mathrm{G}_i}\,.$$

Or d'après le théorème de classification des groupes abéliens fini, un groupe abélien fini G est produit de groupe cyclique. On peut donc écrire

$$\widehat{\mathrm{G}} \quad \overset{\text{gr.}}{\simeq} \quad \widehat{\prod_{i=1}^{s} \mathbb{Z}/d_i\mathbb{Z}} \quad \overset{\text{gr.}}{\simeq} \quad \prod_{i=1}^{s} \widehat{\mathbb{Z}/d_i\mathbb{Z}}\,.$$

On peut même supposer que $d_1 \mid d_2 \mid \cdots \mid d_s$ mais on en aura pas besoin ici. La question **c** donne alors

$$\widehat{\mathrm{G}} \quad \overset{\text{gr.}}{\simeq} \quad \prod_{i=1}^{s} \mathbb{Z}/d_i\mathbb{Z} \quad \overset{\text{gr.}}{\simeq} \quad \mathrm{G}\,.$$

f) Il s'agit d'une version du lemme de Dedekind. On suppose que $\widehat{\mathrm{G}}$ n'est pas un sous-ensemble libre de $\mathscr{F}(\mathrm{G}, \mathbb{C})$. Il existe donc une relation de dépendance linéaire non triviale entre des caractères linéaires : on a

$$\lambda_1\chi_1 + \cdots + \lambda_r\chi_r = 0 \qquad \text{avec} \quad \lambda_i \in \mathbb{C}^\times \tag{1}$$

On choisit une telle relation avec r minimal et on va construire une nouvelle relation avec un nombre strictement plus petit de termes pour aboutir à une contradiction. La minimalité de r assure que $\chi_i \neq \chi_j$ si $i \neq j$ (sinon on regroupe les termes communs).

On a donc, pour $g, g' \in \mathrm{G}$,

$$\lambda_1\chi_1(g)\chi_1(g') + \cdots + \lambda_r\chi_r(g)\chi_r(g') = 0$$

En multipliant la relation (**1**) évaluée en g' par $\chi_1(g)$ et en la soustrayant à la relation précédente, on obtient

$$\forall\,(g, g') \in \mathrm{G}^2, \qquad \lambda_2(\chi_2(g) - \chi_1(g))\chi_2(g') + \cdots + \lambda_r(\chi_r(g) - \chi_1(g))\chi_r(g') = 0$$

et donc

$$\forall\, g \in \mathrm{G}, \qquad \lambda_2(\chi_2(g) - \chi_1(g))\chi_2 + \cdots + \lambda_r(\chi_r(g) - \chi_1(g))\chi_r = 0 \tag{2}$$

Comme $\chi_1 \neq \chi_2$, il existe g tel que $\chi_2(g) \neq \chi_1(g)$. Ainsi $\lambda_2(\chi_2(g) - \chi_1(g)) \neq 0$ et (**2**) est une relation de dépendance entre éléments de $\widehat{\mathrm{G}}$ avec au plus $r - 1$ termes ce qui contredit la minimalité de r.

Remarques. On en déduit la liberté de la famille $(x \mapsto \exp(ax))_{a\in\mathbb{C}}$ dans $\mathscr{F}(\mathbb{R}, \mathbb{C})$ et celle de la famille $(z \mapsto \exp(az))_{a\in\mathbb{C}}$ dans $\mathscr{F}(\mathbb{C}, \mathbb{C})$. En effet, pour $a \in \mathbb{C}$, l'application $x \mapsto \exp(ax)$ est un morphisme de groupe de $\mathbb{R}$ ou $\mathbb{C}$ dans $\mathbb{C}^\times$. Ainsi ce sont des sous-familles respectivement de $\widehat{\mathbb{R}}$ et $\widehat{\mathbb{C}}$. De plus, si $\exp(ax) = \exp(bx)$ pour tout $x \in \mathbb{R}$ (resp. $x \in \mathbb{C}$), on a $(a - b)x \in 2i\pi\mathbb{Z}$ pour tout $x \in \mathbb{R}$ (resp. $x \in \mathbb{C}$). Ainsi si $a \neq b$, on a $\mathbb{R} \subset 2i\pi/(a - b)\mathbb{Z}$ (resp. $\mathbb{C} \subset 2i\pi/(a - b)\mathbb{Z}$) ce qui est absurde donc $a = b$. Ainsi les familles considérées sont bien formées de caractères linéaires distincts et donc libre.

Exercice 3 – Polynôme de degré 4.

a) Le polynôme P est irréductible et $\mathrm{P}' = 4\mathrm{X}^3 + 3a\mathrm{X}^2 + 2b\mathrm{X} + c$. Comme car $k \neq 2$, on a $4 \neq 0$. Ainsi, P est irréductible à dérivée non nulle. Donc P est séparable. Or $\mathrm{L} = k(\alpha_1, \alpha_2, \alpha_3, \alpha_4)$, comme le polynôme minimal de α_i est P, on en déduit que α_i séparable. Ainsi L est engendré sur k par des éléments séparables et l'extension $k \subset \mathrm{L}$ est donc séparable. Par ailleurs, L est le corps de décomposition sur k d'un polynôme. L'extension $k \subset \mathrm{L}$ est donc une extension normale. L'extension $k \subset \mathrm{L}$ est normale et séparable donc galoisienne.

b) On a $\mathrm{Q} = (\mathrm{X}-\theta_1)(\mathrm{X}-\theta_2)(\mathrm{X}-\theta_3)$ et donc $\mathrm{Q} = \mathrm{X}^3+u\mathrm{X}^2+v\mathrm{X}+w$ avec $u = -\theta_1+\theta_2+\theta_3$, $v = \theta_1\theta_2+\theta_3\theta_2+\theta_1\theta_3$ et $w = -\theta_1\theta_2\theta_3$.

Les éléments $u, v, w \in \mathrm{L}$ sont des polynômes symétriques en $\alpha_1, \alpha_2, \alpha_3, \alpha_4$ et donc s'exprime en fonction des polynômes symétriques élémentaires en les α_i, c'est-à-dire en fonction des coefficients de P. Ainsi $\mathrm{Q} \in k[\mathrm{X}]$.

c) On applique l'algorithme qui permet d'exprimer les polynômes symétriques en fonction des polynômes symétriques élémentaires. On a

$$\begin{aligned}\theta_1+\theta_2+\theta_3 &= \alpha_1\alpha_3 + \alpha_2\alpha_3 + \alpha_1\alpha_4 + \alpha_2\alpha_4 + \alpha_1\alpha_2 + \alpha_1\alpha_4 + \\ &\quad \alpha_3\alpha_2 + \alpha_3\alpha_4 + \alpha_1\alpha_3 + \alpha_1\alpha_2 + \alpha_3\alpha_4 + \alpha_2\alpha_4 \\ &= 2(\alpha_1\alpha_2+\alpha_1\alpha_3+\alpha_1\alpha_4+\alpha_2\alpha_3+\alpha_2\alpha_4+\alpha_3\alpha_4) = 2b\end{aligned}$$

On passe au calcul de v. On commence par calculer $\theta_1\theta_2$.

$$\begin{aligned}\theta_1\theta_2 &= (\alpha_1\alpha_3+\alpha_2\alpha_3+\alpha_1\alpha_4+\alpha_2\alpha_4)(\alpha_1\alpha_2+\alpha_1\alpha_4+\alpha_3\alpha_2+\alpha_3\alpha_4) \\ &= {\alpha_1}^2\alpha_2\alpha_3 + {\alpha_1}^2\alpha_3\alpha_4 + {\alpha_3}^2\alpha_1\alpha_2 + {\alpha_3}^2\alpha_1\alpha_4 + \\ &\quad {\alpha_2}^2\alpha_1\alpha_3 + \alpha_2{\alpha_3}^2\alpha_4 + \alpha_1\alpha_2\alpha_3\alpha_4 + (\alpha_2\alpha_3)^2 + \\ &\quad {\alpha_1}^2\alpha_2\alpha_4 + \alpha_1\alpha_3{\alpha_4}^2 + \alpha_1\alpha_2\alpha_3\alpha_4 + (\alpha_1\alpha_4)^2 + \\ &\quad \alpha_1{\alpha_2}^2\alpha_4 + \alpha_1\alpha_2{\alpha_4}^2 + {\alpha_2}^2\alpha_3\alpha_4 + \alpha_2\alpha_3{\alpha_4}^2\end{aligned}$$

Pour $i \in [\![1\,,\,4]\!]$, on note σ_i les polynômes symétriques élémentaires en les α_j. Par ailleurs, on pose

$$\begin{aligned}\mathrm{T} = {\alpha_1}^2\alpha_2\alpha_3 + {\alpha_1}^2\alpha_3\alpha_4 + {\alpha_3}^2\alpha_1\alpha_2 + {\alpha_3}^2\alpha_1\alpha_4 + {\alpha_2}^2\alpha_1\alpha_3 + \alpha_2{\alpha_3}^2\alpha_4 + \\ {\alpha_1}^2\alpha_2\alpha_4 + \alpha_1\alpha_3{\alpha_4}^2 + \alpha_1{\alpha_2}^2\alpha_4 + \alpha_1\alpha_2{\alpha_4}^2 + {\alpha_2}^2\alpha_3\alpha_4 + \alpha_2\alpha_3{\alpha_4}^2\,.\end{aligned}$$

C'est un polynôme symétrique en les α_i. On va l'exprimer en fonction des σ_i grâce à l'algorithme. Le plus grand monôme est ${\alpha_1}^2\alpha_2\alpha_3$. On considère donc $\mathrm{T} - {\sigma_1}^{2-1}{\sigma_2}^{1-1}{\sigma_3}^{1-0}{\sigma_4}^0 = \mathrm{T} - \sigma_1\sigma_3$. Or on a

$$\begin{aligned}\sigma_1\sigma_3 &= (\alpha_1+\alpha_2+\alpha_3+\alpha_4)(\alpha_1\alpha_2\alpha_3+\alpha_1\alpha_3\alpha_4+\alpha_1\alpha_2\alpha_4+\alpha_2\alpha_3\alpha_4) \\ &= {\alpha_1}^2\alpha_2\alpha_3 + {\alpha_1}^2\alpha_3\alpha_4 + {\alpha_3}^2\alpha_1\alpha_2 + {\alpha_3}^2\alpha_1\alpha_4 + {\alpha_2}^2\alpha_1\alpha_3 + \alpha_2{\alpha_3}^2\alpha_4 + {\alpha_1}^2\alpha_2\alpha_4 + \\ &\quad \alpha_1\alpha_3{\alpha_4}^2 + \alpha_1{\alpha_2}^2\alpha_4 + \alpha_1\alpha_2{\alpha_4}^2 + {\alpha_2}^2\alpha_3\alpha_4 + \alpha_2\alpha_3{\alpha_4}^2 + 4\alpha_1\alpha_2\alpha_3\alpha_4 \\ &= \mathrm{T} + 4\sigma_4\,.\end{aligned}$$

On a donc $\mathrm{T} = \sigma_1\sigma_3 - 4\sigma_4$. Par symétrie, on obtient alors

$$\begin{aligned}\theta_1\theta_2+\theta_3\theta_2+\theta_1\theta_3 &= 3\mathrm{T} + 6\sigma_4 + ({\alpha_1}^2{\alpha_2}^2 + {\alpha_1}^2{\alpha_3}^2 + {\alpha_1}^2{\alpha_4}^2 + {\alpha_2}^2{\alpha_3}^2 + {\alpha_2}^2{\alpha_4}^2 + {\alpha_3}^2{\alpha_4}^2) \\ &= 3\sigma_1\sigma_3 - 6\sigma_4 + ({\alpha_1}^2{\alpha_2}^2 + {\alpha_1}^2{\alpha_3}^2 + {\alpha_1}^2{\alpha_4}^2 + {\alpha_2}^2{\alpha_3}^2 + {\alpha_2}^2{\alpha_4}^2 + {\alpha_3}^2{\alpha_4}^2)\end{aligned}$$

On pose $\mathrm{U} = ({\alpha_1}^2{\alpha_2}^2 + {\alpha_1}^2{\alpha_3}^2 + {\alpha_1}^2{\alpha_4}^2 + {\alpha_2}^2{\alpha_3}^2 + {\alpha_2}^2{\alpha_4}^2 + {\alpha_3}^2{\alpha_4}^2)$. C'est un polynôme symétrique en les α_i. On va l'exprimer en fonction des σ_i grâce à l'algorithme. Le plus grand monôme de U est ${\alpha_1}^2{\alpha_2}^2$. On considère donc $\mathrm{U} - {\sigma_1}^{2-2}{\sigma_2}^{2-0}{\sigma_3}^{0-0}{\sigma_4}^0 = \mathrm{U} - {\sigma_2}^2$.

En développant le carré ${\sigma_2}^2$. Les termes « carré » donnent U. Il reste alors 15 double-produits parmi lesquels on trouve 12 termes de T (puisqu'on a ${\alpha_1}^2\alpha_2\alpha_3$ dans le produit et donc toute son orbite sous $\mathfrak{S}_4$). Il reste donc 3 double-produit égaux à σ_4. Finalement ${\sigma_2}^2 = \mathrm{U} + 2\mathrm{T} + 6\sigma_4 = \mathrm{U} + 2\sigma_1\sigma_3 - 2\sigma_4$.

