Théorie de Galois

Exercices corrigés de
Algebra[1],
Hungerford, Thomas W.

Adem Öztürk et Fabien Trihan

2 avril 2004

[1]Reprint of the 1974 original. Graduate Texts in Mathematics, 73. Springer-Verlag, New York-Berlin, 1980.

Informations

- L'exercice 2 de la section 3 du chapitre V sera mentionné avec la notation "exercice 2" tout au long de la section 3, et avec la notation "exercice 3.2" dans les autres sections du chapitre V.

  La notation "exercice II 3.2" sera utilisée pour l'exercice 2 de la section 3 du chapitre II.

- Le Lemme (ou Corollaire, Théorème, Proposition) 2 de la section 3 du chapitre V sera mentionné avec la notation "Lemme 3.2" dans toutes les sections du chapitre V.

  La notation "Lemme II 3.2" sera utilisée pour le Lemme 2 de la section 3 du chapitre II.

Notations

0.1

0.1.1.

Soit $n, m \in \mathbb{N}$.

- $n \mid m$ signifie que n divise m.
- $\mathbb{Z}/n$ représente le groupe quotient (ou l'anneau quotient selon le contexte) de $\mathbb{Z}$ par le sous-groupe (ou l'idéal) engendré par n. Lorsque $n = p$ est un naturel premier, $\mathbb{Z}/p$ est un corps que nous noterons $\mathbb{F}_p$.
- $(\mathbb{Z}/n)^\times$ est le groupe multiplicatif des éléments inversibles de l'anneau $\mathbb{Z}/n$.
- S_n est le groupe des permutations sur $\{1, \ldots, n\}$.

Soient $K \subset E \subset F$ trois corps et $H \subset G$ deux sous-groupes de $\mathrm{Aut}_K F$.

- $\mathrm{Aut}_K F$ est le groupe des K-automorphismes de F.
- $K^\times = K \setminus \{0\}$ est le groupe multiplicatif de K.
- $[F : K]$ est la dimenision de F considéré comme espace vectoriel sur K.

- $[G : H]$ est l'indice de H dans G.
- $E' = \{\sigma \in \mathrm{Aut}_K F \mid \sigma(u) = u \quad \forall u \in E\}$ est le plus grand sous-groupe de $\mathrm{Aut}_K F$ dont les éléments fixent les éléments de E.
- $H' = \{u \in F \mid \sigma(u) = u \quad \forall \sigma \in H\}$ est un sous-corps de F contenant K, appelé le fixateur de H dans F. C'est le plus grand sous-corps de F contenant K dont éléments sont fixés par les éléments de H.
- E est dit fermé si $E'' = E$.
- H est dit fermé si $H'' = H$.
- E est dit stable (relativement à K et F) si pour tout $\sigma \in \mathrm{Aut}_K F$ et $u \in E$, $\sigma(u) \in E$.

Chapter 5

Corps et Théorie de Galois

1. Extensions de corps

Exercice 1.(a) Soit F une extension de K et $\alpha \in F$. Si $[F : K] = 1$ alors $\{1_F\}$ est une base de F sur K. Dès lors, il existe $\beta \in K$ tel que $\alpha = \beta 1_F$. Puisque $1_F = 1_K$, $\alpha = \beta 1_F = \beta 1_K = \beta \in K$ et donc $F \subset K$.
(b) Supposons que $F \supset H \supset K$. Alors $[F : K] = [F : H][H : K]$. Comme $[F : K]$ est premier, $[F : H] = 1$ ou $[H : K] = 1$. Du point (a), nous déduisons $F = H$ ou $H = K$.
(c) D'après la formule des corps emboités, $[F : K] = [F : K(u)][K(u) : K]$. Puisque $[K(u) : K] = n$, n divise $[F : K]$.

Exercice 2. Puisque π est transcendant sur $\mathbb{Q}$, $\mathbb{Q}(\pi)$ est une extension de type fini qui n'est pas finie dimensionelle sur $\mathbb{Q}$.

Exercice 7. Soit

$$p(x) = \sum_{i=0}^{n-1} (p_i(u)/q_i(u))x^i + x^n \in K(u)[x]$$

un polynôme non nul tel que $p_i(x), q_i(x) \in K[x]$ et $p(v) = 0$. Si $p_i(x) = 0$, on pose $q_i(x) = 1$. Posons

$$p(x, y) = \sum_{i=0}^{n-1} (p_i(y)/q_i(y))x^i + x^n \quad \text{et} \quad p_i'(y) = (p_i(y)/q_i(y))q_0(y) \cdots q_{n-1}(y).$$

Alors

$$p'(y) := p(v,y)q_0(y)\cdots q_{n-1}(y) = \sum_{i=0}^{n-1} p_i^{'}(y)v^i + q_0(y)\cdots q_{n-1}(y)$$

appartient à $K[v][y]$ et $p'(u) = 0$. Si $p'(y) = 0$ alors $p(v,y) = 0$ puisque $\forall i\ q_i(y) \neq 0$. En particulier $p(v,1) = 0$, ce qui est absurde puisque v est transcendant sur K. Par conséquent $p'(y) \neq 0$ et donc, u est algébrique sur $K(v)$.

Exercice 8. Remarquons que u est une racine de $x^2 - u^2 \in K(u^2)$. Par conséquent, $[K(u) : K(u^2)] \leq 2$. Si $[K(u) : K(u^2)] = 2$ alors

$$[K(u) : K] = [K(u) : K(u^2)][K(u^2) : K]$$

serait pair. Donc $[K(u) : K(u^2)] = 1$.

Exercice 9. Notons que u^m est une racine du polynôme $x^{n/m} - a$. Si

$$x^{n/m} - a = g(x)h(x)$$

alors

$$x^n - a = (x^m)^{n/m} - a = g(x^m)h(x^m).$$

Or $x^n - a$ est irréductible. Par conséquent, $g(x^m) \in K$ or $h(x^m) \in K$. Ceci montre que $x^{n/m} - a$ est irréductible. Le polynôme minimal de u^m est donc $x^{n/m} - a$, c'est-à-dire u^m est de degré n/m sur K.

Exercice 10. Il suffit de montrer que si $d \in D$ est non nul alors $d^{-1} \in D$. Par hypothèse, d est algébrique sur K. Donc, $d^{-1} \in K(d) = K[d]$. Mais, puisque $K[d] \subset D$, nous obtenons $d^{-1} \in D$.

Exercice 11. (a) Il suffit de prendre $\mathbb{Q}(\pi, \sqrt{2}\pi)$.
(b) Soient F une extension de K et $u_1, \ldots, u_n \in K$. Si u_1 est transcendant sur K et si pour $i \in \{2, \ldots, n\}$, u_i est transcendant sur $K(u_1, \ldots, u_{i-1})$ alors il existe un K-isomorphisme de corps $K(u_1, \ldots, u_n) \cong K(x_1, \ldots, x_n)$ où $x_1, \ldots, x_n$ sont des indéterminés. La preuve est laissée au lecteur.

Exercice 12. Le polynôme minimal de $\sqrt{d}$ sur $\mathbb{Q}$ est $x^2 - d$. Du Théorème 1.6, on déduit que $\mathbb{Q}(\sqrt{d})$ est un espace vectoriel de dimension 2 dont une base est donnée par $\{1, \sqrt{d}\}$.

Exercice 13. (a) Le polynôme est irréductible par le critère de Eisenstein. En utilisant le fait que $u^3 = 6u^2 - 9u - 3$, on obtient $u^4 = uu^3 = 27u^2 - 57u - 18$.

On procède de la même manière pour u^5 et on obtient $u^5 = 125u^2 - 297u - 81$.

Sachant les expressions de u^4 et u^5 dans la base $\{1, u, u^2\}$, on calcule celui de $3u^5 - u^4 + 2$.

En effectuant le division euclidienne, on obtient

$$x^3 - 6x^2 + 9x + 3 = (x + 1)(x^2 - 7x + 16) - 13.$$

En remplaçant x par u, on a $(u + 1)^{-1} = u^2/13 - 7u/13 + 16/13$.

La division euclidienne montre que

$$x^3 - 6x^2 + 9x + 3 = x(x^2 - 6x + 8) + x + 3$$

et

$$x^2 - 6x + 8 = (x - 9)(x + 3) + 35.$$

En remplaçant x par u, on a

$$0 = u(u^2 - 6u + 8) + u + 3$$

et

$$u^2 - 6u + 8 = (u - 9)(u + 3) + 35.$$

De $35 = u^2 - 6u + 8 - (u - 9)u(u^2 - 6u + 8)$, on conclut alors que

$$(u^2 - 6u + 8)^{-1} = (1 - (u - 9)u)/35 = -u^2/35 + 9u/35 + 1/35.$$

Exercice 14. (a) Appliquons la formule des corps emboités à $\mathbb{Q}(\sqrt{2}, \sqrt{3}) \supset \mathbb{Q}(\sqrt{2}) \supset \mathbb{Q}$:

$$[\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}] = [\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}(\sqrt{2})][\mathbb{Q}(\sqrt{2}) : \mathbb{Q}].$$

Puisque $\sqrt{3}$ est une racine de $x^2 - 3$, $[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2$ et $[\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}(\sqrt{2})] \leq 2$. Si $[\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}(\sqrt{2})] = 1$, alors $\sqrt{3} \in \mathbb{Q}(\sqrt{2})$, c'est-à-dire $\sqrt{3} = a + b\sqrt{2}$ avec $a, b \in \mathbb{Q}$. En élevant au carré, on obtient

$$a^2 + 2b^2 - 3 + 2ab\sqrt{2} = 0.$$

Puisque $\{1, \sqrt{2}\}$ est une base de $\mathbb{Q}(\sqrt{2})$ sur $\mathbb{Q}$ (Théorème 1.6.), on a

$$\begin{cases} a^2 + 2b^2 - 3 &= 0 \\ 2ab &= 0 \end{cases}$$

Si $b = 0$ alors $\sqrt{3} \in \mathbb{Q}$. Si $a = 0$, $3 = 2b^2$. Dans les deux cas nous obtenons une contradiction. Par conséquent $[\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}(\sqrt{2})] = 2$ et donc,

$$[\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}] = 4.$$

Une base est alors donnée par $\{1, \sqrt{2}, \sqrt{3}, \sqrt{6}\}$.

Exercice 15. Puisque $K(x) = K(u)(x)$, $K(x)$ est une extension simple de $K(u)$. D'autre part, x est une racine de $u(y + 1) - y^3$. Montrons que ce polynôme est irréductible dans $K(u)[y]$. D'après le Théorème III.6.13, il suffit de montrer qu'il est irréductible dans $K[u][y]$ puisque u est transcendant sur K. On montre en comparant le degré en y que ce polynôme n'a pas de racine dans $K[u]$. Il est donc irréductible puisqu'il est de degré trois. Par conséquent, $[K(x) : K(u)] = 3$.

Exercice 16. D'après le Théorème 1.6, $\mathbb{Q}(i)$ et $\mathbb{Q}(\sqrt{2})$ sont des extensions de degré deux sur $\mathbb{Q}$ et $\{1, i\}$ et $\{1, \sqrt{2}\}$ en sont des bases respectives. On définit alors un isomorphisme de $\mathbb{Q}$-espace vectoriel en envoyant $1 \mapsto 1$ et $i \mapsto \sqrt{2}$.
Si σ est un isomorphisme de corps entre $\mathbb{Q}(i)$ et $\mathbb{Q}(\sqrt{2})$, $-1 = \sigma(i^2) = (\sigma(i))^2$ serait un carré dans $\mathbb{Q}(\sqrt{2})$. Il n'existe donc pas d'isomorphisme de corps entre $\mathbb{Q}(i)$ et $\mathbb{Q}(\sqrt{2})$.

Exercice 17. Le polynôme $p(x) = x^2 + x + 1$ est irréductible dans $\mathbb{F}_2[x]$ puisqu'il n'a pas de racine dans $\mathbb{F}_2$. Par le Théorème 1.6, $\mathbb{F}_2(u) \cong \mathbb{F}_2[x]/(p(x))$ est une extension de degré 2 dont une base est $\{1, u\}$. Donc $\mathbb{F}_2(u) = \{a + bu \mid a, b \in \mathbb{F}_2\}$ est d'ordre 4.
Plus généralement, pour construire un corps d'ordre p^n, il suffit de quotienter $\mathbb{F}_p[x]$ par un idéal engendré par un polynôme irréductible de degré n et appliquer le Théorème 1.6.

Exercice 18. (a) Soit $\sum_{i=0}^{n-1}(a_i/b_i)x^i + x^n$ le polynôme minimal de u dans $\mathbb{Q}[x]$. Alors en multipliant par $b_0 \cdots b_{n-1}$, on montre que $b_0 \cdots b_{n-1}u$ est une racine de $\sum_{i=0}^{n-1}(a_i/b_i)(b_0 \cdots b_{n-1})^{n-i}x^i + x^n \in \mathbb{Z}[x]$.
(b) C'est une conséquence de la Proposition III.6.8.

(c) Si u est une racine de $\sum_{i=0}^{m-1} a_i x^i + x^m \in \mathbb{Z}[x]$ alors nu est une racine de $\sum_{i=0}^{m-1} a_i n^{m-i} x^i + x^m \in \mathbb{Z}[x]$.
Cherchons $b_0, \ldots, b_{m-1} \in \mathbb{Z}$ tels que

$$\sum_{i=0}^{m-1} a_i u^i + u^m = \sum_{i=0}^{m-1} b_i (u+n)^i + (u+n)^m.$$

En comparant les termes en u^i, on obtient le système suivant:

$$\begin{cases} a_0 &= b_0 + b_1 n + b_2 n^2 + \cdots + b_{m-1} n^{m-1} + n^m \\ &\vdots \\ a_i &= b_i + \binom{i+1}{1} b_{i+1} n + \cdots + \binom{m-1}{m-(i+1)} b_{m-1} n^{m-(i+1)} + \binom{m}{m-i} n^{m-i} \\ &\vdots \\ a_{m-2} &= b_{m-2} + \binom{m-1}{1} b_{m-1} n + \binom{m}{2} n^2 \\ a_{m-1} &= b_{m-1} + \binom{m}{1} n. \end{cases}$$

Puisque $a_{m-1}, n \in \mathbb{Z}$, $b_{m-1} \in \mathbb{Z}$. En continuant de la sorte, on trouve $b_0, \ldots, b_{m-1} \in \mathbb{Z}$ satisfaisant le système. Donc, $u+n$ est une racine d'un polynôme à coefficients entiers qui est $\sum_{i=0}^{m-1} b_i x^i + x^m$.

Exercice 19. Puisque u est de degré m sur K et $K \subset K(v)$, u est de degré au plus m sur $K(v)$. Donc

$$[K(u,v) : K] = [K(u,v) : K(v)][K(v) : K] \leq mn.$$

Cette dernière égalité montre que $n = [K(v) : K]$ divise $[K(u,v) : K]$. En appliquant la formule des corps emboités à la chaîne $K \subset K(u) \subset K(u,v)$, on obtient que m aussi divise $[K(u,v) : K]$. Par conséquent, mn divise $[K(u,v) : K]$ lorsque m et n sont premiers entre eux. On a alors $mn \leq [K(u,v) : K] \leq mn$.

Exercice 20. (a) Considérons les chaînes $K \subset L, M \subset LM$. Alors

$$[LM : K] = [LM : M][M : K] = [LM : L][L : K].$$

Donc, si $[LM : K]$ est fini alors $[M : K]$ et $[L : K]$ sont finis. Réciproquement, il suffit de montrer que

$$D = \{\ell_1 m_1 + \cdots + \ell_n m_n \mid \ell_i \in L, m_i \in M \quad \text{pour} \quad i = 1, \ldots n\} = LM.$$

En effet si $\{e_1, \ldots, e_s\}$ et $\{u_1, \ldots, u_r\}$ sont des bases respectives de L et M sur K, alors $\{e_i u_j \mid i = 1, \ldots s \quad \text{et} \quad j = 1, \ldots, r\}$ est une partie génératrice de LM sur K et donc, $[LM : K] < \infty$.

On vérifie que $D \subset LM$. Montrons que $LM \subset D$. Notons que $K \subset D$ car $L, M \subset D$ et que D est un anneau intègre. Puisque F est algébrique sur K, l'exercice 10 entraîne que D est un corps. Or, LM est le plus petit corps contenant L et M. Par conséquent, $LM \subset D$.

(b) Notons que $[LM : K]$ est divisible par $[L : K]$ et $[M : K]$ puisque $[LM : K] = [LM : L][L : K] = [LM : M][M : K]$.

Montrons par induction sur $[LM : K]$ que $[LM : K] \leq [L : K][M : K]$. Il n'y a rien à prouver lorsque $[LM : K] = 1$ et lorsque $L = M$. Soient $L = K(a_1, \ldots, a_s)$ et $K(a_1, \ldots, a_j) \in L$ tels que $j < s$ et $K(a_1, \ldots, a_j)M \subsetneq LM$. Notons alors que $[K(a_1, \ldots, a_j)M : K] < [LM : K]$, $LM = K(a_1, \ldots, a_s)M = M(a_1, \ldots, a_s)$ et $K(a_1, \ldots, a_j)M = M(a_1, \ldots, a_j)$. Comme

$$[M(a_1, \ldots, a_s) : M(a_1, \ldots, a_j)] \leq [K(a_1, \ldots, a_s) : K(a_1, \ldots, a_j)],$$

nous avons par hypothèse d'induction

$$\begin{aligned}
[LM : K] &= [K(a_1, \ldots, a_s)M : K(a_1, \ldots, a_j)M][K(a_1, \ldots, a_j)M : K] \\
&= [M(a_1, \ldots, a_s) : M(a_1, \ldots, a_j)][K(a_1, \ldots, a_j)M : K] \\
&\leq [K(a_1, \ldots, a_s) : K(a_1, \ldots, a_j)][K(a_1, \ldots, a_j) : K][M : K] \\
&\leq [K(a_1, \ldots, a_s) : K][M : K] \\
&\leq [L : K][M : K].
\end{aligned}$$

(c) Par (a), $[LM : K]$ est fini et d'après (b), $[L : K]$ et $[M : K]$ divisent $[LM : K] \leq [L : K][M : K]$. Puisque $[L : K]$ et $[M : K]$ sont premiers entre eux, $[L : K][M : K]$ divise $[LM : K]$. Finalement, nous obtenons

$$[L : K][M : K] \leq [LM : K] \leq [L : K][M : K].$$

(d) On vérifie (exercice) que les éléments de LM sont de la forme

$$\frac{\ell_1 m_1 + \cdots + \ell_r m_r}{\ell_1' m_1' + \cdots + \ell_s' m_s'}$$

où $\ell_1' m_1' + \cdots + \ell_s' m_s' \neq 0$, $i, j \in \mathbb{Z} \setminus \{0\}$ et $\ell_i, \ell_j' \in L$, $m_i, m_j' \in M$ pour $i = 1, \ldots, r$ et $j = 1, \ldots, s$. Soit α un tel élément. Montrons que α est algébrique sur K. Soient

$$L' = K(\ell_1, \ldots, \ell_r, \ell_1', \ldots, \ell_s') \text{ et } M' = K(m_1, \ldots, m_r, m_1', \ldots, m_s').$$

Notons que $L' \subset L$ et $M' \subset M$ sont des extensions finies de K. Du point (b), nous déduisons alors que $L'M'$ est une extension finie de K et donc algébrique. Ce qui termine la preuve puisque

$$\frac{\ell_1 m_1 + \cdots + \ell_r m_r}{\ell_1' m_1' + \cdots + \ell_s' m_s'} \in L'M'.$$

Exercice 21. (a) Supposons que $K \subsetneq L \cap M$ et soit $\alpha \in (L \cap M) \setminus K$. Donc $K(\alpha) \subset L, M$. Par hypothèse et le point (b) de l'exercice 20, nous obtenons alors la contradiction suivante

$$\begin{aligned} [L:K][M:K] &= [LM:K] \\ &= [LM:K(\alpha)][K(\alpha):K] \\ &\leq [L:K(\alpha)][M:K(\alpha)][K(\alpha):K] \\ &\leq [L:K(\alpha)][M:K] \\ &< [L:K][M:K]. \end{aligned}$$

(b) Supposons que $[L:K] = 2$ et considérons la chaîne $K \subset M \subset LM$. Nous avons

$$[LM:K] = [LM:M][M:K].$$

Il suffit de montrer que $[LM:M] = [L:K]$, c'est-à-dire $[LM:M] = 2$. Notons que $[LM:M] \leq 2$ puisque $[LM:M] \leq [L:K]$. Si $[LM:M] = 1$, $LM = M$ et donc, $K \subsetneq L = M \cap L$, ce qui est une contradiction.
(c) Soient $L = \mathbb{Q}(\sqrt[3]{2})$ et $M = \mathbb{Q}(\sqrt[3]{2}\omega)$ où $\omega = e^{i2\pi/3}$. Puisque $\sqrt[3]{2}$ et $\sqrt[3]{2}\omega$ sont racines du polynôme irréductible $x^3 - 2$, $[L:K] = [M:K] = 3$. D'autre part, $[\mathbb{Q}(\sqrt[3]{2}, \omega) : \mathbb{Q}(\sqrt[3]{2})] \leq 2$ car ω est racine de $x^2 + x + 1$. Par conséquent,

$$[LM:K] = [\mathbb{Q}(\sqrt[3]{2}, \omega) : \mathbb{Q}(\sqrt[3]{2})][\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] \leq 6 < [L:K][M:K] = 9.$$

2. Le Théorème Fondamental

Exercice 1. (a) Puisque $\operatorname{Ker}\sigma$ est in idéal de F, $\operatorname{Ker}\sigma = \{0\}$ ou $\operatorname{Ker}\sigma = F$. Donc σ est injective ou $\sigma = 0$. Si $\sigma \neq 0$ alors il existe $a \in F$ tel que $\sigma(a) \neq 0$. Nous avons $\sigma(a) = \sigma(a.1) = \sigma(a)\sigma(1)$. Comme F est un anneau intègre et $\sigma(a) \neq 0$, $\sigma(1) = 1$.

(b) Exercice.