On en déduit que $\mathrm{U} = {\sigma_2}^2 - 2\sigma_1\sigma_3 + 2\sigma_4$ et donc $v = \sigma_1\sigma_3 - 4\sigma_4 + {\sigma_2}^2 = ac + b^2 - 4d$.

d) Calculons $\theta_1-\theta_2$, $\theta_2-\theta_3$ et $\theta_1-\theta_3$. On a

$$\begin{aligned}\theta_1-\theta_2 &= (\alpha_1+\alpha_2)(\alpha_3+\alpha_4) - (\alpha_1+\alpha_3)(\alpha_2+\alpha_4) \\ &= (\alpha_1\alpha_3+\alpha_2\alpha_3+\alpha_1\alpha_4+\alpha_2\alpha_4) - (\alpha_1\alpha_2+\alpha_1\alpha_4+\alpha_3\alpha_2+\alpha_3\alpha_4) \\ &= \alpha_1(\alpha_3-\alpha_2) + (\alpha_2-\alpha_3)\alpha_4 \\ &= (\alpha_2-\alpha_3)(\alpha_4-\alpha_1)\,,\end{aligned}$$

$$\begin{aligned}\theta_2-\theta_3 &= (\alpha_1+\alpha_3)(\alpha_2+\alpha_4) - (\alpha_1+\alpha_4)(\alpha_3+\alpha_2) \\ &= (\alpha_1\alpha_2+\alpha_1\alpha_4+\alpha_3\alpha_2+\alpha_3\alpha_4) - (\alpha_1\alpha_3+\alpha_1\alpha_2+\alpha_3\alpha_4+\alpha_2\alpha_4) \\ &= \alpha_1(\alpha_4-\alpha_3) + (\alpha_3-\alpha_4)\alpha_2 \\ &= (\alpha_1-\alpha_2)(\alpha_4-\alpha_3)\end{aligned}$$

et

$$\begin{aligned}\theta_1-\theta_3 &= (\alpha_1+\alpha_2)(\alpha_3+\alpha_4) - (\alpha_1+\alpha_4)(\alpha_3+\alpha_2) \\ &= (\alpha_1\alpha_3+\alpha_2\alpha_3+\alpha_1\alpha_4+\alpha_2\alpha_4) - (\alpha_1\alpha_3+\alpha_1\alpha_2+\alpha_3\alpha_4+\alpha_2\alpha_4) \\ &= \alpha_2(\alpha_3-\alpha_1) + (\alpha_1-\alpha_3)\alpha_4 \\ &= (\alpha_3-\alpha_1)(\alpha_2-\alpha_4)\,.\end{aligned}$$

On en déduit que

$$\begin{aligned}(\theta_1-\theta_2)(\theta_2-\theta_3)(\theta_1-\theta_3) &= (\alpha_2-\alpha_3)(\alpha_4-\alpha_1)(\alpha_1-\alpha_2)(\alpha_4-\alpha_3)(\alpha_3-\alpha_1)(\alpha_2-\alpha_4) \\ &= -(\alpha_2-\alpha_3)(\alpha_1-\alpha_4)(\alpha_1-\alpha_2)(\alpha_3-\alpha_4)(\alpha_1-\alpha_3)(\alpha_2-\alpha_4)\,.\end{aligned}$$

En élevant au carré, on obtient que les discriminants de P et Q sont égaux.

e) Par définition de Q, il est scindé sur L. En posant $\mathrm{M} = k(\theta_1, \theta_2, \theta_3)$, on construit donc un corps de décomposition de Q sur k.

f) On a $\mathrm{P} \in \mathrm{M}[\mathrm{X}]$ et $\mathrm{L} = \mathrm{M}(\alpha_1, \alpha_2, \alpha_3, \alpha_4)$. Ainsi L est le corps de décomposition de P sur M et donc $\mathrm{M} \subset \mathrm{L}$ est une extension normale. Soit $x \in \mathrm{L}$. Comme tout élément de L est séparable sur k, le polynôme minimal π_x de x sur k est à racine simple. Or le polynôme minimal de x sur M divise π_x et est donc à racine simple. Ainsi x est séparable sur M. L'extension $\mathrm{M} \subset \mathrm{L}$ est séparable. Elle est donc galoisienne.

Tout élément de L est séparable sur k. En particulier, ceux de M. Ainsi $k \subset \mathrm{M}$ est séparable. Comme M est le corps de décomposition de Q sur k, l'extension $k \subset \mathrm{M}$ est normale et donc $k \subset \mathrm{M}$ est galoisienne.

g) Tout élément $\mathrm{Gal}(\mathrm{L} \mid \mathrm{M})$ est un automorphisme du corps L qui laisse fixe tous les éléments de M et donc tous les éléments de k. Ainsi tout élément de $\mathrm{Gal}(\mathrm{L} \mid \mathrm{M})$ appartient à $\mathrm{Gal}(\mathrm{L} \mid k)$. La première flèche est donc simplement l'inclusion qui est bien sûr injective.

Soit $\sigma \in \mathrm{Gal}(\mathrm{L} \mid k)$. Comme $k \subset \mathrm{M}$ est normale, $\sigma(\mathrm{M}) \subset \mathrm{M}$ (et même $\sigma(\mathrm{M}) = \mathrm{M}$ par raison de dimension et injectivité de σ). Ainsi par restriction à M, un élément de $\mathrm{Gal}(\mathrm{L} \mid k)$ définit une application de M dans lui-même qui est bien sûr un k-automorphisme de corps. On peut donc bien définir une application $\mathrm{Rest} : \mathrm{Gal}(\mathrm{L} \mid k) \to \mathrm{Gal}(\mathrm{M} \mid k)$ donnée par $\sigma \mapsto \sigma_{|\mathrm{M}}$. Le noyau de Rest est l'ensemble des k-automorphismes de corps de L dont la restriction à M est id_M c'est-à-dire $\mathrm{Gal}(\mathrm{L} \mid \mathrm{M})$. On en déduit que $\mathrm{Gal}(\mathrm{L} \mid \mathrm{M})$ est un sous-groupe distingué (ce qu'on sait aussi par la correspondance de Galois car $k \subset \mathrm{M}$ est normale) de $\mathrm{Gal}(\mathrm{L} \mid k)$ et que la suite est exacte en $\mathrm{Gal}(\mathrm{L} \mid k)$.

Reste à montrer la surjectivité de Rest. Soit $\sigma \in \mathrm{Gal}(\mathrm{M} \mid k)$. On note $j : \mathrm{M} \mapsto \overline{\mathrm{L}} = \overline{\mathrm{M}}$ l'inclusion. Comme $\mathrm{M} \subset \mathrm{L}$ est un extension algébrique, le morphisme $j \circ \sigma$ se prolonge en un k-morphisme $\widetilde{\sigma} : \mathrm{L} \mapsto \overline{\mathrm{L}}$. Comme $k \subset \mathrm{L}$ est normale, alors $\widetilde{\sigma}$ est à valeurs dans L. Ainsi $\widetilde{\sigma} \in \mathrm{Gal}(\mathrm{L} \mid k)$ et sa restriction à M est σ. On obtient bien la surjectivité de Rest.

h) Donnons deux démonstrations du fait que $\mathrm{Gal}(\mathrm{L} \mid k)$ est divisible par 4.

Version « groupe ». Comme P est irréductible sur k, $\mathrm{Gal}(\mathrm{P}) = \mathrm{Gal}(\mathrm{L} \mid k)$ agit transitivement sur les racines de P. Les racines de P forment donc une orbite sous $\mathrm{Gal}(\mathrm{L} \mid k)$. Or le cardinal d'une orbite divise l'ordre du groupe. Ainsi $4 \mid |\mathrm{Gal}(\mathrm{L} \mid k)|$.

Version « corps ». L'extension $k \subset \mathrm{L}$ est galoisienne, donc $|\mathrm{Gal}(\mathrm{L} \mid k)| = [\mathrm{L} : k]$. Or

$$[\mathrm{L} : k] = [\mathrm{L} : k(\alpha_1)][k(\alpha_1) : k].$$

Comme $\mathrm{P} \in k[\mathrm{X}]$ est irréductible sur k et annule α_1, c'est le polynôme minimal de α_1 sur k et donc $[k(\alpha_1) : k] = 4$. Ainsi $4 \mid |\mathrm{Gal}(\mathrm{L} \mid k)|$.

Comme $\alpha_1, \alpha_2, \alpha_3, \alpha_4$ engendrent L, le groupe $\mathrm{Gal}(\mathrm{L} \mid k)$ s'identifie (par permutation des racines) à un sous-groupe du groupe $\mathfrak{S}_{\{\alpha_1,\alpha_2,\alpha_3,\alpha_4\}} = \mathfrak{S}_4$. Ainsi $4 \mid |\mathrm{Gal}(\mathrm{L} \mid k)| \mid |\mathfrak{S}_4| = 24$.

On en déduit que $\mathrm{Gal}(\mathrm{L} \mid k) \in \{4, 8, 12, 24\}$.

i) Les classes de conjugaison dans $\mathfrak{S}_4$ sont données par la décomposition en cycles à support disjoint. Elles sont donc parametrées par les partitions de 4. On a donc

(i) Partition 4 : les 6 4-cycles.
(ii) Partition $(3, 1)$: les 8 3-cycles.
(iii) Partition $(2, 1, 1)$: les 6 transpositions.
(iv) Partition $(2, 2)$: les 3 double-transpostions.
(v) Partition $(1, 1, 1, 1)$: l'identité.

j) Les cardinaux des sous-groupes de $\mathfrak{S}_4$ divise 24 et donc sont dans $\{1, 2, 3, 4, 6, 8, 12, 24\}$.

Pour le cardinal 1, le seul groupe possible est $\{\mathrm{id}\}$. Il n'est pas transitif mais est distingué !

Pour le cardinal 24, le seul groupe possible est $\mathfrak{S}_4$. Il est transitif et distingué !

Soit G un sous-groupe de cardinal 12, c'est un sous-groupe d'indice 2 qui est donc distingué. Il est donc réunion de classes de conjugaison de $\mathfrak{S}_4$. Comme $\mathrm{id} \in \mathrm{G}$, on en déduit par parité que les double-transpositions sont aussi dans G. Par raison de cardinal, la seule classe de conjugaison qu'on peut ajouter est celle des 3-cycles. On constate que l'ensemble obtenu est $\mathfrak{A}_4$. Ainsi $\mathrm{G} = \mathfrak{A}_4$. Il est transitif et distingué.

Soit G un sous-groupe de cardinal 2. Il est de la forme $\mathrm{G} = \{\mathrm{id}, \sigma\}$ avec σ d'ordre 2. Deux tels sous-groupes sont conjugués si et seulement si les éléments d'ordre 2 le sont. Ainsi, on a deux classes de conjugaison de sous-groupes d'ordre 2. L'une correspondant aux groupes engendrés par une transposition, l'autre aux groupes engendrés par une double-transposition. Ils ne sont ni distingués (ne contiennent pas les classes de conjugaison de leurs éléments) ni transitifs (3 orbites de cardinal respectif $2, 1, 1$ dans le premier cas et 2 orbites de cardinal 2 dans le second cas).

Soit G un sous-groupe de cardinal 3. Il est de la forme $\mathrm{G} = \left\{\mathrm{id}, \sigma, \sigma^2\right\}$ avec σ d'ordre 3. Il s'agit donc d'un sous-groupe engendré par un élément d'ordre 3 c'est-à-dire un 3-cycle. Comme les trois cycles sont tous conjugués, tous les groupes d'ordre 3 sont conjugués. On peut aussi voir ce fait par le fait qu'un groupe d'ordre 3 est un 3-Sylow de $\mathfrak{S}_4$. Ils ne sont ni transitif (2 orbites de cardinal respectif 1 et 3) ni distingué (ils contiennent deux 3-cycles mais pas tous les trois cycles).

Soit G un sous-groupe de cardinal 6. Par le lemme de Cauchy, il contient un élément d'ordre 3 (c'est-à-dire un 3-cycle qu'on note σ) et un élément d'ordre 2 (qu'on note τ). Le cardinal du sous-groupe $\langle \sigma, \tau \rangle \subset \mathrm{G}$ est divisible par 6 (puisqu'il contient un élément d'ordre 2 et un d'ordre 3). Ainsi $\mathrm{G} = \langle \sigma, \tau \rangle$.

Supposons que τ soit une transposition et que le support de τ contenu dans celui de σ alors $\mathrm{G} = \langle \sigma, \tau \rangle$ est contenu dans le groupe des permutations du support de σ qui est isomorphe à $\mathfrak{S}_3$. Par raison de cardinalité, on obtient que G est le groupe des permutations du support de σ.

Supposons toujours τ est une transposition mais que son support n'est pas contenu dans celui de σ. L'intersection des support de σ et τ est alors réduite à un point $\{a\}$. On peut donc écrire $\sigma = (a, b, c)$ et $\tau = (a, d)$. On a alors $\tau\sigma = (a, b, c, d)$ est d'ordre 4 et ne peut donc pas appartenir à un groupe d'ordre 6.

Supposons à présent que τ soit une double-transposition. En considérant d l'élément qui n'est pas dans le support de σ. On peut écrire $\tau = (d, a)(b, c)$ puis $\sigma = (a, b, c)$. L'orbite de a sous $\mathrm{G} = \langle \sigma, \tau \rangle$ contient donc a, b, c et d. Ainsi $|\mathrm{G}|$ est divisible par 4 ce qui est absurde (on aurait pu raisonner de la même façon pour le cas précédent).

Finalement, il y a 4 sous-groupe d'ordres 6 qui sont les sous-groupes $\mathfrak{S}_{\{1,2,3\}}$, $\mathfrak{S}_{\{1,2,4\}}$, $\mathfrak{S}_{\{1,3,4\}}$ et $\mathfrak{S}_{\{2,3,4\}}$ (Ce sont les sous-groupes $\mathfrak{S}_3 \times \mathfrak{S}_1$). Ils ne sont donc ni transitifs (2 orbites de cardinal respectif 1 et 3) ni distingués (puisqu'ils sont conjugués).

Soit G un sous-groupe de cardinal 4. Supposons qu'il contienne un élément d'ordre 4 c'est-à-dire, d'après la description des éléments de $\mathfrak{S}_4$, un 4-cycle. On a alors $\mathrm{G} = \langle \sigma \rangle$ et comme tous les 4-cycles sont conjugués dans $\mathfrak{S}_4$, les sous-groupes d'ordre 4 de $\mathfrak{S}_4$ qui sont cycliques sont conjugués. De plus, chacun de ces groupes contient deux 4-cycles, on en déduit qu'il y a trois tels sous-groupes.

Sinon, G n'est formé que d'éléments d'ordre 1 ou 2. On a donc trois éléments d'ordre 2 dans G. Si ces trois éléments d'ordre 2 sont les double-transpositions, on vérifie (en effectuant les produits des double-transpositions) qu'on obtient bien un groupe d'ordre 4 et qui est distingué (puisque c'est une réunion de classe de conjugaison) et transitif. On l'appelle V_4.

Si G contient deux double-transpositions, par produit, il contient la troisième et $\mathrm{G} = \mathrm{V}_4$.

Sinon G contient au moins deux transpositions qui sont nécessairement à support disjoint puisque le produit de deux transpositions à support non disjoint est un 3-cycle et donc d'ordre 3. On a donc $\{\mathrm{id}, (a, b), (c, d)\} \subset \mathrm{G}$ avec $\{a, b\} \cap \{c, d\} = \varnothing$ et $a \neq b$ et $c \neq d$. Par produit et cardinalité, on obtient que

$$\mathrm{G} = \{\mathrm{id}, (a, b), (c, d), (a, b)(c, d)\}.$$

On vérifie (en effectuant les différents produits) que c'est bien un sous-groupe. Il y a trois sous-groupes de ce type et ils sont tous conjugués. Ainsi un tel sous-groupe n'est pas distingué. Il n'est pas non plus transitif (il y a deux orbites de cardinal 2). En fait ce sont les sous-groupe du type $\mathfrak{S}_2 \times \mathfrak{S}_2$.

Soit G un sous-groupe de cardinal 8. C'est un 2-sylow de G. Ainsi tous les sous-groupes de cardinal 8 sont conjugués. Il n'y a donc à conjugaison près qu'un groupe de cardinal 8. On peut montrer qu'il est isomorphe à D_4 : le groupe des isométries du cube mais on ne va pas le montrer. On va se contenter d'en exhiber un exemple. Comme tout 2-sous-groupe de $\mathfrak{S}_4$ est contenu dans un 2-sylow, G contient un 4-cycle, le sous-groupe V_4 (voir l'exercice 1) et un sous-groupe d'ordre 4 de la dernière forme. À conjugaison près, on peut supposer que $\{\mathrm{id}, (1, 2), (3, 4), (1, 2)(3, 4), (1, 3)(2, 4), (1, 4)(2, 3)\} \subset \mathrm{G}$. Il manque alors simplement le 4-cycle et son inverse qu'on obtient par le produit $(1, 2)(1, 3)(2, 4) = (1, 3, 2, 4)$. Finalement G est conjugué du sous-groupe

$$\{\mathrm{id}, (1, 2), (3, 4), (1, 2)(3, 4), (1, 3)(2, 4), (1, 4)(2, 3), (1, 3, 2, 4), (1, 4, 2, 3)\}$$

Contrairement à ce qui précède, on n'a pas à vérifier que c'est un sous-groupe de $\mathfrak{S}_4$ car on sait qu'il existe des sous-groupes d'ordre 8 par les théorèmes de Sylow. Il est transitif et n'est pas distingué puisqu'il y a trois sous-groupes de ce type.

k) On note $\mathscr{P}$ l'ensemble des partitions d'un ensemble E à 4 éléments en deux parties à deux éléments et $\mathscr{P}_2$ l'ensemble des parties à deux éléments de E. L'application

$$\begin{cases} \mathscr{P}_2 \longrightarrow \mathscr{P} \\ \mathrm{P} \longmapsto \{\mathrm{P}, {}^{\mathrm{c}}\mathrm{P}\} \end{cases}$$

est surjective et chaque élément Q de $\mathscr{P}$ a deux antécédents : chacune des deux parties de Q. Le principe des bergers donne alors $|\mathscr{P}| = 3$. Les partitions sont $\{\{\{1, 2\}, \{3, 4\}\}, \{\{1, 3\}, \{2, 4\}\}, \{\{1, 4\}, \{2, 3\}\}\}$.

Le groupe $\mathfrak{S}_{\mathrm{E}}$ agit de façon naturelle sur l'ensemble des partitions de E en partie à deux éléments : si $\sigma \in \mathfrak{S}_{\mathrm{E}}$ et $\mathrm{Q} = \{\mathrm{P}, {}^{\mathrm{c}}\mathrm{P}\} \in \mathscr{P}$, on pose $\sigma(\mathrm{Q}) = \{\sigma(\mathrm{P}), \sigma({}^{\mathrm{c}}\mathrm{P})\}$. On obtient donc un morphisme de groupes $\psi : \mathfrak{S}_{\mathrm{E}} \to \mathfrak{S}_{\mathscr{P}}$ c'est-à-dire en choisissant une bijection entre E et $\{1,2,3,4\}$ et une bijection de $\mathscr{P}$ avec $\{1,2,3\}$ un morphisme de groupes $\psi : \mathfrak{S}_4 \to \mathfrak{S}_3$.

L'image par ψ de la transposition $(1,3)$ est la transposition des partitions $\{\{1,2\},\{3,4\}\}$ et $\{\{1,4\},\{2,3\}\}$. De même, l'image par ψ de la transposition $(1,2)$ est la transposition des partitions $\{\{1,3\},\{2,4\}\}$ et $\{\{1,4\},\{2,3\}\}$. Ainsi l'image de ψ contient deux transpositions distinctes. Comme deux transpositions distinctes de $\mathfrak{S}_3$ engendrent ce groupe, on obtient que ψ est surjective. Le noyau de ψ est donc un sous-groupe distingué de cardinal 4 de $\mathfrak{S}_4$. D'après la question **j**, ce noyau est nécessairement V_4.

l) La première ligne a été étudiée à la question **g**. La deuxième ligne a été étudiée à la question précédente. Il s'agit donc de décrire les flèches verticales et de vérifier la commutativité des diagrammes.

Par définition, L est le corps de décomposition de P sur k. Le groupe de Galois agit de façon fidèle sur l'ensemble des racines de P. On en déduit un morphisme injectif $j : \mathrm{Gal}(\mathrm{L} \mid k) \to \mathfrak{S}_4$. De même, M est le corps de décomposition de Q sur k. Le groupe de Galois agit de façon fidèle sur l'ensemble des racines de Q. On en déduit un morphisme injectif $\mathrm{Gal}(\mathrm{L} \mid k) \to \mathfrak{S}_3$. Montrons la commutativité du diagramme obtenu.

Par définition ψ s'obtient en regardant la permutation induite par $\sigma \in \mathfrak{S}_{\{\alpha_1,\alpha_2,\alpha_3,\alpha_4\}}$ sur l'ensemble des partitions de $\{\alpha_1,\alpha_2,\alpha_3,\alpha_4\}$ en ensembles à deux éléments. Si $\mathrm{Q} = \{\{\alpha_i,\alpha_j\},\{\alpha_k,\alpha_\ell\}\}$ est une telle partition, on considère alors $(\alpha_i+\alpha_j)(\alpha_k+\alpha_\ell) \in \{\theta_1,\theta_2,\theta_3\}$. On construit ainsi une bijection γ de l'ensemble $\mathscr{P}$ avec $\{\theta_1,\theta_2,\theta_3\}$. De plus, on a $\sigma(\mathrm{Q}) = \{\{\sigma(\alpha_i),\sigma(\alpha_j)\},\{\sigma(\alpha_k),\sigma(\alpha_\ell)\}\}$ et donc comme σ est un morphisme d'anneau, $\gamma(\sigma(\mathrm{Q})) = \sigma(\gamma(\mathrm{Q}))$. La permutation induite par $\sigma \in \mathrm{Gal}(\mathrm{L} \mid k)$ sur l'ensemble des partitions des racines de P en ensemble à deux éléments est donc la même que celle induite par σ sur l'ensemble $\{\theta_1,\theta_2,\theta_3\}$ c'est-à-dire la même que celle induite par la restriction de σ à M ou encore la même que celle induite par l'image de σ dans $\mathrm{Gal}(\mathrm{M} \mid k)$ ce qui donne exactement la commutativité du diagramme

$$\begin{tikzcd}
\mathrm{Gal}(\mathrm{L} \mid k) \arrow[r] \arrow[d, "j"'] & \mathrm{Gal}(\mathrm{M} \mid k) \arrow[d] \\
\mathfrak{S}_4 \arrow[r, "\psi"] & \mathfrak{S}_3
\end{tikzcd}$$

La commutativité du diagramme précédent montre que le noyau de l'application $\mathrm{Gal}(\mathrm{L} \mid k) \to \mathrm{Gal}(\mathrm{M} \mid k)$ c'est-à-dire $\mathrm{Gal}(\mathrm{L} \mid \mathrm{M})$ s'envoie par l'application (injective) $j : \mathrm{Gal}(\mathrm{L} \mid k) \to \mathfrak{S}_4$ dans le noyau de ψ qui est V_4 ce qui donne la commutativité du diagramme. De plus $\mathrm{Gal}(\mathrm{L} \mid \mathrm{M})$ est un sous-groupe de $\mathrm{Gal}(\mathrm{L} \mid k)$ et $\mathrm{Gal}(\mathrm{L} \mid k)$ un sous-groupe de $\mathfrak{S}_4$ (l'application j est injective) et donc l'application $\mathrm{Gal}(\mathrm{L} \mid \mathrm{M}) \to \mathrm{V}_4$ est injective.

m) Le polynôme Q est irréductible sur k. Le groupe de Galois de Q (c'est-à-dire $\mathrm{Gal}(\mathrm{M} \mid k)$) agit donc transitivement sur les racines de Q. Ainsi $\mathrm{Gal}(\mathrm{M} \mid k)$ est divisible par 3. La suite exacte des groupes de Galois montre $\mathrm{Gal}(\mathrm{L} \mid k)$ est divisible par 3. On en déduit (question **h**) que $\mathrm{Gal}(\mathrm{L} \mid k) \in \{12, 24\}$. Comme le discriminant de P est un carré dans k (puisque c'est le discriminant de Q), on en déduit que $\mathrm{Gal}(\mathrm{L} \mid k) \subset \mathfrak{A}_4$. Par cardinalité, on a donc $\mathrm{Gal}(\mathrm{L} \mid k) \subset \mathfrak{A}_4$.

Remarque. Le discriminant de Q est un carré dans k. Ainsi $\mathrm{Gal}(\mathrm{M} \mid k)$ est contenu dans $\mathfrak{A}_3$ et son cardinal est divisible par 3. Or les sous-groupes de $\mathfrak{S}_3$ sont $\{1\}$, les trois sous-groupes d'ordre 2 engendré par les transpositions, $\mathfrak{A}_3$ et $\mathfrak{S}_3$. On en déduit que $\mathrm{Gal}(\mathrm{M} \mid k) = \mathfrak{A}_3$. On obtient alors que $\mathrm{Gal}(\mathrm{L} \mid \mathrm{M})$ est un sous-groupe de $\mathfrak{A}_4$ de cardinal 4 c'est-à-dire V_4.

n) Le polynôme Q est irréductible sur k. Le groupe de Galois de Q (c'est-à-dire $\mathrm{Gal}(\mathrm{M} \mid k)$) agit donc transitivement sur ses racines. Ainsi $\mathrm{Gal}(\mathrm{M} \mid k)$ est divisible par 3. La suite exacte des groupes de Galois montre $\mathrm{Gal}(\mathrm{L} \mid k)$ est divisible par 3. On en déduit que $\mathrm{Gal}(\mathrm{L} \mid k) \in \{12, 24\}$. Comme le discriminant de P n'est pas un carré dans k (puisque c'est le discriminant de Q), on en déduit que $\mathrm{Gal}(\mathrm{L} \mid k) \not\subset \mathfrak{A}_4$. Comme $\mathfrak{A}_4$ est le seul sous-groupe d'ordre 12 de $\mathfrak{S}_4$, on a donc $\mathrm{Gal}(\mathrm{L} \mid k) = \mathfrak{S}_4$.

Remarque. Le discriminant de Q n'est un carré dans k. Ainsi $\mathrm{Gal}(\mathrm{M} \mid k)$ n'est pas contenu dans $\mathfrak{A}_3$ et son cardinal est divisible par 3. Or les sous-groupes de $\mathfrak{S}_3$ sont $\{1\}$, les trois sous-groupes d'ordre 2 engendrés par les transpositions $\mathfrak{A}_3$ et $\mathfrak{S}_3$. On en déduit que $\mathrm{Gal}(\mathrm{M} \mid k) = \mathfrak{S}_3$. On obtient alors que $\mathrm{Gal}(\mathrm{L} \mid \mathrm{M})$ est un sous-groupe distingué de $\mathfrak{S}_4$ de cardinal 4 c'est-à-dire V_4.

o) On écrit $\mathrm{Q} = (\mathrm{X} - \theta_1)\mathrm{Q}_1$ avec $\mathrm{Q}_1 \in k[\mathrm{X}]$, $\deg \mathrm{Q}_1 = 2$ et Q_1 n'a pas de racines dans k. Ainsi Q_1 est irréductible sur k. Le corps de décomposition sur k de Q est $\mathrm{M} = k(\theta_1,\theta_2,\theta_3) = k(\theta_2,\theta_3)$. Ainsi M est le corps de décomposition de Q_1 qui est de degré 2 et irréductible sur k. Le groupe de Galois est donc un sous-groupe de $\mathfrak{S}_2$ qui agit de façon transitive sur les racines de Q_1. Ainsi $\mathrm{Gal}(\mathrm{M} \mid k)$ est d'ordre 2.

Par ailleurs, comme P est irréductible sur M et $P(\alpha_1) = 0$, P est le polynôme minimal de α_1 sur M. On a donc $[M(\alpha_1) : M] = 4$. Comme $[L \mid M] = [L : M(\alpha_1)][M(\alpha_1) : M]$, on en déduit que

$$4 \mid [L : M] = |\mathrm{Gal}(L \mid M)|.$$

Par ailleurs, le diagramme commutatif de la question **l** montre que $\mathrm{Gal}(L \mid M)$ est un sous-groupe de V_4. Par cardinalité, on obtient $\mathrm{Gal}(L \mid M) = V_4$. Par exactitude de la suite de Galois, on obtient que $|\mathrm{Gal}(L \mid k)| = 8$ (et donc c'est un 2-Sylow de $\mathfrak{S}_4$).

p) Le groupe de Galois de P sur M c'est-à-dire $\mathrm{Gal}(L \mid M)$ n'agit pas de façon transitive sur les racines de P puisque P n'est pas irréductible sur M. Comme $\mathrm{Gal}(L \mid M)$ est un sous-groupe de V_4, on en déduit que $\mathrm{Gal}(L \mid M)$ est un sous-groupe strict de V_4 et est de cardinal 1 ou 2. Si $\mathrm{Gal}(L \mid M) = \{1\}$, par la suite exacte, on en déduit que $\mathrm{Gal}(L \mid k) = \mathrm{Gal}(M \mid k)$ est un groupe de cardinal 2 ce qui est absurde d'après la question **h**. Ainsi $\mathrm{Gal}(L \mid M)$ est de cardinal 2 et $\mathrm{Gal}(L \mid k)$ est de cardinal 4. De plus, $\mathrm{Gal}(L \mid k)$ n'est pas V_4 puisque $\mathrm{Gal}(M \mid k)$ n'est pas trivial et $\mathrm{Gal}(L \mid k)$ agit transitivement sur les racines de P dans L. La liste des sous-groupes d'ordre 4 de $\mathfrak{S}_4$ assure que $\mathrm{Gal}(L \mid k)$ est cyclique d'ordre 4 et donc $\mathrm{Gal}(L \mid k) = \mathbb{Z}/4\mathbb{Z}$.

q) On a donc $M = k$. Ainsi $\mathrm{Gal}(M \mid k) = \{1\}$ et par la suite exacte, on en déduit que $\mathrm{Gal}(L \mid M) = \mathrm{Gal}(L \mid k)$. En particulier, on en déduit que $\mathrm{Gal}(L \mid k)$ est un sous-groupe de V_4 dont le cardinal est divisible par 4. La question **h** montre, par cardinalité, $\mathrm{Gal}(L \mid M) = V_4 = (\mathbb{Z}/2\mathbb{Z})^2$.

r) Les cas des questions **m** à **q** s'excluent mutuellement, donne la liste exhaustive des situations et aboutissent à des groupes de Galois distincts. On obtient ainsi les réciproques souhaitées.

s) On est dans le cas des questions **o**, **p** et **q**. Le discriminant de Q est un carré dans k si et seulement si le discriminant de P est un carré dans k si et seulement si $\mathrm{Gal}(P \mid k)$ est contenu dans $\mathfrak{A}_4$.