(c) On a $\mathrm{Aut}_K F \subset \mathrm{Aut}\, F$ et $\mathrm{id} \in \mathrm{Aut}_K F$. Si $\sigma, \mu \in \mathrm{Aut}_K F$, $\sigma\mu^{-1} \in \mathrm{Aut}K$ puisque $\mathrm{Aut}K$ est un groupe. Il suffit donc de montrer que $\sigma\mu^{-1}$ est K-linéaire, ce qui est laissé en exercice.

Exercice 2. Montrons d'abord que les automorphismes de $\mathbb{R}$ préservent l'ordre dans $\mathbb{R}$. Soient $\sigma \in \mathrm{Aut}_{\mathbb{Q}}\mathbb{R}$, et $a \geq 0$. Alors

$$\sigma(a) = \sigma(\sqrt{a}\sqrt{a}) = (\sqrt{a})^2 \geq 0.$$

Si $a < b$, alors $b - a \geq 0$ entraîne que $\sigma(b - a) \geq 0$. et donc, $\sigma(a) \leq \sigma(b)$. Supposons qu'il existe un nombre réel a tel que $\sigma(a) \neq a$. Sans perte de généralité, nous supposons $\sigma(a) < a$. Comme $\mathbb{Q}$ est dense dans $\mathbb{R}$, il existe un $q \in \mathbb{Q}$ tel que $\sigma(a) < q < a$. Puisque $q < a$, $\sigma(q) < \sigma(a)$ et donc, $\sigma(a) < q = \sigma(q) < \sigma(a)$, une contradiction.

Exercice 3. Rappelons que $\sigma \in \mathrm{Aut}_{\mathbb{Q}}\mathbb{Q}(\sqrt{d})$ est complètement déterminé par son action sur $\sqrt{d}$ (Théorème 1.6). Si d est un carré dans $\mathbb{Q}$, alors $\mathbb{Q}(\sqrt{d}) = \mathbb{Q}$ et donc, $\mathrm{Aut}_{\mathbb{Q}}\mathbb{Q}(\sqrt{d}) = \mathrm{Aut}_{\mathbb{Q}}\mathbb{Q} = \{id\}$. Si d n'est pas un carré dans $\mathbb{Q}$, le polynôme minimal de d sur $\mathbb{Q}$ est $x^2 - d$. Par le Théorème 2.2, $\sigma(\sqrt{d}) = \pm\sqrt{d}$ entraîne que $\mathrm{Aut}_{\mathbb{Q}}\mathbb{Q}(\sqrt{d}) \cong \mathbb{Z}/2$.

Exercice 4. Si $\sigma \in G = \mathrm{Aut}_{\mathbb{Q}}\mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5})$ alors $\sigma(\sqrt{2}) = \pm\sqrt{2}$, $\sigma(\sqrt{3}) = \pm\sqrt{3}$ et $\sigma(\sqrt{5}) = \pm\sqrt{5}$; il y a donc 8 possibilités de définir σ et donc, G est un groupe d'ordre 8. Décrivons les éléments de G. Notons σ, δ et γ les automorphismes de G tels que

$$\begin{array}{rcl} \sigma(\sqrt{2}) & = & -\sqrt{2} \quad \text{et} \quad \sigma \quad \text{fixe} \quad \mathbb{Q}(\sqrt{3}, \sqrt{5}) \\ \delta(\sqrt{3}) & = & -\sqrt{3} \quad \text{et} \quad \delta \quad \text{fixe} \quad \mathbb{Q}(\sqrt{2}, \sqrt{5}) \\ \gamma(\sqrt{5}) & = & -\sqrt{5} \quad \text{et} \quad \gamma \quad \text{fixe} \quad \mathbb{Q}(\sqrt{2}, \sqrt{3}). \end{array}$$

On montre alors que $G = \langle \sigma, \delta, \gamma \rangle$. Tout élément de G est d'ordre 2 et donc, G est commutatif (exercice I 1.13). Finalement, nous avons $G \cong \mathbb{Z}/2 \times \mathbb{Z}/2 \times \mathbb{Z}/2$.

Remarque:

Ce raisonnement est incorrecte lorsque le corps est $\mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{6})$. En effet, puisque $\sqrt{6} = \sqrt{2}\sqrt{3}$, $\sigma(\sqrt{6}) = \sigma(\sqrt{2})\sigma(\sqrt{3})$ et donc, l'image de $\sqrt{6}$ est complètement déterminé par $\sigma(\sqrt{2})$ et $\sigma(\sqrt{3})$. On vérifie que $\mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{6}) = \mathbb{Q}(\sqrt{2}, \sqrt{3})$ et $\mathrm{Aut}_{\mathbb{Q}}\mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{6}) \cong \mathbb{Z}/2 \times \mathbb{Z}/2$.

Exercice 5. (a) D'après l'exercice 3, soit $\mathbb{Q}(\sqrt{d}) = \mathbb{Q}$ et $\mathrm{Aut}_{\mathbb{Q}}\mathbb{Q}(\sqrt{d}) = \{id\}$ (et donc, $\mathbb{Q}(\sqrt{d})$ est une extension galoisienne de $\mathbb{Q}$) soit $\mathrm{Aut}_{\mathbb{Q}}\mathbb{Q}(\sqrt{d}) = \{id, \sigma\}$ où $\sigma(\sqrt{d}) = -\sqrt{d}$. Si $\alpha \in \mathbb{Q}(\sqrt{d}) \setminus \mathbb{Q}$, $\alpha = a + b\sqrt{d}$ avec $a, b \in \mathbb{Q}$ et $b \neq 0$. Par conséquent, $\sigma(\alpha) \neq \alpha$ et donc, $\mathbb{Q}(\sqrt{d})' = \mathbb{Q}$.
(b) Sachant que la conjuguaison σ dans $\mathbb{C}$ est dans $\mathrm{Aut}_{\mathbb{R}}\mathbb{C}$, $\alpha \in \mathbb{C} \setminus \mathbb{R}$ implique que $\sigma(\alpha) \neq \alpha$. Donc, $\mathbb{C}$ est une extension galoisienne de $\mathbb{R}$.

Exercice 6. Soit $\phi(y) = \frac{f(x)}{g(x)}g(y) - f(y) \in K(\frac{f(x)}{g(x)})[y]$. Comme $\phi(y) \neq 0$ et $\phi(x) = \frac{f(x)}{g(x)}g(x) - f(x) = 0$, x est algébrique sur $K(\frac{f(x)}{g(x)})$. Le degré en y de $\phi(y)$ est $\max(\deg_y f, \deg_y g)$ puisque $\frac{f(x)}{g(x)} \notin K$. Montrons que $\frac{f(x)}{g(x)}$ est transcendant sur K. Supposons qu'il existe des rationels non tous nuls $a_0, \ldots, a_{n-1}$ tels que

$$(f(x)/g(x))^n + a_{n-1}\,(f(x)/g(x))^{n-1} + \cdots a_0 = 0.$$

En multipliant par $g(x)^n$, nous obtenons une équation polynômiale

$$f(x)^n + a_{n-1}f(x)^{n-1}g(x) + \cdots a_0 g(x)^n = 0$$

qui est non triviale puisque $f(x)$ et $g(x)$ sont premiers entre eux. Ceci est impossible car x est transcendant sur K. Dès lors, le Théorème 1.8 montre que $K(\frac{f(x)}{g(x)}) \cong K(z)$ où z est une indéterminée sur K. Sans perte de généralité nous posons $z = \frac{f(x)}{g(x)}$.
A présent, montrons que $\phi(y) = zg(y) - f(y)$ est irréductible dans $K(z)[y]$. Etant donné que f et g sont premiers entre eux, les diviseurs communs des coefficients de ϕ sont les éléments non nuls de K et[1] donc ϕ est primitif. Par le Lemme III 6.13, il suffit alors de montrer que ϕ est irréductible dans $K[z][y] = K[z, y]$. Soit $\phi(y) = p(y)q(y)$. Nous pouvons supposer que $\deg_z p = 1$ et $\deg_z q = 0$ puisque ϕ est de degré 1 en z. Alors $q(y) \in K[y]$ et $q(y)$ divise ϕ et donc, il divise f et g. Or f et g sont premiers entre eux, ce qui montre que $q(y) \in K$. Donc ϕ est irréductible. Nous avons alors

$$[K(x) : K(f(x)/g(x))] = \max(\deg f, \deg g).$$

(b) Si $K \subsetneq E$ alors il existe un élément $\frac{f(x)}{g(x)} \in E \setminus K$. Considérons la chaîne $K(\frac{f(x)}{g(x)}) \subset E \subset K(x)$. Puisque

$$[K(x) : K(f(x)/g(x))] = [K(x) : E][E : K(f(x)/g(x))]$$

[1] c'est-à-dire les inversibles dans $K[z]$.

est fini par (a), $[K(x) : E]$ l'est aussi.
(c) D'après l'exercice 1(a), σ est toujours injective. Donc, σ est un K-automorphisme si et seulement si σ est surjective. Il est clair que $\operatorname{Im}\sigma = K(\frac{f(x)}{g(x)}) \subset K(x)$. D'après (a), nous avons alors

$1 = \max(\deg f, \deg g) \Leftrightarrow K(x) = K(f(x)/g(x)) \Leftrightarrow \sigma$ est un $K-$automorphisme.

(d) Soit $\sigma \in \operatorname{Aut}_K K(x)$ et $\sigma(x) = \frac{f(x)}{g(x)}$. Le point précédent montre que $f = ax + b, g = cx + d$ avec $a \neq 0$ ou $c \neq 0$ et f, g premiers entre eux. Mais $ad = bc \Leftrightarrow df(x) = bg(x) \Leftrightarrow \frac{f(x)}{g(x)} \in K \Leftrightarrow f$ et g ne sont pas premiers entre eux. Ce qui termine la preuve.

Exercice 7. Notons σ le $\mathbb{Q}$-automorphisme $x \mapsto 1/(1-x)$. Alors σ^2 est le $\mathbb{Q}$-automorphisme $x \mapsto (x-1)/x$ et $\sigma^3 = \mathrm{id}$. Donc $G = \{id, \sigma, \sigma^2\}$ est le sous-groupe de $\operatorname{Aut}_K K(x)$ engendré par σ. Dans la preuve du Théorème d'Artin (2.15), il apparait que $[K(x) : G'] = |G| = 3$. Alors, si $\frac{f(x)}{g(x)} \in G' \setminus K$ et f, g sont premiers entre eux, l'égalité

$$\begin{aligned} \max(\deg f, \deg g) &= [K(x) : K\,(f(x)/g(x))] \\ &= [K(x) : G'][G' : K\,(f(x)/g(x))] \end{aligned}$$

implique que $G' = K(\frac{f(x)}{g(x)})$ si $\max(\deg f, \deg g) = 3$. Cherchons alors deux polynômes f, g premiers entre eux tels que $\deg f(x) = \deg g(x) = 3$ et $\sigma(\frac{f(x)}{g(x)}) = \frac{f(x)}{g(x)}$. Soit $f(x) = x^3 + ax^2 + bx + c$. Remarquons que

$$\begin{aligned} \sigma(f(x)) &= (\frac{1}{1-x})^3 + a(\frac{1}{1-x})^2 + b\frac{1}{1-x} + c \\ &= \frac{1 + a(1-x) + b(1-x)^2 + c(1-x)^3}{(1-x)^3}, \end{aligned}$$

et donc,

$$(1-x)^3\sigma(f(x)) = 1 + a + b + c - (a + 2b + 3c)x + (b + 3c)x^2 - cx^3.$$

Notons alors que si $f(x), g(x)$ sont tels que

$$(1-x)^3\sigma(f(x)) = -f(x) \quad \text{et} \quad (1-x)^3\sigma(g(x)) = -g(x)$$

alors[2]

$$\sigma(f(x)/g(x)) = \frac{\sigma(f(x))}{\sigma(g(x))} = \frac{-f(x)}{-g(x)} = \frac{f(x)}{g(x)}.$$

[2] l'égalité $(1-x)^3\sigma(f(x)) = f(x)$ mène à un système impossible.