Or si Q n'a qu'une seule racine dans k alors le groupe de Galois d'ordre 8 ou cyclique d'ordre 4 et donc n'a aucune chance d'être contenu dans $\mathfrak{A}_4$ puisque $8 \nmid 12$ et que $\mathfrak{A}_4$ ne contient pas d'élément d'ordre 4 (puisque ce serait un 4-cycle).

Exercice 4 – Sous-corps de $\mathbb{Q}(\sqrt[15]{2}, j)$.

a) Le polynôme $X^{15} - 2 \in \mathbb{Q}[X]$ annule $\sqrt[15]{2}$. Montrons qu'il est irréductible sur $\mathbb{Q}$. Le polynôme $X^{15} - 2$ est unitaire et à coefficients entiers. Tous ses coefficients sauf celui de plus haut degré est divisible par 2 et le coefficient constant n'est pas divisible par $4 = 2^2$. Le critère d'Eisenstein pour $p = 2$ s'applique et montre l'irréductibilité sur $\mathbb{Q}$ de $X^{15} - 2$. Ainsi $X^{15} - 2$ est le polynôme minimal de x sur $\mathbb{Q}$.

On a $j^2 + j + 1 = 0$ donc $X^2 + X + 1 \in \mathbb{Q}[X]$ annule j. Comme $j \notin \mathbb{Q}$. Le polynôme minimal de j n'est pas de degré 1. Ainsi le polynôme minimal de j est $X^2 + X + 1$.

b) On a $[L : \mathbb{Q}] = [L : \mathbb{Q}(x)][\mathbb{Q}(x) : \mathbb{Q}]$. Comme $\sqrt[15]{2} \in \mathbb{R}$, on a $\mathbb{Q}(x) \subset \mathbb{R}$ et $j \notin \mathbb{R}$. On a donc $j \notin \mathbb{Q}(x)$. On en déduit que $[L : \mathbb{Q}(x)] \geqslant 2$. Comme $X^2 + X + 1 \in \mathbb{Q}(x)$ est un polynôme annulateur de j sur $\mathbb{Q}(x)$, on en déduit que $[L : \mathbb{Q}(x)] \leqslant 2$. Ainsi $[L : \mathbb{Q}(x)] = 2$. On a donc $[L : \mathbb{Q}] = 2 \cdot 15 = 30$.

c) $\mathbb{Q}(j)$ est l'unique sous-corps de L car $4 \nmid 30$. En effet, si K est un sous-corps de L de degré 2 sur $\mathbb{Q}$. Si $j \in K$ alors $\mathbb{Q}(j) \subset K$ et par raison de dimension $\mathbb{Q}(j) = K$. Si $j \notin K$ alors j est de degré 2 sur K donc $[K(j) : \mathbb{Q}] = [K(j) : K][K : \mathbb{Q}] = 4$. Comme $K(j) \subset L$, on a $[L : \mathbb{Q}] = 30 = [L : K(j)][K(j) : \mathbb{Q}]$ et donc $4 \mid 30$. Ainsi $j \in K$ et donc $K = \mathbb{Q}(j)$.

d) Soient K un corps et G un sous-groupe fini de $\mathrm{Aut}(K)$. Le lemme d'Artin montre que l'extension $K^G \subset K$ est galoisienne de dimension $|G|$ et de groupe de galois G. Or $|\mathrm{Aut}(L)| = |\mathrm{Gal}(L \mid \mathbb{Q})| \leqslant [L : \mathbb{Q}]$ est fini, l'extension $L^{\mathrm{Aut}(L)}$ est donc galoisienne de groupe $\mathrm{Aut}(L)$ de dimension $|\mathrm{Aut}(L)|$.

e) Comme $\zeta \neq 1$, on a $1 + \zeta + \zeta^2 + \zeta^3 + \zeta^4 = (\zeta^5 - 1)/(\zeta - 1) = 0$. Ainsi $P = 1 + X + X^2 + X^3 + X^4$ est un polynôme annulateur de ζ. On a $P = (X^5 - 1)/(X - 1)$ et donc

$$P(X+1) = \frac{(X+1)^5 - 1}{(X+1) - 1} = \frac{1 + C_5^1 X + C_5^2 X^2 + C_5^3 X^3 + C_5^4 X^4 + X^5 - 1}{X} = 5 + C_5^2 X + C_5^3 X^2 + 5X^3 + X^4\,.$$

Ainsi $P(X+1) \in \mathbb{Z}[X]$ est unitaire, a tous ses coefficients divisibles par 5 sauf celui de plus haut degré ($C_5^2 = C_5^3 = 10$) et son coefficient de plus bas degré n'est pas divisible par $5^2 = 25$. Ainsi, grâce au critère d'Eisenstein appliqué à $p = 5$, $P(X+1)$ est irréductible sur $\mathbb{Q}$. En composant avec l'automorphisme de $\mathbb{Q}[X]$ donné par $X \mapsto X - 1$, on obtient que P est irréductible. Ainsi P est le polynôme minimal de ζ.

f) D'après la question précédente, on a $[\mathbb{Q}(\zeta) : \mathbb{Q}] = 4$. Si $\zeta \in L$ alors

$$30 = [L : \mathbb{Q}] = [L : \mathbb{Q}(\zeta)][\mathbb{Q}(\zeta) : \mathbb{Q}] = 4[L : \mathbb{Q}(\zeta)]$$

ce qui est absurde.

g) Soit $\sigma \in \mathrm{Aut(L)}$. Comme j est racine de $\mathrm{X}^2+\mathrm{X}+1 \in \mathbb{Q}[\mathrm{X}]$ alors $\sigma(j)$ est racine de $\mathrm{X}^2+\mathrm{X}+1$ donc $\sigma(j) \in \{j, j^2\}$. De même, $\sigma(j^2) \in \{j, j^2\}$. Par injectivité de σ, on en déduit que $\sigma(\{j, j^2\}) = \{j, j^2\}$.

L'image $\sigma(x)$ de x par σ est une racine de $\mathrm{X}^{15}-2$ contenue dans L. Or les racines de $\mathrm{X}^{15}-2$ sont

$$\mathrm{rac} = \{x, \zeta x, \zeta^2 x, \zeta^3 x, \zeta^4 x, jx, j\zeta x, j\zeta^2 x, j\zeta^3 x, j\zeta^4 x, j^2 x, j^2\zeta x, j^2\zeta^2 x, j^2\zeta^3 x, j^2\zeta^4 x\}.$$

Comme $\zeta \notin \mathrm{L}$ (ni $\zeta^2, \zeta^3, \zeta^4$ puisque ce sont aussi des racines 5e primitive de l'unité) alors que $j, x \in \mathrm{L}$, on en déduit que $\sigma(x) \in \mathrm{rac} \cap \mathrm{L} = \{x, jx, j^2x\}$. De même, $\sigma(jx) \in \{x, jx, j^2x\}$ et $\sigma(j^2x) \in \{x, jx, j^2x\}$. Encore par injectivité de σ, on obtient $\sigma(\{x, jx, j^2x\}) = \{x, jx, j^2x\}$.

Ainsi $\sigma(\{j, j^2, x, jx, j^2x\}) = \{j, j^2, x, jx, j^2x\}$.

h) On a construit dans la question précédente une application

$$\Delta\colon \begin{cases} \mathrm{Aut(L)} \longrightarrow \mathfrak{S}_{\{x,jx,j^2x\}} \\ \sigma \quad \longmapsto \sigma\big|_{\{x,jx,j^2x\}} \end{cases}$$

Comme la restriction commute avec la composition, on en déduit que Δ est un morphisme de groupes. Enfin, comme $\mathrm{L} = \mathbb{Q}(x, jx)$ puisque $jx \in \mathrm{L}$ et $j = jx/x \in \mathbb{Q}(x, jx)$, la famille (x, jx) et donc (x, jx, j^2x) est génératrice de L. Ainsi Δ est injective.

On en déduit que Aut(L) est un sous-groupe de $\mathfrak{S}_3$ et donc $|\mathrm{Aut(L)}| \in \{1, 2, 3, 6\}$. On va maintenant construire des automorphismes de L pour pouvoir obtenir le cardinal de Aut(L).

L'extension $\mathbb{Q}(x) \subset \mathbb{Q}(x, j)$ est monogène engendrée par j. Ainsi $|\mathrm{Aut}_{\mathbb{Q}(x)}(\mathbb{Q}(x, j))|$ est le nombre de racines du polynôme minimal de j sur $\mathbb{Q}(x)$ contenue dans $\mathbb{Q}(x, j)$. On a vu (question **b**) que ce polynôme minimal est $\mathrm{X}^2+\mathrm{X}+1$. On en déduit qu'il existe deux $\mathbb{Q}(x)$-automorphismes de L. De plus, ils sont déterminés par $\sigma_1(x) = x$, $\sigma_1(j) = j$ et $\sigma_2(x) = x$, $\sigma_2(j) = j^2$. Finalement $\sigma_1 = \mathrm{id}$ et $\sigma_2(jx) = j^2x$ et $\sigma_2(j^2x) = jx$. Ainsi $\Delta(\sigma_2)$ est la transposition (jx, j^2x).

Par ailleurs, on a $\mathrm{L} = \mathbb{Q}(jx, j)$ puisque $jx, j \in \mathrm{L}$ et $x = jx/j, j \in \mathbb{Q}(jx, j)$. De plus, $[\mathbb{Q}(jx) : \mathbb{Q}] = 15$ puisque $(jx)^{15} - 2 = 0$ et $\mathrm{X}^{15}-2$ est irréductible sur $\mathbb{Q}$. Comme $2 \nmid 15$, on en déduit que $j \notin \mathbb{Q}(jx)$ et donc j est de degré 2 sur $\mathbb{Q}(jx)$ et de polynôme minimal $\mathrm{X}^2+\mathrm{X}+1$. Comme précédemment, on peut construire deux $\mathbb{Q}(jx)$-automorphismes de L. L'un est l'identité, l'autre vérifie $\sigma_3(jx) = jx$ et $\sigma_3(j) = j^2$. On a alors $\sigma_3(x) = \sigma_3(j^2jx) = jjx = j^2x$ et $\sigma_3(j^2x) = x$. Ainsi $\Delta(\sigma_3)$ est la transposition (x, j^2x).

Finalement l'image de Δ contient deux transpositions distinctes et donc contient aussi le groupe engendré par ces deux transpositions c'est-à-dire $\mathfrak{S}_{\{x,jx,j^2x\}}$. Ainsi $|\mathrm{Aut(L)}| = 6$ et $\mathrm{Aut(L)} \simeq \mathfrak{S}_3$.

Enfin, d'après la question précédente, on peut définir une application

$$\Psi\colon \begin{cases} \mathrm{Aut(L)} \longrightarrow \{j, j^2\} \times \{x, jx, j^2x\} \\ \sigma \quad \longmapsto (\sigma(j), \sigma(x)). \end{cases}$$

Comme (j, x) engendre L, l'application Ψ est injective et donc bijective par cardinalité. On peut donc décrire un automorphisme de L par les images de j et x.

i) Décrivons les permutations de $\{j, j^2, x, jx, j^2x\}$ induites par $\sigma \in \mathrm{Aut(L)}$. D'après la question précédente, on peut permuter comme on veut $\{x, jx, j^2x\}$. On calcule alors l'image j par $\sigma(j) = \sigma(jx)/\sigma(x)$ et $\sigma(j^2) = \sigma(j)^2$. Ainsi on a les permutations

$$\begin{pmatrix} j & j^2 & x & jx & j^2x \\ j & j^2 & x & jx & j^2x \end{pmatrix}, \quad \begin{pmatrix} j & j^2 & x & jx & j^2x \\ j^2 & j & x & j^2x & jx \end{pmatrix}, \quad \begin{pmatrix} j & j^2 & x & jx & j^2x \\ j^2 & j & j^2x & jx & x \end{pmatrix},$$

$$\begin{pmatrix} j & j^2 & x & jx & j^2x \\ j^2 & j & jx & x & j^2x \end{pmatrix}, \quad \begin{pmatrix} j & j^2 & x & jx & j^2x \\ j & j^2 & jx & j^2x & x \end{pmatrix}, \quad \begin{pmatrix} j & j^2 & x & jx & j^2x \\ j & j^2 & j^2x & x & jx \end{pmatrix}.$$

j) Les sous-groupes de $\mathfrak{S}_3$ sont $\{\mathrm{id}\}, \{\mathrm{id}, (1,2)\}, \{\mathrm{id}, (1,3)\}, \{\mathrm{id}, (2,3)\}, \mathfrak{A}_3 = \{\mathrm{id}, (1,2,3), (1,3,2)\}$ et $\mathfrak{S}_3$. Ici, par l'identification de $\mathfrak{S}_3$ avec les permutations de l'ensemble $\{x, jx, j^2x\}$, on obtient les sous-groupes $\{\mathrm{id}\}$, $\mathrm{G}_1 = \{\mathrm{id}, \sigma_1\}$ avec $\sigma_1(x) = jx$ et $\sigma_1(j) = j^2$, $\mathrm{G}_2 = \{\mathrm{id}, \sigma_2\}$, $\mathrm{G}_3 = \{\mathrm{id}, \sigma_3\}$, $\mathrm{G} = \{\mathrm{id}, \sigma, \sigma^2\}$ avec $\sigma(x) = jx$ et $\sigma(j) = j$ et Aut(L).

k) Pour $\sigma \in \mathrm{Aut(L)}$, on a $\sigma(x) = j^\ell x$ avec $\ell \in \{0, 1, 2\}$ et donc $\sigma(x^3) = j^{3\ell}x^3 = x^3$. Ainsi $x^3 \in \mathrm{L}^{\mathrm{Aut(L)}}$ et donc $\mathbb{Q}(x^3) \subset \mathrm{Aut(L)}$. De plus, d'après les questions **d** et **h**, on a $[\mathrm{L} : \mathrm{L}^{\mathrm{Aut(L)}}] = |\mathrm{Aut(L)}| = 6$ et donc $[\mathrm{L}^{\mathrm{Aut(L)}} : \mathbb{Q}] = 5$. Comme $(x^3)^5 - 2 = 0$, $\mathrm{X}^5 - 2$ est un polynôme annulateur de x^3 sur $\mathbb{Q}$ qui est irréductible sur $\mathbb{Q}$ (en utilisant le critère d'Eisenstein pour $p = 2$). Donc $\mathrm{X}^5 - 2$ est le polynôme minimal de x^3 et $[\mathbb{Q}(x^3) : \mathbb{Q}] = 5$. On obtient donc $\mathrm{L}^{\mathrm{Aut(L)}} = \mathbb{Q}(x^3)$.

l) À la question précédente, on a vu que le polynôme minimal de x^3 est $X^5 - 2$ et que $[\mathbb{Q}(x^3) : \mathbb{Q}] = 5$.

m) L'extension $k \subset L$ est galoisienne. Les sous-corps de L contenant k sont donnés par le théorème de correspondance galoisienne. Ils sont au nombre de 6 et de la forme L^H où H est un sous-groupe de Aut(L). On a $L^{id} = L$, $L^{Aut(L)} = k$. La description de la question **i** montre que $\mathbb{Q}(j^2x) \subset L^{G_1}$. D'après le théorème de correspondance de Galois, $[L : L^{G_1}] = |G_1| = 2$. Ainsi $[L^{G_1} : \mathbb{Q}] = 15$. Comme $(j^2x)^{15} - 2 = 0$ et $X^{15} - 2$ est irréductible sur $\mathbb{Q}$, on obtient $L^{G_1} = \mathbb{Q}(j^2x)$.

De même, $L^{G_2} = \mathbb{Q}(x)$ est de degré 15 sur $\mathbb{Q}$ et $L^{G_3} = \mathbb{Q}(jx)$ est de degré 15 sur $\mathbb{Q}$.

Enfin, on a L^G est de degré $30/|G| = 10$ sur $\mathbb{Q}$. De plus, la description de la question **i** montre que $j \in L^G$. Ainsi $\mathbb{Q}(x^3, j) \subset L^G$. Or $\mathbb{Q}(x^3) \subset \mathbb{R}$ et $j \notin \mathbb{R}$. Donc j est de degré 2 sur $\mathbb{Q}(x^3)$ et $\mathbb{Q}(x^3, j)$ est de degré 10 sur $\mathbb{Q}$. Ainsi $L^G = \mathbb{Q}(x^3, j)$.

Finalement les sous-corps de L contenant $\mathbb{Q}(x^3)$ sont $\mathbb{Q}(x^3)$, $\mathbb{Q}(x^3, j)$, $\mathbb{Q}(x), \mathbb{Q}(jx), \mathbb{Q}(j^2x)$ et L.

n) Soit $\mathbb{Q} \subset K \subset \mathbb{Q}(x^3)$. On a $[K : \mathbb{Q}] \mid [\mathbb{Q}(x^3) : \mathbb{Q}] = 5$. Ainsi $[K : \mathbb{Q}] \in \{1, 5\}$ et $K = \mathbb{Q}(x^3)$ ou $K = \mathbb{Q}$.

o) On a $[L : E(x^3)][E(x^3) : E][E : \mathbb{Q}] = 30$. Ainsi $[E(x^3) : E] \mid 30$. Par ailleurs, $X^5 - 2$ est un polynôme annulateur de x^3 sur E. On en déduit que $[E(x^3) : E] \leqslant 5$ et donc $[E(x^3) : E] \in \{1, 2, 3, 5\}$. Si $[E(x^3) : E] = 1$ alors $x^3 \in E$ et donc $k = \mathbb{Q}(x^3) \subset E$ ce qui n'est pas le cas. Ainsi $[E(x^3) : E] \in \{2, 3, 5\}$.

p) On suppose que $\deg P \neq 5$. Comme $\deg P = [E(x^3) : E] \in \{2, 3, 5\}$, on en déduit que P est de degré 2 ou 3. Comme $X^5 - 2$ annule x^3, on a $P \mid X^5 - 2$. Les racines de P sont donc des éléments de

$$\left\{x^3, \zeta x^3, \zeta^2 x^3, \zeta^3 x^3, \zeta^4 x^3\right\} .$$

Si $\deg P = 2$ alors la deuxième racine de P est de la forme $\zeta^\ell x^3$ avec $\ell \in \{1, 2, 3, 4\}$ et appartient à $E(x^3)$. On en déduit que $\zeta^\ell \in L$ et que ζ^ℓ est une racine 5e primitive de l'unité ce qui est absurde d'après la question **f**.

Si $\deg P = 3$ alors $P = (X - x^3)(X - \zeta^i x^3)(X - \zeta^j x^3) \in E[X]$ avec $i, j \in \{1, 2, 3, 4\}$ et $i \neq j$. Ainsi, en regardant le terme constant, on obtient $\zeta^{i+j} x^9 \in E$. En élevant au carré et en utilisant $x^{15} = 2$, on obtient $2\zeta^{2(i+j)} x^3 \in E$. Comme $x^3 \in L$, on en déduit que $\zeta^{2(i+j)} \in L$ avec $4 \leqslant 2(i + j) \leqslant 16$. La question **f** montre alors que $2(i+j)$ est un multiple de 5. Ainsi $2(i+j) = 10$ et donc $2x^3 \in E$. On obtient ainsi une contradiction avec le fait que E ne contienne pas $\mathbb{Q}(x^3)$.

Finalement $\deg P = 5$.

q) On a $\deg P = 5 = [E(x^3) : E]$ et donc $P = X^5 - 2$ (puisque $X^5 - 2 \in E[X]$ et annule x^3).

r) On a $[L : \mathbb{Q}] = [L : E(x^3)][E(x^3) : E][E : \mathbb{Q}]$. Ainsi $[L : E(x^3)][E : \mathbb{Q}] = 30/5 = 6$. Donc $[E : \mathbb{Q}] \in \{1, 2, 3, 6\}$. Comme $E \neq \mathbb{Q}$, on a $[E : \mathbb{Q}] \in \{2, 3, 6\}$.

s) On a $[E(x^3) : \mathbb{Q}] = [E(x^3) : E][E : \mathbb{Q}] = 5 \cdot 6 = 30 = [L : \mathbb{Q}]$. Ainsi $L = E(x^3)$.

t) Si $j \notin E$ alors j est de degré 2 sur E et donc $[E(j) : \mathbb{Q}] = 6 \cdot 2 = 12 \mid [L : \mathbb{Q}] = 30$ ce qui est absurde. On en déduit que $j \in E$. Supposons que $x^5 \notin E$. Comme $X^3 - 2 \in E[X]$ annule x^5. On en déduit que x^5 est de degré $1, 2$ ou 3 sur E. Si x^5 est de degré 2 ou 3 alors $E(x^5)$ est de degré 12 ou 18 sur $\mathbb{Q}$ et $[E(x^5) : \mathbb{Q}] \mid [L : \mathbb{Q}] = 30$ ce qui est absurde. On en déduit que $x^5 \in E$.

Finalement $\mathbb{Q}(x^5, j) \subset E$. Par ailleurs, le polynôme $X^3 - 2$ est irréductible sur $\mathbb{Q}$ (par Eisenstein) et annule x^5. Ainsi $[\mathbb{Q}(x^5) : \mathbb{Q}] = 3$. De plus, $j \notin \mathbb{Q}(x^5) \subset \mathbb{R}$. On en déduit que

$$[\mathbb{Q}(x^5, j) : \mathbb{Q}] = [\mathbb{Q}(x^5, j) : \mathbb{Q}(x^5)][\mathbb{Q}(x^5) : \mathbb{Q}] = 2 \cdot 3 = 6$$

et donc $E = \mathbb{Q}(x^5, j)$.

u) L'extension $\mathbb{Q} \subset \mathbb{Q}(x^5, j)$ est séparable car on est en caractéristique nulle. De plus $\mathbb{Q}(x^5, j) = \mathbb{Q}(x^5, jx^5, j^2x^5)$ est le corps de décomposition sur $\mathbb{Q}$ de $X^3 - 2 \in \mathbb{Q}[X]$. L'extension est donc normale. Ainsi $\mathbb{Q} \subset \mathbb{Q}(x^5, j)$ est galoisienne. Comme $X^3 - 2$ est irréductible sur $\mathbb{Q}$ (par le critère d'Eisenstein), $\mathrm{Gal}(\mathbb{Q}(x^5, j) \mid \mathbb{Q})$ agit transitivement sur les racines de $X^3 - 2$. Ainsi $|\mathrm{Gal}(\mathbb{Q}(x^5, j) \mid \mathbb{Q})|$ est divisible par 3 et est un sous-groupe du groupe des permutations de $\left\{x^5, jx^5, j^2x^5\right\}$. Ainsi $\mathrm{Gal}(\mathbb{Q}(x^5, j) \mid \mathbb{Q}) \simeq \mathfrak{A}_3$ ou $\mathrm{Gal}(\mathbb{Q}(x^5, j) \mid \mathbb{Q}) \simeq \mathfrak{S}_3$. On calcule alors le discriminant D de $X^3 - 2$:

$$D = [(x^5 - jx^5)(x^5 - j^2x^5)(jx^5 - j^2x^5)]^2 = x^{30}9(j - j^2)^2 = 36j^2(1 - 2j + j^2) = 36(-3) .$$

Comme D n'est pas un carré dans $\mathbb{Q}$ (puisque $D < 0$), on obtient $\mathrm{Gal}(\mathbb{Q}(x^5, j) \mid \mathbb{Q})$ n'est pas contenu dans $\mathfrak{A}_3$ et donc $\mathrm{Gal}(\mathbb{Q}(x^5, j) \mid \mathbb{Q}) \simeq \mathfrak{S}_3$. L'isomorphisme étant réalisé comme groupe de permutation de l'ensemble $\left\{x^5, jx^5, j^2x^5\right\}$.

v) Comme $\mathfrak{S}_3$ a 6 sous-groupes (voir la question **j**) dont trois d'ordre 2 et un d'ordre 3, on en déduit que $\mathbb{Q}(x^5, j)$ a 6 sous-corps dont trois de degré $2 = 6/3$ sur $\mathbb{Q}$ et un de degré $3 = 6/2$ sur $\mathbb{Q}$. Or $\mathbb{Q}(j)$ est une extension de degré 2 de $\mathbb{Q}$ contenu dans $\mathbb{Q}(x^5, j)$. Comme $X^3 - 2$ est irréductible de degré 3 sur $\mathbb{Q}$ et que ses racines sont $\left\{x^5, jx^5, j^2x^5\right\}$, les corps $\mathbb{Q}(x^5)$, $\mathbb{Q}(jx^5)$ et $\mathbb{Q}(j^2x^5)$ sont des corps de degré 3 sur $\mathbb{Q}$

contenus dans $\mathbb{Q}(j, x^5)$. De plus, ils sont distincts car si $\mathbb{Q}(j^a x^5) = \mathbb{Q}(j^b x^5)$ avec $a, b \in \{0, 1, 2\}$ et $a \neq b$ alors $j^{a-b} = (j^a x^5)/(j^b x^5) \in \mathbb{Q}(j^a x^5) = \mathbb{Q}(j^b x^5)$ avec $a - b \in \{-2, -1, 1, 2\}$. Ainsi $\mathbb{Q}(j^a x^5) = \mathbb{Q}(j^b x^5) = \mathbb{Q}(j, x^5)$ ce qui est absurde par raison de dimension. On a donc bien trouvé les trois sous-corps de degré 3 sur $\mathbb{Q}$ de $\mathbb{Q}(x^5, j)$.

Finalement les sous-corps de $\mathbb{Q}(x^5, j)$ sont $\mathbb{Q}, \mathbb{Q}(j), \mathbb{Q}(x^5), \mathbb{Q}(jx^5), \mathbb{Q}(j^2x^5), \mathbb{Q}(j, x^5)$.

w) Si $[\mathrm{E} : \mathbb{Q}] = 2$ alors $\mathrm{E} = \mathbb{Q}(j)$ d'après la question **c**.

Donnons une autre démonstration plus longue mais utilisant la question précédente (c'est-à-dire la description des sous-corps de $\mathbb{Q}(x^5, j)$). Comme $[\mathrm{E} : \mathbb{Q}] = 2$, on a $x^5 \notin \mathrm{E}$ puisque x^5 est de degré 3 sur $\mathbb{Q}$. On en déduit que $[\mathrm{E}(x^5) : \mathrm{E}] \in \{2, 3\}$. Si $[\mathrm{E}(x^5) : \mathrm{E}] = 2$, on obtient que $[\mathrm{E}(x^5) : \mathbb{Q}] = 4$ et $[\mathrm{E}(x^5) : \mathbb{Q}] \mid [\mathrm{L} : \mathbb{Q}] = 30$ ce qui est absurde. Ainsi $[\mathrm{E}(x^5) : \mathrm{E}] = 6$ et donc ne peut contenir x^3 (puisque les extensions contenant x^3 sont de degré $5, 10, 15, 30$ sur $\mathbb{Q}$). La question **t** montre que $\mathrm{E}(x^5) = \mathbb{Q}(x^5, j)$. Ainsi E est une extension de degré 2 contenu dans $\mathbb{Q}(x^5, j)$ et donc d'après la question **v** c'est $\mathbb{Q}(j)$.

x) Si $[\mathrm{E} : \mathbb{Q}] = 3$ alors $j \notin \mathrm{E}$ puisque j est de degré 2 sur $\mathbb{Q}$ et $2 \nmid 3$. Ainsi $[\mathrm{E}(j) : \mathbb{Q}] = 6$ et $\mathrm{E}(j)$ ne contient pas x^3 (les extensions contenant x^3 sont de degré $5, 10, 15$ et 30). Ainsi d'après la question **t**, $\mathrm{E}(j) = \mathbb{Q}(x^5, j)$ et donc E est une extension de degré 3 contenue dans $\mathbb{Q}(x^5, j)$. Finalement $\mathrm{E} = \mathbb{Q}(x^5), \mathbb{Q}(jx^5)$ ou $\mathbb{Q}(j^2x^5)$.