Cherchons a, b, c tels que $-f(x) = -(x^3 + ax^2 + bx + c) = 1 + a + b + c - (a + 2b + 3c)x + (b + 3c)x^2 - cx^3$. On déduit de cette égalité que $c = 1$ et $a + b = 3$. Il suffit alors de donner des valeurs à a et b afin que f et g soient premiers entre eux. Prenons par exemple $f(x) = x^3 - 3x^2 + 1$ $(a = -3, b = 0)$ et $g(x) = x^3 - 2x^2 - x + 1$ $(a = -2, b = -1)$ et montrons que $f(x)$ et $g(x)$ sont premiers entre eux. Il suffit de montrer que f et g n'ont pas de racine commune. Rappelons que les racines communes sont aussi racines du reste de la division euclidienne de $f(x)$ par $g(x)$ qui est $x(-5x + 1)$. Si $\operatorname{car} K \neq 5$, les racines de $x(-5x+1)$ sont 0 et 5^{-1} qui ne sont pas racines de $f(x)$ et $g(x)$. Si $\operatorname{car} K = 5$, f et g sont aussi premiers entre eux puisque 0 est la seule racine de $x(-5x + 1) = x$ et 0 n'est pas une racine de f et g. On a donc

$$G' = K(\frac{x^3 - 3x^2 + 1}{x^3 - 2x^2 - x + 1}).$$

Exercice 8. Notons σ l'automorphisme donné. On montre par induction sur n que $\sigma^n(x) = x+n$. Comme $\operatorname{car} K = 0$, $\forall i \in \mathbb{N} \setminus \{0\}$ $\sigma^n \neq \mathrm{id}$ et donc, G est un groupe cyclique infini. Si $K \subset G'$, $[K(x) : G']$ est fini d'après l'exercice 6(b). Le Lemme 2.8 entraîne alors $|G''| = |\mathrm{Aut}_{G'}K(x)| \leq [K(x) : G']$ est fini; ce qui est absurde puisque $G \subset G''$ par le Lemme 2.6. Par conséquent, $G' = K$.

Exercice 9. (a) Si $K(x)$ n'est pas Galois sur K, alors $(\mathrm{Aut}_K K(x))' \supsetneq K$ et donc, par l'exercice 6(b), $[K(x) : (\mathrm{Aut}_K K(x))'] < \infty$. Le Lemme 2.8 montre alors que

$$|\mathrm{Aut}_{(\mathrm{Aut}_K K(x))'}K(x)| < \infty.$$

Or, $\mathrm{Aut}_{(\mathrm{Aut}_K K(x))'}K(x) = \mathrm{Aut}_K K(x)$ est infini d'après l'exercice 6(d) puisque K est infini.

(b) Si K est fini alors l'exercice 6(d) montre que $\mathrm{Aut}_K K(x)$ est fini. Si $K(x)$ est Galois sur K, le Théorème d'Artin (2.15) implique alors que $K(x)$ est une extension finie de K, ce qui est absurde.

Exercice 10. Puisque K est infini, l'exercice précédent entraîne que $K(x)$ est galois sur K et donc, $\mathrm{Aut}_K K(x)$ est fermé. Soient H un sous-groupe propre fermé de $\mathrm{Aut}_K K(x)$ et H' le corps fermé correspondant. Montrons que $H' \supsetneq K$. Puisque $K(x)$ est Galois sur K, si $H' = K$ alors

$$\mathrm{Aut}_K K(x) = K' = H'' = H.$$

Ce qui est absurde puisque H est un sous groupe propre de $\mathrm{Aut}_K K(x)$ et donc, $H' \supsetneq K$. Alors, par 6(b), $[K(x) : H'] < \infty$. Le Lemme 2.8 implique alors que

$$|H| = [H : 1] = [H'' : 1] < [K(x) : H'] < \infty.$$

Tout sous-groupe propre fermé de $\mathrm{Aut}_K K(x)$ est donc fini.
Montrons à présent que tout sous-groupe fini H de $\mathrm{Aut}_K K(x)$ est fermé. Nous savons par le Théorème d'Artin (2.15) que $\mathrm{Aut}_{H'} K(x) = H$, et puisque $(H')' = \mathrm{Aut}_{H'} K(x)$, nous obtenons

$$H'' = \mathrm{Aut}_{H'} K(x) = H.$$

Exercice 11. Notons que x est une racine du polynôme irréductible $y^2 - x^2$ qui est irréductible dans $\mathbb{Q}(x^2)[y]$ (exercice). L'image de x par un $\mathbb{Q}(x^2)$-automorphisme de $\mathbb{Q}(x)$ ne peut être alors que $\pm x$. Par conséquent,

$$\mathbb{Q}(x^2)' = \{id, \sigma\}$$

où σ est l'automorphisme de $\mathbb{Q}(x)$ induit par la flèche $x \mapsto -x$. Puisque $\sigma(x) = -x \neq x$, $x \notin \mathbb{Q}(x^2)''$ implique que $\mathbb{Q}(x^2)'' \subsetneq \mathbb{Q}(x)$ et donc, $[\mathbb{Q}(x) : \mathbb{Q}(x^2)''] \neq 1$. Considérons la chaîne $\mathbb{Q}(x^2) \subset \mathbb{Q}(x^2)'' \subsetneq \mathbb{Q}(x)$. Alors

$$2 = [\mathbb{Q}(x) : \mathbb{Q}(x^2)] = [\mathbb{Q}(x) : \mathbb{Q}(x^2)''][\mathbb{Q}(x^2)'' : \mathbb{Q}(x^2)]$$

et donc, $\mathbb{Q}(x^2)'' = \mathbb{Q}(x^2)$.
Montrons que $\mathbb{Q}(x^3)$ n'est pas fermé. Remarquons que x^3 est une racine de $y^3 - x^3$ qui est irréductible dans $\mathbb{Q}(x^3)[y]$. Ce polynôme n'a qu'une racine dans $\mathbb{Q}(x)$: en effet, $y^3 - x^3 = (y - x)(y^2 + yx + x^2)$, si $f(x)/g(x)$ est une racine de $y^2 + yx + x^2$ alors pour $q \in \mathbb{Q} \setminus \{0\}$ tel que $f(q)/g(q) \neq 0$ nous avons

$$\begin{aligned} 0 &= (\frac{f(q)}{g(q)})^2 + \frac{f(q)}{g(q)} q + q^2 \\ &= (\frac{f(q)}{g(q)q})^2 + \frac{f(q)}{g(q)q} + 1. \end{aligned}$$

Il en découle que le polynôme $y^2 + y + 1 \in \mathbb{Q}[y]$ a une racine $\frac{f(q)}{g(q)q}$ dans $\mathbb{Q}$; ce qui est absurde puisque $y^2 + y + 1$ est irréductible dans $\mathbb{Q}[y]$. Par conséquent, $\mathbb{Q}(x^3)' = \{id\}$ et donc,

$$\mathbb{Q}(x^3)'' = \{id\}' = \mathbb{Q}(x) \neq \mathbb{Q}(x^3)$$

.

Exercice 12. Montrons que quelque soit $u \in F \setminus K$, il existe un K-automorphisme $\sigma \in \mathrm{Aut}_K F$ tel que $\sigma(u) \neq u$. Etant donné que F est une extension galoisienne de E, si $u \in F \setminus E$, il existe un E-automorphisme $\sigma \in \mathrm{Aut}_E F \subset \mathrm{Aut}_K F$ tel que $\sigma(u) \neq u$. De même, Si $u \in E \setminus K$, il existe $\tilde{\sigma} \in \mathrm{Aut}_K E$ tel que $\tilde{\sigma}(u) \neq u$. Par hypothèse, il existe $\sigma \in \mathrm{Aut}_K F$ qui étend $\tilde{\sigma}$ et donc, $\sigma(u) \neq u$.

Exercice 13. Par 9.(a), $K(x)$ est une extension galoisienne de K. Soit σ le K automorphisme de $\mathrm{Aut}_K K(x, y)$ tel que $\sigma(x) = y$ et $\sigma(y) = x$. Il est clair alors que $K(x)$ n'est pas stable.

3. Corps de rupture, clôture algébrique et normale

Exercice 1. Le résultat est clair puisque l'ensemble des racines des polynômes $f_1, \ldots, f_n$ est exactement celui de $f_1 \cdots f_n$.

Exercice 2. Remarquons que $S \subset E[x]$ puisque $K \subset E$ et $S \subset K[x]$. Nous savons par hypothèse que si $f \in S$ alors f est scindé sur F. Il suffit donc de montrer que F est engendré sur E par toutes les racines des polynômes de S, notons U cet ensemble. Puisque $K \subset E \subset F$, $U \subset F$ et $F = K(U)$, $F = K(U) \subset E(U) \subset F$ et donc, $F = E(U)$.

Exercice 3. a) Le "seulement si" découle de l'exercice précédent. Supposons que F est un corps de rupture de f sur E et notons $u_1, \ldots, u_r, \ldots, u_n$ les racines de f dans F. Alors

$$\begin{aligned} F &= E(u_1, \ldots, u_r, \ldots, u_n) \\ &= K(u_1, \ldots, u_r)(u_1, \ldots, u_r, \ldots, u_n) \\ &= K(u_1, \ldots, u_r, \ldots, u_n). \end{aligned}$$

De plus, f étant scindé sur F, nous obtenons que F est un corps de rupture de f sur K.

(b) Soient $S \subset K[x]$, U' un ensemble de racine des polynômes de S, $E = K(U')$ et F un surcorps de E. Alors F est corps de rupture de S sur K si et seulement si F est un corps de rupture de S sur E.
Supposons que F est un corps de rupture de $S \subset K[x]$ sur E. Alors $F = E(U)$ où U est l'ensemble des racines des polynômes de S. Comme $U' \subset U$,

$$\begin{aligned} F &= E(U) \\ &= K(U')(U) \\ &= K(U). \end{aligned}$$

De plus, par hypothèse, si $f \in S$ alors f est scindé sur F et donc, F est un corps de rupture de S sur K. L'autre sens découle de l'exercice 2.

Exercice 4. Si $f \in T$ alors il existe $g \in S$ tel que f divise g. Puisque g est scindé sur F, f aussi est scindé sur F. On vérifie que l'ensemble U des racines des polyômes de S est égal à l'ensemble des racines des polynômes de T. Puisque $F = K(U)$, nous obtenons alors que F est un corps de rupture de T sur K.