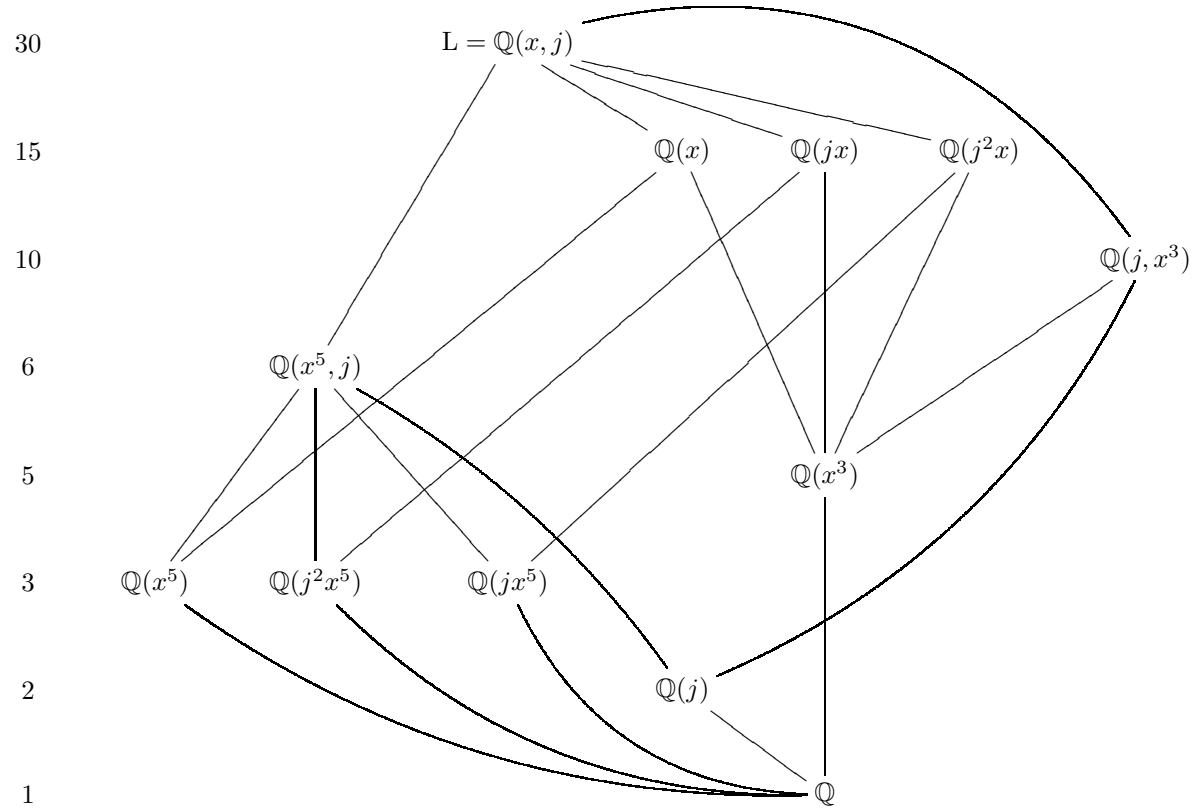
Donnons une autre démonstration suivant les indications de l'énoncé. Si $[\mathrm{E} : \mathbb{Q}] = 3$ alors $\mathrm{E}(x^3)$ est une extension de degré 15 de $\mathbb{Q}$ contenant $k = \mathbb{Q}(x^3)$. La question **m** montre que $\mathrm{E}(x^3) = \mathbb{Q}(tx)$ avec $t \in \{1, j, j^2\}$. On en déduit que $t^5x^5 = t^2x^5 \in \mathrm{E}(x^3)$. Par ailleurs, $\mathrm{X}^3 - 2$ est un polynôme irréductible sur $\mathbb{Q}$ (par le critère d'Eisenstein appliqué à $p = 2$) et annule t^2x^5. Ainsi t^2x^5 est de degré 3 sur $\mathbb{Q}$ et donc de degré inférieur ou égal à 3 sur E.

Si $t^2x^5 \notin \mathrm{E}$ alors on a t^2x^5 est de degré 2 ou 3 sur E. On a alors

$$15 = [\mathrm{E}(x^3) : \mathbb{Q}] = [\mathbb{Q}(tx) : \mathbb{Q}] = [\mathbb{Q}(tx) : \mathrm{E}(t^2x^5)][\mathrm{E}(t^2x^5) : \mathrm{E}][\mathrm{E} : \mathbb{Q}].$$

Comme $[\mathrm{E}(t^2x^5) : \mathrm{E}] \in \{2, 3\}$ et $[\mathrm{E} : \mathbb{Q}] = 3$, on en déduit que 6 ou 9 divise 15 ce qui est absurde. Ainsi $t^2x^5 \in \mathrm{E}$ et est de degré 3 sur $\mathbb{Q}$. Ainsi $\mathrm{E} = \mathbb{Q}(t^2x^5)$.

y)



Tous les corps sont représentés. Il s'agit de vérifier que toutes les inclusions le sont aussi. Celles des extensions $\mathbb{Q} \subset \mathbb{Q}(x^5, j)$ et $\mathbb{Q}(x^3) \subset \mathrm{L}$ sont données par la correspondance de Galois et sont bien représentées. Ils s'agit de vérifier les liens entre les deux. La question **n** donne les sous-corps de $\mathbb{Q}(x^3)$. Un sous-corps de $\mathbb{Q}(x^3, j)$ est de degré 1, 2 ou 5 sur $\mathbb{Q}$. Comme $\mathbb{Q}(x^3)$ est le seul sous-corps de degré 5 sur $\mathbb{Q}$ de L et $\mathbb{Q}(j)$ le seul sous-corps de $\mathbb{Q}$ degré 2. On a bien décrit les sous-corps de $\mathbb{Q}(x^3, j)$. Regardons maintenant les sous-corps de $\mathbb{Q}(x)$ qui est de degré 15 sur $\mathbb{Q}$. Ils sont de degré 1, 3 ou 5 sur $\mathbb{Q}$. Pour le degré 5, on a $\mathbb{Q}(x^3)$ qui est bien un sous-corps de $\mathbb{Q}(x)$. Pour le degré 3, on a $\mathbb{Q}(x^5)$. Pourrait-on avoir $\mathbb{Q}(jx^5)$ ou $\mathbb{Q}(j^2x^5)$ contenu dans $\mathbb{Q}(x)$. On aurait

alors $j = (jx^5)/x^5 \in \mathbb{Q}(x)$ ou $j^2 \in \mathbb{Q}(x)$ et donc $\mathrm{L} = \mathbb{Q}(x)$ ce qui est absurde. De même, on montre que $\mathbb{Q}(jx)$ a un unique sous-corps de degré 3 sur $\mathbb{Q}$ qui est $\mathbb{Q}(j^2x^5)$ et que l'unique sous-corps de degré 3 sur $\mathbb{Q}$ de $\mathbb{Q}(j^2x)$ est $\mathbb{Q}(jx^5)$.

z) Il s'agit de trouver un générateur pour les corps $\mathbb{Q}(j, x^5)$, $\mathbb{Q}(j, x^3)$ et $\mathbb{Q}(j, x)$. On utilise pour cela le résultat suivant.

Soient $\mathrm{K} \subset \mathrm{K}'$ une extension de corps et $\alpha, \beta \in \mathrm{K}'$ algébriques sur K. On suppose que β est séparable sur K. On note $\beta = \beta_1, \ldots, \beta_n$ les conjugués de β et $\alpha = \alpha_1, \ldots, \alpha_m$ les conjugués de α dans une clôture algébrique de K'. On considère $c \in \mathrm{K}$ tel que

$$c \notin \left\{ \frac{\alpha - \alpha_j}{\beta_i - \beta}, \quad i \in [\![2 \,,\, n]\!],\ j \in [\![1 \,,\, m]\!] \right\} \cap \mathrm{K} \quad = \quad \{0\} \cup \left(\left\{ \frac{\alpha - \alpha_j}{\beta_i - \beta}, \quad i \in [\![2 \,,\, n]\!],\ j \in [\![2 \,,\, m]\!] \right\} \cap \mathrm{K} \right).$$

On a alors $\mathrm{K}(\alpha, \beta) = \mathrm{K}(\alpha + c\beta)$.

Remarque. On ne se pose pas ici la question de l'existence d'un tel c qui est claire si K est infini.

Dans notre cas, comme on est en caractéristique nulle x et j sont séparables sur $\mathbb{Q}$. On peut choisir de chercher un élément générateur sous la forme $x + cj$ ou $j + cx$. Optons pour la première forme. Les conjugués de x sont les ζx où ζ appartient à $\mathbb{U}_{15}$ l'ensemble des racines quinzièmes de l'unité. Les conjugués de j sont j et j^2. On cherche donc

$$c \notin \{0\} \cup \left(\left\{ \frac{x - \zeta x}{j^2 - j}, \quad \zeta \in \mathbb{U}_{15} \smallsetminus \{1\} \right\} \cap \mathbb{Q} \right).$$

Or, pour $\zeta = \exp(2ik\pi/15)$ avec $k \in [\![1 \,,\, 14]\!]$, on a

$$\frac{x - \zeta x}{j^2 - j} = x \frac{1 - \exp(2ik\pi/15)}{-2i \sin(2\pi/3)} = x \exp(ik\pi/15) \frac{\exp(-ik\pi/15) - \exp(ik\pi/15)}{-2i \sin(2\pi/3)} = x \exp(ik\pi/15) \frac{\sin k\pi/15}{\sin 2\pi/3} \notin \mathbb{R}\,.$$

Finalement, n'importe quel $c \in \mathbb{Q} \smallsetminus \{0\}$ convient. En particulier, pour $c = 1$, on obtient $\mathbb{Q}(x+j) = \mathbb{Q}(x, j) = \mathrm{L}$.

Comme les conjugués de x^3 sont les ζx^3 où $\zeta \in \mathbb{U}_5$ l'ensemble des racines cinquièmes de l'unité, on obtient par un calcul similaire au précédent que $\mathbb{Q}(x^3 + j) = \mathbb{Q}(x^3, j)$. Enfin comme les conjugués de x^5 sont les ζx^5 où $\zeta \in \mathbb{U}_3$ l'ensemble des racines cubique de l'unité, on obtient que $\mathbb{Q}(x^5 + j) = \mathbb{Q}(x^5, j)$.

Montrons à présent le résultat. Il est clair que $\mathrm{K}(\alpha + c\beta) \subset \mathrm{K}(\alpha, \beta)$. De plus, si $\beta \in \mathrm{K}(\alpha + c\beta)$ alors $\alpha = (\alpha + c\beta) - c\beta \in \mathrm{K}(\alpha + c\beta)$ et donc $\mathrm{K}(\alpha, \beta) \subset \mathrm{K}(\alpha + c\beta)$. Finalement, il reste à montrer que $\beta \in \mathrm{K}(\alpha + c\beta)$ ou encore que le polynôme minimal π_β de β sur $\mathrm{K}(\alpha + c\beta)$ est de degré 1.

On note $\pi_{\alpha,\mathrm{K}}$ le polynôme minimal de α sur K et $\pi_{\beta,\mathrm{K}}$ celui de β sur K. Or β est séparable sur K, donc

$$\pi_{\beta,\mathrm{K}} = \prod_{i=1}^{n} (\mathrm{X} - \beta_i)\,.$$

Ainsi, comme $\pi_\beta \mid \pi_{\beta,\mathrm{K}}$, il existe $\mathrm{I} \subset [\![1 \,,\, n]\!]$ contenant 1 telle que

$$\pi_\beta = \prod_{i \in \mathrm{I}} (\mathrm{X} - \beta_i)\,.$$

Pour obtenir d'autres informations sur π_β, on cherche un polynôme appartenant à $\mathrm{K}(\alpha + c\beta)[\mathrm{X}]$ dont β est racine. $\pi_{\alpha,\mathrm{K}}((\alpha + c\beta) - c\mathrm{X})$ convient et est donc un multiple de π_β. Toutes les racines de π_β sont donc racines de $\pi_{\alpha,\mathrm{K}}((\alpha + c\beta) - c\mathrm{X})$. En particulier si $\{1\} \subsetneq \mathrm{I}$, il existe $j \geqslant 2$ tel que $\pi_{\alpha,\mathrm{K}}((\alpha + c\beta) - c\beta_j) = 0$. Ainsi $(\alpha + c\beta) - c\beta_j$ est l'un des conjugués de α sur K et donc il existe $i \in [\![1 \,,\, m]\!]$ tel que $\alpha + c\beta = \alpha_i + c\beta_j$. On contredit ainsi l'hypothèse sur c.

aa) La famille $(1, x, \ldots, x^{14})$ est une $\mathbb{Q}$-base de $\mathbb{Q}(x)$. De plus $(1, j)$ est une $\mathbb{Q}(x)$-base de $\mathrm{L} = \mathbb{Q}(x, j)$ puisque $j \notin \mathbb{Q}(x)$. Ainsi, d'après le théorème de la base télescopique, $(1, x, \ldots, x^{14}, j, jx, \ldots, jx^{14})$ est une $\mathbb{Q}$-base de L. La matrice de la multiplication par $x \in \mathrm{L}$ dans cette base est constituée de deux blocs compagnons du polynôme $\mathrm{X}^{15} - 2$. Comme $\mathrm{X}^{15} - 2 \mid \mathrm{X}^{15} - 2$, on peut ainsi lire les invariants de similitude sur cette matrice : il s'agit de $(\mathrm{X}^{15} - 2, \mathrm{X}^{15} - 2)$.