Exercice 5. Nous procédons par induction sur $\deg f = n$. On vérifie lorsque $n = 1$. Supposons alors $n > 1$ et traitons d'abord le cas où f est irréductible. Soit $c \in F$ une racine de f. Alors $f = (x - c)g$ avec $g \in K(c)[x]$. De plus, F est un corps de rupture de g sur $K(c)$ et $\deg g = n - 1 < n$. L'hypothèse d'induction montre alors que $[F : K(c)] \mid (n-1)!$ et donc,

$$[F : K] = [F : K(c)][K(c) : K] \mid (n-1)!n = n!.$$

Supposons que $f = gh$ est réductible dans $K[x]$ et notons L le corps de rupture de h sur K. On montre que F est un corps de rupture de g sur L. Puisque $\deg h, \deg g < n$, par hypothèse d'induction, $[L : K] \mid \deg h!$ et $[F : L] \mid \deg g! = (n - \deg h)!$ et donc,

$$[F : K] = [F : L][L : K] \mid (n - \deg h)! \deg h! \mid n!$$

car $\binom{n}{\deg h} \in \mathbb{N}$.

Exercice 6. Soit $f \in K[x]$ et α une racine de f dans un corps de rupture de f sur K. Comme $K(\alpha)$ est une extension algébrique de K, $K(\alpha) = K$ par hypothèse et donc, $\alpha \in K$.

Exercice 7. Notons que E est un corps et E est algébrique sur K (Théorème 1.14). Montrons alors que E est algébriquement clos. Soient $f \in E[x]$ et α une racine de f. Puisque $E \subset F$ et que F est algébriquement clos, $\alpha \in F$. Comme α est algébrique sur E et E est algébrique sur K, α est algébrique sur K par le Théorème 1.13 et donc, $\alpha \in E$. Ce qui montre que E est algébriquement clos, et puisque E est une extension algébrique de K, E est une clôture algébrique de K.

Exercice 8. Si $K = \{a_0, \ldots, a_n\}$ est fini et $a_0 \neq 0$ alors

$$a_0 + (x - a_0) \cdots (x - a_n)$$

n'a pas de racine dans K et donc, K n'est pas algébriquement clos.

Exercice 9. Supposons que F est une clôture algébrique de K et soit F' une clôture algébrique de K contenant E. D'après le Théorème 3.4, F et F' sont des corps de rupture de l'ensemble de tous les polynômes dans $K[x]$. Il existe donc un K-isomorphisme $\delta : F' \to F$ par le Théorème 3.8 (il suffit de considérer $\mathrm{id} : K \to K$). Alors $\delta|_E$ est le K-monomorphisme desiré.
Réciproquement, soit F' une clôture algébrique de K. Par hypothèse, il existe un K-monomorphisme $\sigma : F' \to F$. Nous avons $\sigma(F') \subset F$. Montrons que $F \subset \sigma(F')$. Remarquons d'abord que $\sigma(F')$ est une clôture algébrique de K. Soient alors $a \in F$ et f son polynôme minimal dans $K[x]$. Comme $f \in \sigma(F')[x]$ et $\sigma(F')$ est algébriquement clos, $a \in \sigma(F')$.

Exercice 11. (a) Soient $f_1, \ldots, f_n$ les polynômes minimaux respectifs de $a_1, \ldots, a_n$ sur K et F un corps de rupture de $f_1, \ldots, f_n$ sur K contenant $K(a_1, \ldots, a_n)$. Puisque $a_1, \ldots, a_n$ sont séparables sur K, $f_1, \ldots, f_n$ sont aussi séparables. Alors, le Théorème 3.11 montre que F est séparable sur K et donc, $K(a_1, \ldots, a_n)$ aussi est séparable sur K.
(b) Soient S un ensemble d'éléments séparables sur K, $F = K(S)$ et $\alpha \in F$. Il existe $a_1, \ldots, a_n \in S$ tels que $\alpha \in K(a_1, \ldots, a_n)$. Le point précédent permet alors de conclure.

Exercice 12. (a) Notons f et g le polynôme minimal de u sur K et E respectivement. Comme f est séparable et g divise f car $K \subset E$, g est séparable et donc, u est séparable sur E.
(b) Si F est séparable sur K alors F est séparable sur E par (a) et E est séparable sur K puisque $E \subset F$.

Exercice 13. $(i) \Rightarrow (ii)$ Par hypothèse $[F : K] = n$ et donc, F est algébrique sur K. Le Théorème 3.11 montre alors que F est séparable sur K et un corps de rupture sur K d'un ensemble S de polynômes dans $K[x]$. De plus S est l'ensemble des polynômes minimaux sur K des éléments d'une base de F sur K. Si $\{e_1, \ldots, e_n\}$ est une base de F sur K et $f_1, \ldots, f_n$ sont les polynômes minimaux respectifs sur K alors $S = \{f_1, \ldots, f_n\}$. L'exercice 1 entraîne alors que F est un corps de rupture de $f = f_1 \cdots f_n$ sur K.

$(ii) \Rightarrow (iii)$ Considérons une décomposition de $f = f_1 \cdots f_n$ en polynômes irréductibles dans $K[x]$. Puisque F contient toutes les racines de f, les polynômes $f_1, \ldots, f_n$ sont des polynômes minimaux sur K de certaines racines de f et donc, ils sont séparables par hypothèse.

$(iii) \Rightarrow (i)$ Soient $f = f_1 \cdots f_n$ une décomposition de f en polynômes irréductibles dans $K[x]$ et $T = \{f_1, \ldots, f_n\}$. Puisque $f_1, \ldots, f_n$ sont séparables, le Théorème 3.11 montre que F est Galois sur K.

Exercice 17. Soient $u \in E$, f son polynôme minimal sur K et $\sigma \in \mathrm{Aut}_K F$. Puisque $\sigma(u)$ est aussi une racine de f (Théorème 2.2) et E contient toutes les racines de f (E est normal sur K), $\sigma(u) \in E$ et donc, E est stable.

Exercice 18. Supposons que E est stable. Soient $u \in E \backslash K$ et f son polynôme minimal sur K. Il faut montrer que E contient toutes les racines de f. Soit v une autre racine de f et montrons que $v \in E$. Notons que $v \in F$ puisque F est normal sur K. Par le Corollaire 1.9, il existe un K-isomorphisme $\tilde{\sigma}$ entre $K(u)$ et $K(v)$ tel que $\tilde{\sigma}(u) = v$. D'après le Théorème 3.14, F est un corps de rupture sur K d'un ensemble $S \subset K[x]$ et donc, on peut étendre $\tilde{\sigma}$ en un K-isomorphisme $\sigma \in \mathrm{Aut}_K F$ par le Théorème 3.8 (notons que $S = S'$ puisque $\tilde{\sigma}$ est un K-isomorphisme et $S \subset K[x]$). Comme E est stable et $u \in E$, $\sigma(u) = \tilde{\sigma}(u) = v \in E$.

La réciproque est donnée par l'exercice 17.

Le Lemme 2.14 montre que $\mathrm{Aut}_K F/E' = \mathrm{Aut}_K F/\mathrm{Aut}_E F$ est isomorphe au groupe des K-isomorphismes de E extensibles à F. Mais, par le Théorème 3.8, tout K-isomorphisme de E s'étend en un K-isomorphisme de F puisque F est un corps de rupture sur K et, donc sur E. Ce qui montre que $\mathrm{Aut}_K F/E' \cong \mathrm{Aut}_K E$.

Exercice 23. Soit $u \in F \setminus K$ et f son polynôme minimal sur K. Puisque $K \neq K(u) \subset F$ et $[F : K] = 2$, $\deg f = 2$, soit $f = x^2 - ax + b$. Si v est

la seconde racine de f alors $u + v = a \in K$ et donc, $v = a - u \in F$. Par conséquent, toutes les racines de f sont dans F et f est donc, scindé sur F.

Exercice 20. Considérons les corps $\mathbb{Q} \subset \mathbb{Q}(\sqrt{2}) \subset \mathbb{Q}(\sqrt[4]{2})$. On montre que le polynôme minimal de $\sqrt[4]{2}$ sur $\mathbb{Q}$ est $x^4 - 2$, celui de $\sqrt[4]{2}$ sur $\mathbb{Q}(\sqrt{2})$ est $x^2 - \sqrt{2}$ et celui de $\sqrt{2}$ sur $\mathbb{Q}$ est $x^2 - 2$. Donc,

$$[\mathbb{Q}(\sqrt[4]{2}) : \mathbb{Q}(\sqrt{2})] = [\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2.$$

Nous déduisons alors de l'exercice 23 que $\mathbb{Q}(\sqrt[4]{2})$ et $\mathbb{Q}(\sqrt{2})$ sont des extensions normales de $\mathbb{Q}(\sqrt{2})$ et $\mathbb{Q}$ respectivement. Cependant $\mathbb{Q}(\sqrt[4]{2})$ n'est pas une extension normale de $\mathbb{Q}$ car $\sqrt[4]{2}i$ est une racine de $x^4 - 2$ et $\sqrt[4]{2}i \notin \mathbb{Q}(\sqrt[4]{2})$.

Exercice 22. Soient $u \in F$ et f son polynôme minimal sur K. Par hypothèse, il existe une extension normale $F' \subset F$ de K contenant u. Le polynôme f est scindé sur F' et donc sur F.

Exercice 24. Soient f un polynôme irréductible dans $K[x]$ et $f = f_1 \cdots f_n$ une décomposition en facteurs irréductibles dans $F[x]$. Montrons que $\deg f_1 = \cdots = \deg f_n$. Soient $i, j \in \{1, \ldots, n\}$ et α, β des racines de f_i et f_j respectivement dans un surcorps de F. Puisque f est le polynôme minimal de α et β sur K,

$$K(\alpha) \cong K(\beta)$$

d'après le Corollaire 1.9. D'autre part, F est un corps de rupture sur K car F est normal sur K et donc, $F(\alpha)$ et $F(\beta)$ sont des corps de rupture sur $K(\alpha)$ et $K(\beta)$ respectivement. Alors, le Théorème 3.8 montre que

$$F(\alpha) \cong F(\beta).$$

Dès lors,

$$\deg f_i = [F(\alpha) : F] = [F(\beta) : F] = \deg f_j.$$

Le réciproque est laissée en exercice.

4. Le groupe de Galois associé à un polynôme

Exercice 1. (a) Il est clair que g est scindé sur F. Comme $F = K(u_1, \ldots, u_k)$ et $K \subset E \subset F$, $F = E(u_1, \ldots, u_k)$. Le corps F est donc un corps de rupture de g sur E .

(b) D'après le Théorème 3.11, F est Galois sur E puisque F est un corps de rupture de g sur E et g est séparable.
(c) L'inclusion $\mathrm{Aut}_E F \subset \mathrm{Aut}_K F$ est un exercice. Montrons l'inclusion réciproque. Remarquons que les coefficients de

$$g = x^k + v_1 x^{k-1} + \cdots + v_k = (x - u_1) \cdots (x - u_k)$$

sont les polynômes élémentaires symétriques en $u_1, \ldots, u_k$:

$$v_i = \sum_{1 \leq j_1 < \cdots < j_i \leq n} u_{j_1} \cdots u_{j_i}.$$

Soit $\sigma \in \mathrm{Aut}_K F$. D'après le Théorème 4.2 (a), σ échange les racines $u_1, \ldots, u_k$ de g et donc, $\sigma(v_i) = v_i$. Par conséquent, $\sigma|_E = \mathrm{id}$ et donc, $\sigma \in \mathrm{Aut}_E F$.

Exercice 2. Notons que les racines de f sont distinctes puisque $\mathrm{car}\,\mathbb{R} = 0$.
(a) Si a, b et c sont des réels,

$$D = (a - b)^2 (a - c)^2 (b - c)^2 > 0.$$

Réciproquement, supposons que f n'a pas trois racines réelles. Comme $\deg f = 3$ et $f \in \mathbb{R}[x]$, f a une racine réelle c et deux racines complexes conjugués, disons $\bar{a} = b$. Alors $(a - b)^2 < 0$ et $\overline{(a - c)^2} = (b - c)^2$ et donc,

$$D = (a - b)^2 (a - c)^2 (b - c)^2 < 0.$$

(b) découle de (a).

Exercice 3. Notons que f est irréductible dans $K[x]$ puisque son groupe de Galois est S_3. Notons que $F = K(u_1, u_2, u_3)$ est un corps de rupture de f sur K, et puisque f est séparable, F est séparable et donc Galois sur K (Théorème 3.11). Par conséquent,

$$[F : K] = |S_3| = 6.$$

Pour connaître tous les sous-corps entre K et F, d'après le Théorème 2.5, il suffit de trouver tous les sous-groupes de S_3 et de calculer leur fixateur dans F.

Exercice 4. Le résultat découle de la Proposition 4.8.

Exercice 5. Si f n'est pas irréductible dans $K[x]$, $f = (x - u)h$ avec $u \in K$ et $h \in K[x]$. Si h est réductible dans $K[x]$ alors h se scinde dans K puisque

$\deg h = 2$. Supposons alors que h est irréductible dans $K[x]$ et notons v, w ses racines. Alors, le groupe de Galois G de f sur K est égal au groupe de Galois de h sur K et donc, $G = \{\mathrm{id}, \sigma\}$ où $\sigma(v) = w$. Il en découle que

$$\begin{aligned}\sigma(\Delta) &= \sigma((u-v)(u-w)(v-w)) \\ &= (u-w)(u-v)(w-v) \\ &= -\Delta.\end{aligned}$$

Or, par hypothèse, $\Delta \in K$ car $\Delta^2 \in K^2$ et donc, $\sigma(\Delta) = \Delta$. Nous obtenons ainsi une contradiction.

Exercice 6. Supposons $\mathrm{car}\, K \neq 2, 3$. Nous avons $D = 3 \cdot 27 = 81 = 9^2$ et donc, $\Delta \in K$. L'exercice précédent montre alors que $x^3 - 3x + 1$ est soit scindé dans K soit irréductible dans $K[x]$.
Si $\mathrm{car}\, K = 3$, $x^3 - 3x + 1 = x^3 + 1 = (x+1)^3$.
Supposons que $\mathrm{car}\, K = 2$ et que $x^3 - 3x + 1 = (x+u)g$ est réductible dans $K[x]$. On montre que $g = x^2 + ux + u^2 + 1$. Il faut montrer que g est réductible dans $K[x]$. Puisque u^2 est racine de g, g est réductible dans $K[x]$.

Exercice 7. Par le Théorème de Lagrange, nous savons qu'un sous-groupe d'ordre 6 de S_4 ne contient que des 2 ou 3-cycles. Les sous-groupes d'ordre 6 sont de la forme

$$H = \{\mathrm{id}, (ij), (ik), (jk), (ijk), (kji)\}$$

avec $\{i, j, k\} \subset \{1, 2, 3, 4\}$. Donc si $\ell \in \{1, 2, 3, 4\} \setminus \{i, j, k\}$, il n'existe pas $\sigma \in H$ tel que $\sigma(\ell) = i$.

Exercice 8. Supposons $G = \mathrm{Aut}_K F = S_4$. Remarquons d'une part que F est Galois sur K et d'autre part que si $K \subsetneq L \subsetneq K(u)$, $[L : K] = [K(u) : F] = 2$ puisque $[K(u) : K] = 4$. Comme F est Galois sur K, il l'est aussi sur L (et $K(u)$) et donc,

$$|\mathrm{Aut}_L F| = [F : L] = [F : K]/[L : K] = 4!/2$$

Ce qui montre que $\mathrm{Aut}_L F$ est un sous-groupe d'indice 2 de $\mathrm{Aut}_K F = S_4$ et donc,

$$\mathrm{Aut}_L F = A_4.$$

De même, $\mathrm{Aut}_{K(u)} F$ est un sous-groupe d'indice 2 de $\mathrm{Aut}_L F = A_4$ et donc, $|\mathrm{Aut}_{K(u)} F| = 6$. Or il n'y a pas de sous-groupe d'ordre 6 dans A_4.

On procède de la même manière lorsque $\mathrm{Aut}_K F = A_4$.
Réciproquement, d'après la Proposition 4.11, si $G = Aut_K F \neq A_4, S_4$ alors il est isomorphe $V = \{\mathrm{id}, (12)(34), (13)(24), (14)(23)\}, \mathbb{Z}/4$ ou D_4. Si $G = \mathbb{Z}/4$, $F = K(u)$ puisque $K \subset K(u) \subset F, [k(u) : K] = 4$ et $[F : K] = |\mathbb{Z}/4| = 4$ (car F est Galois sur K). En appliquant la correspondance de Galois à la chaîne

$$\{0\} \subsetneq \{0, 2\} \subsetneq \mathbb{Z}/4$$

nous obtenons

$$K(u) \supsetneq \{0, 2\}' \supsetneq K.$$

De même si $G = V$, on montre que $F = K(u)$ et à la chaîne

$$\{\mathrm{id}\} \subsetneq \{\mathrm{id}, (12)(34)\} \subsetneq V$$

correspond

$$K(u) \supsetneq \{\mathrm{id}, (12)(34)\}' \supsetneq K.$$

Si $G = D_4 = \langle a, b \mid a^4 = b^2 = 1, ba = a^{-1}b\rangle$ alors $|\mathrm{Aut}_{K(u)}F| = 2$ puisque $|D_4| = 8$ et $[K(u) : K] = 4$. Alors à la chaîne

$$\{1, a^2\} \subsetneq \{1, a, a^2, a^3\} \subsetneq D_4$$

correspond

$$K(u) \supsetneq \{1, a, a^2, a^3\}' \supsetneq K.$$

Exercice 10. Notons que dans les exercices qui suivent, les polynômes seront séparables dès qu'ils seront irréductibles puisque $\mathrm{car}\,\mathbb{Q} = 0$. Nous noterons G le groupe de Galois du polynôme considéré.
(a) Le polynôme $f = x^4 - 5$ est irréductible par le critère d'Eisenstein. Le résolvant de f est

$$x^3 + 20x = x(x^2 + 20)$$

dont les racines sont $0, 2\sqrt{5}i$ et $-2\sqrt{5}i$. Par conséquent,

$$m = [\mathbb{Q}(\sqrt{5}i) : \mathbb{Q}] = 2.$$

D'autre part,

$$f = (x^2 - \sqrt{5})(x^2 + \sqrt{5}) = (x - \sqrt[4]{5})(x + \sqrt[4]{5})(x - \sqrt[4]{5}i)(x + \sqrt[4]{5}i).$$

Or $\sqrt{5}, \sqrt[4]{5}, \sqrt[4]{5}i, \sqrt[4]{5} - \sqrt[4]{5}i, \sqrt[4]{5} + \sqrt[4]{5}i \notin \mathbb{Q}(\sqrt{5}i)$ et donc, f est irréductible dans $\mathbb{Q}(\sqrt{5}i)[x]$. La Proposition 4.11 montre alors que $G \cong D_4$.

(c) Par Gauss, $f = x^3 - x - 1$ est irréductible sur $\mathbb{Q}$ puisque 1 et -1 ne sont pas racines de f. Puisque le discriminant vaut -23 qui n'est pas un carré dans $\mathbb{Q}$, du Corollaire 4.7, nous déduisons que $G = S_3$.

(d) On procède comme dans (c), on montre que le discriminant vaut -2700 et donc, $G = S_3$.

(f) Le critère d'Eisenstein montre que $f = x^5 - 6x + 3$ est irréductible sur $\mathbb{Q}$. Montrons que les hypothèses du Théorème 4.12 sont satisfaites par f. Comme $f(-2) < 0, f(0) > 0, f(0) < 0, f(2) > 0$, le Théorème de la valeur intermédiaire montre que f a au moins trois racines réelles. Rappelons que Les racines réelles de f sont séparées par les racines réelles de la dérivée de f:

$$f' = 5x^4 - 6 = (\sqrt{5}x^2 - \sqrt{6})(\sqrt{5}x^2 + \sqrt{6}).$$

Comme f' a deux racines réelles, f en a au plus trois et donc, f a exactement trois racines réelles. Dès lors, le Théorème 4.12 montre que $G = S_5$.

(i) On vérifie que $f = x^4 - 4x^2 + 5$ n'a pas de racines dans $\mathbb{Q}$. Montrons que f n'admet pas de décomposition 2×2:

$$f = (x^2+ax+b)(x^2+cx+d) = x^4+(a+c)x^3+(b+d+ac)x^2+(ad+bc)x+bd.$$

On obtient le système suivant:

$$\begin{cases} a+c &= 0 \\ b+d+ac &= -4 \\ ad+bc &= 0 \\ bd &= 5 \end{cases}$$

Sachant que $a, b, c, d \in \mathbb{Q}$, on déduit que $b \neq d$, $b, d \in \{1, -1, 5, -5\}$ et donc, $b + d \in \{-6, 6\}$. De $ad + bc = 0$, on obtient alors $a = c = 0$ puisque $b \neq d$. Dès lors, $b + d + ac = -4$ montre que $b + d = -4$, ce qui est absurde. Par conséquent, f n'admet pas de décomposition 2×2.
Le résolvant de f est

$$x^3 + 4x^2 - 20x - 80 = (x + 4)(x - 2\sqrt{5})(x + 2\sqrt{5}).$$

Par conséquent, $m = 2$ et puisque

$$f = (x^2 - 2 - i)(x^2 - 2 + i),$$

f n'a pas de racine dans $\mathbb{Q}(\sqrt{5})$. Supposons que $f = (x^2+ax+b)(x^2+cx+d)$ avec $a, b, c, d \in \mathbb{Q}(\sqrt{5})$. On obtient le système ci-dessus. On en déduit que

$$a = -c,\ 0 = ad - ab = a(d-b)$$

et donc, $a = 0 = c$ ou $d = b$. Si $d = b$ alors $b = \pm\sqrt{5}$. Sachant que $a = -c$, on déduit de $b+d+ac = -4$ que $a^2 = 4 \pm 2\sqrt{5}$ qui n'a pas de solution dans $\mathbb{Q}(\sqrt{5})$. On obtient la même conclusion lorsque $a = c = 0$ et donc, f est irréductible sur $\mathbb{Q}(\sqrt{5})$. Par conséquent, $G = D_4$ puisque $m = 2$.