En généralisant ce qui précède, on montre facilement que si $k \subset \mathrm{L}$ est une extension de corps et $x \in \mathrm{L}$ alors les invariants de similitude de la multiplication par x (en tant que k-endomorphisme de L) sont $(\pi_x, \ldots, \pi_x)$ où π_x est le polynôme minimal de x et où le nombre de π_x est $[\mathrm{L} : \mathbb{Q}(x)]$.

Exercice 5 — Bases de réseaux d'un espace vectoriel euclidien.

a) Γ est un groupe abélien de type fini. Le théorème de classification des $\mathbb{Z}$-modules de type fini (c'est-à-dire des groupes abéliens de type fini) assure qu'il suffit de montrer que Γ est sans torsion pour montrer qu'il est libre. Considérons donc $x \in \Gamma \smallsetminus \{0\}$ et $n \in \mathbb{Z}$ tel que $nx = 0$. L'égalité $nx = 0$ est vrai dans le k-espace vectoriel V contenant Γ, on a donc $n = 0$ puisque $x \neq 0$. Ainsi x n'est pas de torsion et $\Gamma_{\mathrm{tors}} = \{0\}$.

b) Si $\mathrm{X} \in \mathrm{GL}_n(\mathbb{Z})$ alors il existe $\mathrm{Y} \in \mathrm{M}_n(\mathbb{Z})$ tel que $\mathrm{XY} = \mathrm{YX} = \mathrm{I}_n$. On a donc $\det \mathrm{X} \in \mathbb{Z}$ et $\det \mathrm{Y} \in \mathbb{Z}$ et $\det \mathrm{X} \det \mathrm{Y} = \det \mathrm{Y} \det \mathrm{X} = \det \mathrm{I}_n = 1$. Ainsi $\det \mathrm{X}$ est inversible dans $\mathbb{Z}$ c'est-à-dire $\det \mathrm{X} \in \{-1, 1\}$.

Réciproquement si $\det \mathrm{X} \in \{-1, 1\}$ et $\mathrm{X} \in \mathrm{M}_n(\mathbb{Z})$. La comatrice $\mathrm{Com}(\mathrm{X})$ de X est à coefficient dans $\mathbb{Z}$. De plus X est inversible dans $\mathrm{M}_n(\mathbb{Q})$ et son inverse est $\det(\mathrm{X})^{-1}\, {}^t\mathrm{Com}(\mathrm{X}) = \det(\mathrm{X})\, {}^t\mathrm{Com}(\mathrm{X}) \in \mathrm{M}_n(\mathbb{Z})$. Ainsi en posant $\mathrm{Y} = \det(\mathrm{X})^{-1}\, {}^t\mathrm{Com}(\mathrm{X})$, on obtient que $\mathrm{XY} = \mathrm{YX} = \mathrm{I}_n$ avec $\mathrm{Y} \in \mathrm{M}_n(\mathbb{Z})$. Finalement $\mathrm{X} \in \mathrm{GL}_n(\mathbb{Z})$.

c) Soient $\mathscr{B} = (e_1, \dots, e_t)$ une $\mathbb{Z}$-base de Γ et $\mathscr{C} = (f_1, \dots, f_s)$ une base du groupe abélien libre Γ. Il s'agit de démontrer que $\mathscr{C}$ est une famille libre de V c'est-à-dire que l'espace vectoriel engendré par les f_i est de dimension s.

Comme $\mathscr{B}$ et $\mathscr{C}$ sont des bases du groupe abélien Γ, on a $s = t = \mathrm{rg}_{\mathbb{Z}}(\Gamma)$. Il s'agit donc de montrer que l'espace vectoriel engendré par les f_i est de dimension t.

Comme $\mathscr{B}$ est une base du groupe abélien Γ, on peut écrire

$$\forall\, j \in [\![1\,,\, t]\!], \qquad f_j = \sum_{j=1}^{t} a_{ij} e_i \qquad \text{avec} \quad a_{ij} \in \mathbb{Z}.$$

Ainsi $f_j \in \mathrm{vect}\,(e_1, \dots, e_t)$. L'espace vectoriel engendré par les f_j est donc contenu dans $\mathrm{vect}\,(e_1, \dots, e_t)$. Il est donc de dimension t si et seulement s'il est égal à $\mathrm{vect}\,(e_1, \dots, e_t)$.

Comme $e_i \in \Gamma$ et que $\mathscr{C}$ est une base du groupe abélien Γ, on peut écrire,

$$\forall\, j \in [\![1\,,\, t]\!], \qquad e_j = \sum_{i=1}^{t} a_{ij} f_i \qquad \text{avec} \quad a_{ij} \in \mathbb{Z}$$

En particulier, on a $e_j \in \mathrm{vect}\,(f_1, \dots, f_t)$ pour tout $j \in [\![1\,,\, t]\!]$ et donc $\mathrm{vect}\,(e_1, \dots, e_t) \subset \mathrm{vect}\,(f_1, \dots, f_t)$. Finalement $\mathrm{vect}\,(f_1, \dots, f_t)$ est bien de dimension t.

d) $(i) \Rightarrow (ii)$. On considère Λ' tel que $\Lambda' \oplus \Lambda = \Gamma$. La restriction à Λ' de la surjection canonique $\pi : \Gamma \to \Gamma/\Lambda$ réalise un isomorphisme entre Γ' et Γ/Λ. En effet $\pi(\Lambda') = \pi(\Lambda' + \Lambda) = \pi(\Gamma) = \Gamma/\Lambda$ et le noyau de la restriction de π est $\Lambda' \cap \mathrm{Ker}\,\pi = \Lambda' \cap \Lambda = \{0\}$. Ainsi $\Lambda' \simeq \Gamma/\Lambda$. Comme Λ' est un sous-module d'un module libre de type fini, Λ' est libre et donc Λ/Γ aussi.

$(ii) \Rightarrow (iii)$ est toujours vrai. Un module libre sur un anneau intègre n'a jamais d'éléments de torsion (autre que 0).

$(iii) \Rightarrow (ii)$. Γ/Λ est un quotient d'un $\mathbb{Z}$-module de type fini, c'est donc un $\mathbb{Z}$-module de type fini puisque l'image par π d'une famille génératrice de Γ est une famille génératrice de Γ/Λ. Comme $\mathbb{Z}$ est un anneau principal, un $\mathbb{Z}$-module de type fini sans torsion est libre.

$(iii) \Rightarrow (iv)$. Par définition des facteurs invariants de Λ, il existe une base $\mathscr{B} = (e_1, \dots, e_n)$ du groupe abélien Γ tel que $(a_1 e_1, \dots, a_s e_s)$ soit une base du groupe abélien Λ. En écrivant

$$\Gamma = \mathbb{Z}e_1 \oplus \cdots \oplus \mathbb{Z}e_n \qquad \text{et} \qquad \Lambda = \mathbb{Z}a_1 e_1 \oplus \cdots \oplus \mathbb{Z}a_s e_s\,.$$

On obtient
$$\Gamma/\Lambda \quad \simeq \quad \mathbb{Z}/a_1\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/a_s\mathbb{Z} \oplus \mathbb{Z}^{n-s}\,.$$

Or, par définition des facteurs invariants, on a $a_i \neq 0$. On obtient donc $(\Gamma/\Lambda)_{\mathrm{tors}} = \mathbb{Z}/a_1\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/a_s\mathbb{Z}$ qui est de cardinal $a_1 \cdots a_s$. Comme Γ/Λ est sans torsion, on obtient que $|(\Gamma/\Lambda)_{\mathrm{tors}}| = 1$. Ainsi $a_1 \cdots a_s = 1$ et donc $a_i = 1$ pour tout $i \in [\![1\,,\, s]\!]$.

$(iv) \Rightarrow (i)$. Par définition des facteurs invariants de Λ, il existe une base $\mathscr{B} = (e_1, \dots, e_n)$ du groupe abélien Γ tel que $(e_1, \dots, e_s)$ soit une base du groupe abélien Λ. En posant $\Lambda' = \langle e_{s+1}, \dots, e_n \rangle_{\mathbb{Z}-\mathrm{mod.}}$. On obtient que $\Gamma = \Lambda \oplus \Lambda'$.

e) $(iii) \Rightarrow (ii)$. On a $\Lambda \subset \Gamma$ et $\Lambda \subset \mathrm{vect}_{\mathbb{Q}}(\Lambda)$. Donc $\Lambda \subset \Gamma \cap \mathrm{vect}_{\mathbb{Q}}(\Lambda)$. Par ailleurs, $\mathrm{vect}_{\mathbb{Q}}(\Lambda) \subset \mathrm{vect}_k(\Lambda)$ et donc $\Gamma \cap \mathrm{vect}_{\mathbb{Q}}(\Lambda) \subset \Gamma \cap \mathrm{vect}_k(\Lambda) = \Gamma$. On a bien l'égalité souhaitée.

$(ii) \Rightarrow (i)$. On reprend les notations de la question précédente : on note $(a_1, \dots, a_s)$ les facteurs invariants de Λ par rapport à Γ. Soit $\mathscr{B} = (e_1, \dots, e_n)$ une base adaptée à Λ. La famille $(a_1 e_1, \dots, a_s e_s)$ est donc une base Λ.

Pour $i \in [\![1\,,\, s]\!]$, on a $e_i = {a_i}^{-1} a_i e_i \in \Gamma \cap \mathrm{vect}_{\mathbb{Q}}(\Lambda) = \Lambda$. Ainsi, on peut écrire

$$e_i = \sum_{j=1}^{s} n_j a_j e_j \qquad \text{avec} \quad n_j \in \mathbb{Z}\,.$$

Comme la famille $(e_1, \dots, e_n)$ est une base du groupe abélien Γ, on obtient que $n_i a_i = 1$ et donc a_i est inversible dans $\mathbb{Z}$. Ainsi $a_i = 1$ et d'après la question précédente, Λ est facteur direct dans Γ.

$(i) \Rightarrow (iii)$. On a $\Lambda \subset \Gamma$ et $\Lambda \subset \operatorname{vect}_k(\Lambda)$. Donc $\Lambda \subset \Gamma \cap \operatorname{vect}_k(\Lambda)$. On reprend les notations de $(ii) \Rightarrow (i)$. Comme les éléments de Λ sont les combinaisons linéaires à coefficients entiers des $a_i e_i$ et que $a_i \neq 0$, on obtient que $e_i \in \operatorname{vect}_k(\Lambda)$ et $\Lambda \subset \operatorname{vect}_k(e_1, \ldots, e_s)$. On a donc $\operatorname{vect}_k(\Lambda) = \operatorname{vect}_k(e_1, \ldots, e_s)$.

Un élément $x \in \operatorname{vect}_k(\Lambda) \cap \Gamma$ s'écrit donc

$$x = \sum_{i=1}^{s} \lambda_i e_i = \sum_{i=1}^{n} n_i e_i \qquad \text{avec} \qquad \lambda_i \in k,\ n_i \in \mathbb{Z}.$$

Comme $(e_1, \ldots, e_n)$ est une base du réseau Γ, la question **c** montre que $(e_1, \ldots, e_n)$ est une famille libre de V. Ainsi, on a $n_i = 0$ pour $i > s$ et $n_i = \lambda_i$ pour $i \in [\![1\,,\, s]\!]$.

Enfin, comme Λ est facteur direct de Γ, la question précédente montre que $a_1 = \cdots = a_s = 1$ et donc $e_i \in \Lambda$ pour tout $i \in [\![1\,,\, s]\!]$. Ainsi

$$x = \sum_{i=1}^{s} n_i e_i \in \Lambda\,.$$

f) $\Gamma \cap \mathrm{F}$ est un sous-groupe de Γ. C'est donc un sous-groupe d'un groupe abélien libre de type fini. Ainsi $\Gamma \cap \mathrm{F}$ est un groupe abélien libre de type fini.

Comme Γ est un groupe abélien de type fini, $p(\Gamma)$ est un groupe abélien de type fini (engendré par les images par p d'une famille génératrice finie de Γ). De plus, $p(\Gamma)$ est contenu dans W. La question **a** montre que $p(\Gamma)$ est libre.

g) Considérons une base $\mathscr{B}$ adaptée au sous-groupe $\Gamma \cap \mathrm{F}$ de Γ. Ainsi $\mathscr{B} = (e_1, \ldots, e_n)$ est une base du groupe abélien Γ et il existe donc $(a_1, \ldots, a_s) \in (\mathbb{N}^\times)^s$ tel que $(a_1 e_1, \ldots, a_s e_s)$ soit une base de $\Gamma \cap \mathrm{F}$.

Par ailleurs, l'application $p : \Gamma \mapsto p(\Gamma)$ est surjective et de noyau $\Gamma \cap \operatorname{Ker} p = \Gamma \cap \mathrm{F}$. Ainsi p induit un isomorphisme entre $\Gamma/\Gamma \cap \mathrm{F}$ et $p(\Gamma)$. La question précédente montre que $p(\Gamma)$ est libre. Ainsi $\Gamma/\Gamma \cap \mathrm{F}$ est libre et la question **d** montre que $a_1 = \cdots = a_s = 1$. Finalement $(e_1, \ldots, e_s)$ est une base de $\Gamma \cap \mathrm{F}$. En particulier, $e_i \in \mathrm{F}$.

Montrons que la famille $(p(e_{s+1}), \ldots, p(e_n))$ est une base de $p(\Gamma)$. La famille $(e_1, \ldots, e_n)$ est génératrice de Γ donc la famille $(p(e_1), \ldots, p(e_n))$ est génératrice de $p(\Gamma)$. Or $p(e_i) = 0$ pour $i \in [\![1\,,\, s]\!]$ puisque $e_i \in \mathrm{F} = \operatorname{Ker} p$. Ainsi $(p(e_{s+1}), \ldots p(e_n))$ est génératrice de $p(\Gamma)$.

Montrons la $\mathbb{Z}$-liberté de $(p(e_{s+1}), \ldots, p(e_n))$.