(j) Puisque $g = x^4+2x^2+x+3 = x^4+2x^2+(x+\frac{1}{2})^2+\frac{11}{4}$, g n'a pas de racine dans $\mathbb{Q}$. Montrons que g n'admet pas de décomposition 2×2:

$$g = (x^2+ax+b)(x^2+cx+d) = x^4+(a+c)x^3+(b+d+ac)x^2+(ad+bc)x+bd.$$

On obtient le système suivant:

$$\begin{cases} a+c &= 0 \\ b+d+ac &= 2 \\ ad+bc &= 1 \\ bd &= 3 \end{cases}$$

Alors $b, d \in \{1, 3\}$ ou $b, d \in \{-1, -3\}$ et donc, $b+d \in \{\pm 4\}$. Comme $c = -a$, $a^2 \in \{2, -6\}$, ce qui est impossible dans $\mathbb{Q}$. Le polynôme g est donc irréductible sur $\mathbb{Q}$. Le résolvant de ce polynôme est

$$f = x^3 - 2x^2 - 12x + 23$$

qui est irréductible aussi sur $\mathbb{Q}$. Nous savons par le Proposition 4.8 que le discriminant de f est égal au discriminant de

$$f(x+2/3) = x^3 - (40/3)x + 389/27$$

et donc, $D = 3877$ qui n'est pas un carré dans $\mathbb{Q}$. Par conséquent, Le groupe de Galoid de f est S_3. Il suit alors que $m = 6$ et donc, $G = S_4$ par la Proposition 4.11.

5. Les corps finis

Exercice 1. Nous savons par le Corollaire 5.2 que $|K| = p^n$ pour un certain naturel $n \geq 1$. Comme $(K, +)$ est un groupe fini commutatif, d'après

le Théorème 2.1 du chapitre II, il existe $p_1, \ldots, p_k$ des naturels premiers et $n_1, \ldots, n_k \in \mathbb{N}$ tels que

$$K \cong \mathbb{Z}/p_1^{n_1} \oplus \cdots \oplus \mathbb{Z}/p_k^{n_k}$$

en tant que groupe. Puisque tout élément de K est d'ordre p, $p_i = p$ et $n_i = 1$. Dès lors, $k = n$ car

$$p^n = |K| = |\mathbb{Z}/p \oplus \cdots \oplus \mathbb{Z}/p| = p^k$$

et donc, K est isomorphe à $n = [K : \mathbb{F}_p]$ copies de $\mathbb{Z}/p$.
Autre solution: soit $e_1, \ldots, e_n$ une base de K sur son corps premier K_0. Rappelons que $K_0 \cong \mathbb{F}_p$ avec p un naturel premier. Alors

$$K = \{a_1 e_1 + \cdots + a_n e_n \mid a_1, \ldots, a_n \in K_0\}.$$

En tant que groupe, K est alors isomorphe à n copies de $\mathbb{Z}/p$:

$$K \cong K_0 \oplus \cdots \oplus K_0 \cong \mathbb{Z}/p \oplus \cdots \oplus \mathbb{Z}/p.$$

Exercice 2. Si $a = 0$, le résultat est vrai. Si $a \neq 0$, $a \in (\mathbb{F}_p)^\times$ et donc, par le Théorème de Lagrange $a^{p-1} = 1$, ou encore $a^p = a$.

Exercice 3. Comme $\sigma : K \longrightarrow K : x \longrightarrow x^p$ est un $\mathbb{F}_p$-automorphisme de corps (Lemme 5.5), quelque soit $v \in K$, il existe un unique élément $x \in K$ tel que $x^p = \sigma(x) = y$.

Exercice 4. Notons F l'ensemble de toutes les racines de f dans un corps de rupture F' de f sur K. Puisque les racines de f sont distinctes $|F| = \deg f < \infty$. Alors F est un corps fini et donc, $\operatorname{car} F = p$ et $\deg f = p^n$. Par conséquent, $\operatorname{car} F' = p$ puisque $F \subset F'$. De même, $\operatorname{car} K = p$ car $K \subset F'$. La Proposition 5.6 montre alors que F est un corps de rupture de $x^{p^n} - x$ sur $\mathbb{F}_p$. Dès lors, $x^{p^n} - x$ divise f. Mais $\deg f = \deg(x^{p^n} - x)$, par conséquent $f = x^{p^n} - x$.

Exercice 5. (a) On vérifie que $x^2 + 1$ est irréductible sur $\mathbb{F}_3$ (exercice). Le Théorème 1.6 montre alors que si u est une racine de $x^2 + 1$ dans un surcorps de $\mathbb{F}_3$, alors

$$\frac{\mathbb{F}_3[x]}{(x^2+1)} \cong \mathbb{F}_3(u) = \{a + bu \mid a, b \in \mathbb{F}_3\}$$

qui est un corps a 9 élément.

(b) Pour construire un corps à p^n éléments, il suffit de quotienter $\mathbb{F}_p[x]$ par un idéal engendré par un polynôme irréductible de degré n dans $\mathbb{F}_p[x]$.

Exercice 6. Soir $K_0 \subset F$, l'ensemble de toutes les racines de $x^n - 1$. Comme $(n, q) = 1$, $n \neq 0$ dans K. Alors $(x^n - 1)' = nx^{n-1}$ et $x^n - 1$ sont premiers entre eux et donc, $x^n - 1$ a n racines distinctes et $|K_0| = n$. On vérifie (exercice) que $(K_0, .)$ est un groupe et que K_0 est un sous-groupe de $F^\times$. Si on pose $[F : K] = k$, par le Théorème de Lagrange,

$$n = |K_0| \mid |F^\times| = q^k - 1.$$

Montrons à présent que k est le plus petit entier tel que $n \mid q^k - 1$. Supposons que $k' < k$ et $n \mid q^{k'} - 1$. Soit $1, u_2, \ldots, u_n$ les racines de $x^n - 1$ dans F. Alors $F = K(u_2, \ldots, u_n)$. Remarquons que $z^{q^{k'}} = z$ pour tout $z \in K$ puisque $|K| = q$, et $u_i^{q^{k'}} = u_i$ puisque $n \mid q^{k'} - 1$. Par conséquent, quelque soit $v \in F$, $v^{q^{k'}} = v$ et donc,

$$|F| \leq \deg(x^{q^{k'}} - x) = q^{k'} < q^k = |F|.$$

Exercice 7. Soient F un corps de rupture de $x^{q^n} - x$ sur K et u une racine de f dans F. Dés lors,

$$n = [F : K] = [F : K(u)][K(u) : K] = [F : K(u)] \deg f$$

et donc, $\deg f$ divise n. Réciproquement, supposons que $n = \deg f \cdot r$ et que u est une racine de f. Notons que $|K(u)| = q^{\deg f}$ puisque $[K(u) : K] = degf$ et donc,

$$u^n = u^{\deg f \cdot r} = u.$$

Nous venons de montrer que u est une racine de $x^{q^n} - x$ et donc, f divise $x^{q^n} - x$.

Exercice 8. Si on note $[F : K] = \ell$ alors

$$p^n = |F| = (p^r)^\ell = p^{r\ell}$$

et donc, $r \mid n$.

Le lecteur vérifiera que $\mathrm{Aut}_K F \subset \mathrm{Aut}_{\mathbb{F}_p} F = \langle\varphi\rangle$ où φ est le $\mathbb{F}_p$-automorphisme de F tel que $x \to x^p$. De plus si $x \in K$, $\varphi^r(x) = x^{p^r} = x$ et donc, $\varphi^r \in \mathrm{Aut}_K F$. Montrons à présent que $|\varphi^r| = n/r$. Quelque soit $x \in F$,

$$(\varphi^r)^{n/r}(x) = x^{p^{r(n/r)}} = x.$$

Donc, $(\varphi^r)^{n/r} = \mathrm{id}$. Supposons que $k < n/r$ et $(\varphi^r)^k = \mathrm{id}$. Alors, quelque soit $x \in F$, $(\varphi^r)^k(x) = x^{p^{rk}} = x$ et donc,

$$|F| \leq \deg(x^{p^{rk}} - x) = p^{rk} < p^{r(n/r)} = p^n = |F|.$$

Exercice 10. Si $\mathrm{car}\, K = 2$, $\varphi : F \longrightarrow F : x \mapsto x^2$ est un automorphisme (Lemme 5.5) et donc, tout élément est un carré.
Supposons $\mathrm{car}\, K \neq 2$, $|K| = q$ et $\alpha \in K$. Notons K^2 l'ensemble des carrés et $K^2_\alpha = \{\alpha - a^2 \mid a \in K\}$. Si $a, b \in K^\times$ alors $a^2 = (-a)^2$, et si $a^2 = b^2$ alors $a = \pm b$. Donc,

$$|K^2| = (q-1)/2 + 1 = (q+1)/2.$$

Si $\alpha - a^2 = \alpha - b^2$ alors $a = \pm b$ et donc, $|K^2| = |K^2_\alpha|$. Par conséquent, $K^2 \cap K^2_\alpha \neq \emptyset$ car K ne possède que q éléments. Alors, il existe $a, b \in K$ tels que $\alpha - a^2 = b^2$ et donc, $\alpha = a^2 + b^2$.
Autre preuve lorsque $\mathrm{car}\, K = 2$: notons alors que q est paire. Puisque $K^\times, .$ est cyclique, si g est un générateur de $K^\times$ alors $g^q = g$. Donc, $g = (g^{\frac{q}{2}})^2$ est un carré dans $K^\times$. Dès lors, tout élément de $K^\times$ est un carré.

Exercice 11. (a) Puisque F est un corps de rupture de $\{x^{p^n} - x \mid n \in \mathbb{N}\setminus\{0\}\}$ et que $x^{p^n} - x$ est séparable pour tout n car $(x^{p^n} - x)' = -1$, F est algébrique et Galois sur K d'après le Théorème 3.11.
(b) Soit $u \in F \setminus \mathbb{F}_p$ une racine de $x^{p^n} - x$. Alors $\varphi(u) \neq u$. Le Lemme 5.5 montre que φ est en fait un $\mathbb{F}_p$-automorphisme de $\mathbb{F}_p(u)$. Comme F est un corps de rupture de $\{x^{p^n} - x \mid n \in \mathbb{N} \setminus \{0\}\}$, le Théorème 3.8 montre que φ peut s'étendre en un automorphisme de F.

6. Séparabilité

Exercice 1. Soit $n' \equiv_p n$, alors $n' \in \mathbb{F}_p \subset K$. On a $(n', p) = 1$ et donc, n' est inversible dans $\mathbb{F}_p$. Puisque $\mathrm{car}\, K = p$, $n'v = nv \in K$ et donc, $v = (n')^{-1}n'v \in K$.

Exercice 2. Par le Théorème 6.4, il existe $n \in \mathbb{N}$ tel que $u^{p^n} \in K \subset E$ et donc, par le même Théorème u est purement inséparable sur E.

Exercice 3. Supposons qu'il existe un élément $x \in F \setminus K$ séparable sur K et donc sur E. Puisque E est purement inséparable sur K, $x \notin E$. Alors, F n'est pas une extension purement inséparable de E.

Exercice 4. On a $K(u, v) \supset K(u + v)$. Montrons l'inclusion réciproque. Comme v est purement ins'eparable, il existe $n \in \mathbb{N}$ tel que $v^{p^n} \in K$ et donc, de $(u + v)^{p^n} = u^{p^n} + v^{p^n}$, on déduit que

$$u^{p^n} \in K(u + v)^{p^n} \subset K(u + v).$$

Par le Théorème 6.4, u est alors purement inséparable sur $K(u + v)$, mais u est séparable sur K et donc sur $K(u + v)$ (Théorème 6.2). Par conséquent, $u \in K(u + v)$ et donc, $v = (u + v) - u$ aussi.
Remarquons que $(uv)^{p^n} = u^{p^n} v^{p^n}$. Comme $v^{p^n} \in K$,

$$v^{p^n} \in K(uv)^{p^n} \subset K(uv).$$

Donc, u est purement inséparable sur $K(uv)$, mais u est séparable sur K et donc sur $K(uv)$. Par conséquent, $u \in K(uv)$ et donc, $v = u^{-1}(uv)$ aussi.