Première méthode : à la main. Soient $n_i \in \mathbb{Z}$ tels que

$$\sum_{i=s+1}^{n} n_i p(e_i) = 0$$

On a donc

$$x = \sum_{i=s+1}^{n} n_i e_i \in \mathrm{F}$$

Comme les e_i forment une base du groupe abélien Γ, on a $x \in \Gamma$. Ainsi $x \in \Gamma \cap \mathrm{F}$ et s'écrit comme une combinaison linéaire à coefficients entiers des e_i pour $i \in [\![1\,,\, s]\!]$. Comme $(e_1, \ldots, e_n)$ forme une base du groupe abélien Γ, on obtient que $x = 0$ et $n_i = 0$ pour tout $i \geqslant s + 1$.

Deuxième méthode : plus abstraite. Comme $\Gamma \cap \mathrm{F}$ est facteur direct de Γ (puisque $a_1 = \cdots = a_s = 1$), $\Gamma/\Gamma \cap \mathrm{F}$ est un module libre de rang $\operatorname{rg}(\Gamma) - \operatorname{rg}(\mathrm{F} \cap \Gamma) = n - s$. Or $p(\Gamma)$ est un groupe abélien libre isomorphe à $\Gamma/\Gamma \cap \mathrm{F}$. Ainsi $p(\Gamma)$ est un groupe libre de rang $n - s$. La famille génératrice $(p(e_{s+1}), \ldots, p(e_n))$ a pour cardinal $n - s$, c'est donc une base de $p(\Gamma)$.

Attention, on utilise le résultat suivant : soient M un module libre de rang n sur un anneau commutatif A (on n'a même pas besoin de le supposer principal ou intègre) et $(f_1, \ldots, f_n)$ une famille génératrice de M alors $(f_1, \ldots, f_n)$ est une base de M.

Attention, le résultat correspondant pour les familles libres est faux, comme le montre l'exemple suivant. L'élément $2 \in \mathbb{Z}$ est une famille libre du $\mathbb{Z}$-module $\mathbb{Z}$ qui est libre de rang 1 mais n'est pas une base puisque les bases de $\mathbb{Z}$ sont $\{1\}$ et $\{-1\}$.

Montrons le résultat annoncé. On considère $(e_1, \ldots, e_n)$ une base de M. En écrivant les f_i en fonction des e_j, on construit une matrice (carré car la famille génératrice a pour cardinal le rang de M) $\mathrm{U} \in \mathrm{M}_n(\mathrm{A})$. De même, en écrivant les e_i en fonction des f_j (ce qu'on peut faire puisque la famille $(f_1, \ldots, f_n)$ est génératrice), on obtient $\mathrm{V} \in \mathrm{M}_n(\mathrm{A})$. Comme la famille $(e_1, \ldots, e_n)$ est libre, on obtient $\mathrm{UV} = \mathrm{I}_n$. Ainsi $\det \mathrm{U} \in \mathrm{A}^\times$ et U est inversible (voir la question **b** en remplaçant $\mathbb{Z}$ par A) et la famille $(f_1, \ldots, f_n)$ est une base.

h) On remarque que pour les deux questions qui précèdent, on n'a pas utilisé la surjectivité de p ni le fait que Γ était un réseau ou un sous-réseau de V juste le fait que Γ est libre de type fini. On note r la dimension de F. Comme p est surjective, on a $\dim \mathrm{W} = \dim \mathrm{V} - r$.

On applique la question **g** à Γ. Comme Γ est un réseau de V, on a $n = \dim \mathrm{V}$ et $(e_1, \dots, e_n)$ est une base de V d'après la question **c**.

$(iii) \Leftrightarrow (iv)$. Comme $\mathrm{rg}\,(p(\Gamma)) = n - s$ et $\dim_k \mathrm{W} = n - r$, la condition (iii) s'écrit $n - s \leqslant n - r$ c'est-à-dire $r \leqslant s$. Comme $\mathrm{rg}\,(\Gamma \cap \mathrm{F}) = s$ et $\dim_k \mathrm{F} = r$, la condition (iv) s'écrit $s \geqslant r$.

On a évidemment $(v) \Rightarrow (iii)$ et $(vi) \Rightarrow (iv)$.

D'après la question **c** et la question **g**, on a $p(\Gamma)$ est un réseau si et seulement si $(p(e_{s+1}), \dots, p(e_n))$ est une base de W ce qui implique $n - s = \dim_k \mathrm{W}$ et donc $(i) \Rightarrow (v)$.

D'après la question **c** et la question **g**, on a $\Gamma \cap \mathrm{F}$ est un réseau si et seulement si $(e_1, \dots, e_s)$ est une base de F ce qui implique $s = \dim_k \mathrm{F}$ et donc $(ii) \Rightarrow (vi)$.

On suppose (iii). La famille $(e_1, \dots, e_n)$ est une k-base de V, donc la famille $(p(e_1), \dots, p(e_n))$ est une famille k-génératrice de $p(\mathrm{V}) = \mathrm{W}$. Comme $p(e_i) = 0$ pour $i \in [\![1\,,\, s]\!]$, on en déduit que $(p(e_{s+1}), \dots, p(e_n))$ est une famille k-génératrice de W. On a donc $n - s \geqslant \dim_k \mathrm{W} = n - r$. La condition (iii) donne alors $r = s$ et $(p(e_{s+1}), \dots, p(e_n))$ est une k-base de W. Ainsi, comme $(p(e_{s+1}), \dots, p(e_n))$ est aussi une $\mathbb{Z}$-base de $p(\Gamma)$, $p(\Gamma)$ est bien un réseau de W.

On suppose (iv). La famille $(e_1, \dots, e_n)$ est une k-base de V. Comme $e_i \in \mathrm{F}$ pour $i \in [\![1\,,\, s]\!]$, la famille $(e_1, \dots, e_s)$ est une famille k-libre de F. Ainsi $\mathrm{rg}\,(\Gamma \cap \mathrm{F}) = s \leqslant \dim_k \mathrm{F}$. Le point (iv) donne alors

$$\mathrm{rg}\,(\Gamma \cap \mathrm{F}) = \dim_k(\mathrm{F})\,.$$

Ainsi la famille $(e_1, \dots, e_s)$ est une k-base de F. Comme $(e_1, \dots, e_s)$ est aussi une $\mathbb{Z}$-base de $\Gamma \cap \mathrm{F}$, $\Gamma \cap \mathrm{F}$ est bien un réseau de F.

i) L'application p est surjective de noyau $\mathrm{F} = \mathrm{Vect}_{\mathbb{R}}(\Lambda)$. D'après la question précédente, il suffit de montrer que $\mathrm{rg}\,(\Lambda) \geqslant \dim_k \mathrm{F}$. On considère une base du groupe abélien Λ. C'est une famille génératrice de l'espace vectoriel $\mathrm{F} = \mathrm{Vect}_{\mathbb{R}}(\Lambda)$. On a donc bien $\mathrm{rg}\,(\Lambda) \geqslant \dim_k \mathrm{F}$ et $p(\Gamma)$ est un réseau de W.

j) On va montrer que $\mathrm{W} \neq 0$. Comme Λ est facteur direct de Γ, la question **d** et le théorème de la base adaptée montre qu'il existe une base $(e_1, \dots, e_n)$ de Γ telle que $(e_1, \dots, e_s)$ soit une base de Λ. Comme $\Lambda \neq \Gamma$, on a $s < n$. Par ailleurs, Γ est un réseau de V et la question **c** montre que $(e_1, \dots, e_n)$ est une base de V. Ainsi $\mathrm{F} = \mathrm{vect}_{\mathbb{R}}(\Lambda)$ est de dimension au plus s et donc $\mathrm{F} \neq \mathrm{V}$. Ainsi $\mathrm{W} \neq 0$. On en déduit qu'il existe $x \in p(\Gamma)$ tel que $|x| = \mathrm{Min}_{\mathrm{ar}}(p(\Gamma))$. Il existe donc $v \in \Gamma$ tel que $x = p(v)$. Comme $|x| \neq 0$, on a $v \notin \mathrm{Ker}\, p = \mathrm{F}$ et donc $v \notin \Lambda \subset \mathrm{F}$. Ainsi $v \in \Gamma \smallsetminus \Lambda$.

k) Si $\mathscr{B}$ est une base du groupe Λ, les questions **h** et **i** montrent que $\mathscr{B}$ est une $\mathbb{R}$-base de F. Comme $v \notin \mathrm{F}$ puisque $p(v) \neq 0$. La famille $(\mathscr{B}, v)$ est $\mathbb{R}$-libre et donc $\mathbb{Z}$-libre et engendre (en tant que groupe) $\Lambda + \mathbb{Z}v$. Ainsi c'est une base du groupe abélien $\Lambda + \mathbb{Z}v$ qui est donc libre de rang $\mathrm{rg}\,(\Lambda) + 1$.

l) Montrons que $p(v)$ commence une base de $p(\Gamma)$. Soit $\mathscr{C} = (e_1, \dots, e_r)$ une base de $p(\Gamma)$. On peut écrire

$$p(v) = \sum_{i=1}^{r} n_i e_i \qquad \text{avec} \qquad n_i \in \mathbb{Z}.$$

Soit $d = \mathrm{pgcd}\,(n_i,\ 1 \leqslant i \leqslant r)$. On a alors $d = 1$. En effet, si $d > 1$ alors $p(v)/d \in p(\Gamma)$ et $\|p(v)/d\| < \|p(v)\|$ ce qui contredit la construction de v.

Le théorème de classification des matrices à équivalence près sur l'anneau principal $\mathbb{Z}$ assure qu'il existe $\mathrm{P} \in \mathrm{GL}_r(\mathbb{Z})$ tel que

$$\mathrm{P} \begin{bmatrix} n_1 \\ n_2 \\ \vdots \\ n_r \end{bmatrix} = \begin{bmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{bmatrix}$$

On note alors $\mathrm{P}^{-1} = (q_{ij})_{i,j}$. En posant, pour $j \in [\![1\,,\, r]\!]$,

$$f_j = \sum_{i=1}^{r} q_{ij} e_i\,,$$

on construit une base $\mathscr{C}$ de $p(\Gamma)$ dont le premier vecteur est

$$\sum_{i=1}^{r} q_{i1} e_i = \sum_{i=1}^{r} n_i e_i = p(v).$$

Ainsi, $\mathbb{Z}p(v)$ admet un supplémentaire dans $p(\Gamma)$ et, d'après la question **d**, $p(\Gamma)/\mathbb{Z}p(v)$ est sans torsion.

L'application $p : \Gamma \to p(\Gamma)$ est surjective de noyau $\operatorname{Ker} p \cap \Gamma = \operatorname{vect}_{\mathbb{R}}(\Lambda) \cap \Gamma$. Or, d'après la question **e**, $\operatorname{vect}_{\mathbb{R}}(\Lambda) \cap \Gamma = \Lambda$. Ainsi p induit, par passage au quotient, un isomorphisme entre Γ/Λ et $p(\Gamma)$ qui envoie $v + \Lambda$ sur $p(v)$. Le sous-groupe de Γ/Λ correspondant à $\mathbb{Z}p(v)$ via l'isomorphisme donné par p est donc $\mathbb{Z}(v + \Lambda) = (\mathbb{Z}v + \Lambda)/\Lambda$. On a donc

$$(\Gamma/\Lambda)/((\mathbb{Z}v + \Lambda)/\Lambda) \simeq p(\Gamma)/\mathbb{Z}p(v)$$

Ainsi $(\Gamma/\Lambda)/((\mathbb{Z}v + \Lambda)/\Lambda)$ est sans torsion. Les isomorphismes classiques montrent que

$$(\Gamma/\Lambda)/((\mathbb{Z}v + \Lambda)/\Lambda) \simeq \Gamma/(\mathbb{Z}v + \Lambda).$$

Ainsi $\Gamma/(\mathbb{Z}v + \Lambda)$ est sans torsion. La question **d** prouve que $\mathbb{Z}v + \Lambda$ est facteur direct dans Γ.

m) (i) On pose $\mathscr{B} = \varnothing$.

(ii) Si $|\mathscr{B}| = \dim \mathrm{V}$, donner $\mathscr{B}$.

(iii) Sinon, on pose $\Lambda = \langle \mathscr{B} \rangle_{\mathrm{Gr}}$, $\mathrm{F} = \mathrm{Vect}_{\mathbb{R}}(\mathscr{B}) = \mathrm{Vect}_{\mathbb{R}}(\Lambda)$, $\mathrm{W} = \mathrm{F}^{\perp}$ et $p : \mathrm{V} \to \mathrm{W}$ la projection orthogonale parallèlement à F et on choisit v tel que $p(v) = \mathrm{Min}_{\mathrm{ar}}(p(\Gamma))$.

(iv) On pose $\mathscr{B} = \mathscr{B} \cup \{v\}$ et on revient en (ii).

Montrons que l'algorithme aboutit à la base souhaitée. On montre par récurrence sur $j \in [\![0 , n]\!]$, qu'au $j + 1^{\mathrm{e}}$ passage dans la boucle, Λ est un facteur direct de Γ de rang j et $\mathscr{B}$ est une famille $\mathbb{R}$-libre.

Au rang 0, $\Lambda = \{0\}$ est bien facteur direct de Γ de rang 0 et $\mathscr{B}$ est $\mathbb{R}$-libre. Supposons $j < \dim \mathrm{V}$ et qu'au $(j + 1)^{\mathrm{e}}$ passage dans la boucle Λ est facteur direct de Γ de rang j. En particulier, $\Lambda \neq \Gamma$. Les questions **j**, **k** et **l** s'appliquent et assurent que $\Lambda + \mathbb{Z}v = \langle \mathscr{B} \cup v \rangle_{\mathrm{Gr}}$ est libre de rang $j + 1$ et facteur direct de Γ. De plus, à la question **j**, on a vu que $v \notin \mathrm{F}$ et donc $\mathscr{B} \cup \{v\}$ est libre. Au rang $\dim \mathrm{V}$, on obtient donc que Λ est facteur direct de Γ de rang Γ. On peut donc écrire $\Lambda \oplus \Lambda' = \Gamma$ avec $\operatorname{rg}(\Lambda') = \operatorname{rg} \Gamma - \operatorname{rg} \Lambda$ et donc $\Lambda' = \{0\}$. Ainsi $\Lambda = \Gamma$. De plus, $\mathscr{B}$ est une famille génératrice de Γ qui est $\mathbb{R}$-libre et donc $\mathbb{Z}$-libre. Ainsi $\mathscr{B}$ est une base du groupe abélien Γ.