Exercice 5. Si b est une racine de $x^{p^n} - a$, b est purement inséparable sur K puisque $b^{p^n} = a \in K$. Le Théorème 6.4 montre que le polynôme minimal de b sur K est de la forme $x^{p^m} - b^{p^m}$ ($b^{p^m} \in K$). Montrons que $m = n$, ce qui entraînera l'irréductibilité de $x^{p^n} - a$. Si $p^m < p^n$ alors

$$b^{p^{n-1}} = (b^{p^m})^{p^{n-m-1}} \in K$$

et donc, $a = (b^{p^{n-1}})^p \in K^p$, ce qui contredit l'hypothèse $a \notin K^p$. Par conséquent, $n = m$.

Exercice 6. Soit b une racine de f dans un surcorps de K. Par hypothèse, $f = (x - b)^m$ et donc,

$$f' = m(x - b)^{m-1} \in K[x].$$

Puisque f est le polynôme minimal de b sur K et que $f'(b) = 0$, il faut que $f' = 0$. Comme $m \geq 2$, $\operatorname{car} K$ ne peut être que différent de zéro, disons $\operatorname{car} K = p$. Comme $p \mid m$, $m = p^n k$ avec $(p, k) = 1$. Alors

$$f = (x - b)^m = (x - b)^{p^n k} = (x^{p^n} - b^{p^n})^k \in K[x].$$

Mais, f est irréductible sur K, donc $k = 1$ et $b^{p^n} \in K$. Ce qui montre que f est bien de la forme $x^{p^n} - a$ avec $a \in K$.

Exercice 7. Notons que cet exercice ne possède d'intérêt qu'en caractéristique différente de zéro.
(a) Supposons que $S \subset E$. Comme F est purement inséparable sur S, l'exercice 2 montre que F est purement inséparable sur E. Réciproquement, supposons que F est purement inséparable sur E et que $S \not\subset E$. Si $x \in S \setminus E$, d'une part x est alors séparable sur K et donc sur E (exercice 3.12), et d'autre part x est inséparable sur E puisque $x \in F \setminus E$. Le Théorème 6.2 montre alors que $x \in E$, une contradiction.
(b) Si $u \in P$ alors u est purement inséparable sur E par l'exercice 2. Mais u est séparable sur E par hypothèse. Donc, $u \in E$ par le Théorème 6.2.
(c) Soit $u \in E \subset F$. Le Théorème 6.7 montre alors que u est purement inséparable sur S. D'après le Théorème 6.4, $u^{p^n} \in S$ pour un certain naturel n. Comme $u^{p^n} \in E$ aussi, $u^{p^n} \in K$ puisque $E \cap S = K$. Dès lors, u est purement inséparable sur K d'après le Théorème 6.4, et donc, $u \in P$ par définition de P.

Exercice 8. Notons P l'ensemble des éléments purements inséparables de F sur K. Alors $[P : K] = p^n$, et puisque $[F : K] = [F : P][P : K]$ et p ne divise pas $[F : K]$, $n = 0$ et donc, $P = K$; ce qui implique que F est séparable sur K par le Théorème 6.7.

Exercice 9. Si u est séparable sur K, $K(u^p) = K(u)$ d'après le Corollaire 6.9 et $K(u)$ est une extension séparable de K d'après le Lemme 6.6. Donc, u^p est séparable sur K. Alors, par le Corollaire 6.9,

$$K(u) = K(u^p) = K(u^{p^2}).$$

On termine la preuve par induction sur n.
Réciproquement, comme

$$K(u) = K(u^p) = KK^pK(u^p) = K(K(u)^p),$$

le Corollaire 6.9 implique que $K(u)$ est séparable sur K puisque $[K(u) : K]$ est fini.

Exercice 11. Soit u une racine de f. L'exercice 8 montre que $K(u)$ est séparable sur K et donc, u est séparable sur K.

Exercice 15. Soit $\alpha = \sum_{i,j} a_{ij} u^i v^j \in K(u,v)$. Alors $\alpha^p = \sum_{i,j} a_{ij}^p (u^p)^i (v^p)^j \in K$ puisque $a_{ij}, u^p, v^p \in K$. Par conséquent, $[K(\alpha) : K] = 1$ ou p puisque $[K(\alpha) : K]$ divise $[K(u,v) : K] = p^2$. Donc, $K(\alpha) \subsetneq K(u,v)$.

Montrons que si $k \neq k'$ alors $K(u + vk) \neq K(u + vk')$. Sinon $(u + vk)$ et $(u + vk')$ ont le même polynôme minimal $x^p - (u + vk)^p = x^p - (u + vk')^p$. On en déduit que $k^p = (k')^p$. Par le Lemme 5.5 ($r = 1$), nous avons $k = k'$ puisque φ est injectif ($k^p = \varphi(k) = \varphi(k') = (k')^p$). Par conséquent, il y a une infinité de sous corps dans F puisque K est infini.

7. Extensions cycliques

Exercice 2. Notons $|K| = q$ et $|F| = q^n$. L'application $N_K^F : F^\times \longrightarrow K^\times$ est un morphisme de groupe. Il suffit donc de montrer que $|\operatorname{Im} N| = q - 1$. La Proposition 5.10 montre que F est une extension cyclique de K. Nous savons alors que

$$\ker N = \{u(\varphi(u))^{-1} \mid u \in F^\times\}$$

où $\varphi : F \longrightarrow F : u \mapsto u^q$. Rappelons que φ est un générateur de $\operatorname{Aut}_K F$. Calculons le nombre d'éléments dans $\ker N$:

$$\begin{aligned} u(\varphi(u))^{-1} \neq v(\varphi(v))^{-1} &\iff v^{-1}u \neq \varphi(v^{-1}u) \\ &\iff v^{-1}u \notin \langle\varphi\rangle' = \operatorname{Aut}_K F = K \\ &\iff uK \neq vK. \end{aligned}$$

Le nombre d'éléments dans $\ker N$ est donc égal au nombre de classes modulo $K^\times$ dans $F^\times$:

$$|\ker N| = \frac{|F^\times|}{|K^\times|} = \frac{q^n - 1}{q - 1}.$$

Puisque

$$\operatorname{Im} N \cong \frac{F^\times}{\ker N},$$

nous obtenons $|\operatorname{Im} N| = q - 1$.

On procède de manière semblable pour montrer que T_K^F est surjectif.

Exercice 3. Soit F une extension normale finie de E. Si $\operatorname{Aut}_E F$ n'est pas cyclique, $\forall \sigma \in \operatorname{Aut}_E F$, $\langle\sigma\rangle \subsetneq \operatorname{Aut}_E F$. La correspondance de Galois montre

alors que[3] $E \subsetneq \langle\sigma\rangle' \subsetneq F$ et donc, $\forall \sigma \in \mathrm{Aut}_E F, v \in \langle\sigma\rangle'$. Ce qui entraîne que $v \in (\mathrm{Aut}_E F)' = E$ car F est Galois sur E, une contradiction.

Exercice 4. Soit M une extension normale finie de F. Supposons que $\mathrm{Aut}_F M$ n'est pas cyclique. Comme $\sigma|_M \in \mathrm{Aut}_F M$ d'après le Théorème 3.14, $\langle\sigma|_M\rangle \subsetneq \mathrm{Aut}_F M$ et donc,

$$F \subset (\mathrm{Aut}_F M)' \subsetneq \langle\sigma|_M\rangle' = F,$$

une contradiction.

Exercice 5. Notons que $\mathrm{Aut}_K F \cong \mathbb{Z}/p^n$ puisque F est une extension cyclique de degré p^n de K. Les sous-groupes de $\mathbb{Z}/p^n$ sont

$$\{0\} \subset \langle p^{n-1}\rangle \subset \cdots \subset \langle p^i\rangle \subset \cdots \subset \langle p\rangle \subset \mathbb{Z}/p^n.$$

Comme $K(u)'$ et L' sont des sous-groupes de $\mathrm{Aut}_K F \cong \mathbb{Z}/p^n$, $K(u)' \subset L'$ ou $L' \subset K(u)'$. Puisque F est galois sur K, $L = L''$ et $K(u) = K(u)''$ et donc, soit $L \subset K(u)$ soit $K(u) \subset L$. Comme $u \notin L$, $L \subsetneq K(u)$ et donc, $[K(u) : L] \neq 1$. Alors,

$$p^n = [F : K] = [F : K(u)][K(u) : L][L : K] = [F : K(u)][K(u) : L]p^{n-1}$$

entraîne que $[F : K(u)] = 1$.

Exercice 7. Soit ω une racine primitive $n^{\text{ième}}$ de 1. Remarquons alors que les racines de $x^{2n} - 1 = (x^n - 1)(x^n + 1)$ sont $\pm 1, \pm\omega, \ldots, \pm\omega^{n-1}$ puisque n est impair. De plus $-\omega$ est d'ordre $2n$, ce qui montre que $-\omega$ est une racine primitive $2n^{\text{ième}}$ de 1.

Exercice 8. Puisque $\mathrm{car}\,\mathbb{Q} = 0$, F est séparable sur $\mathbb{Q}$. Le Théorème de l'élément primitif 6.15 montre alors que F est une extension simple de $\mathbb{Q}$ et donc, il n'y a qu'un nombre fini de corps intermédiaires entre $\mathbb{Q}$ et F. Notons aussi que si $\omega \in F \setminus \{\pm 1\}$ est une racine de l'unité, $\mathbb{Q}(\omega)$ est un corps intermédiaire de $\mathbb{Q}$ et F. Dès lors, F ne peut contenir qu'un nombre fini de racines de l'unité.

Exercice 10. (a) Si $\mathrm{car}\, K = p$ et b est une racine de $x^p - a$ alors $b^p = a$ et donc, $x^p - a = (x - b)^p$. Ce qui montre que b est purement inséparable sur K.

[3] on prend $\sigma \neq \mathrm{id}$.

Le Corollaire 6.5 entraîne alors que $[K(b) : K] = 1$ ou p. Si c'est 1 alors $b \in K$ et donc, $x^p - a = (x - b)^p$ est scindé dans K. Si $[K(b) : K] = p$ alors $x^p - a$ est irréductible sur K.

Supposons que car $K \neq 0$ et que $\omega \in K$ est une racine primitive $p^{\text{ième}}$ de 1. Si b est une racine de $x^p - a$ alors le Lemme 7.10 montre que $K(b)$ est un corps de rupture de $x^p - a$ sur K. D'après le Théorème 7.11, $K(b)$ est cyclique de degré d avec $d \mid p$. Par conséquent $d = 1$ ou p. Si $d = 1$, $b \in K$ et donc, $x^p - a$ se scinde dans K. Si $d = p$, $[K(b) : K] = p$ et donc, $x^p - a$ est irréductible dans $K[x]$.

(b) Notons d'abord que $K(u^p) = K$ puisque $u^p = a$. Donc, si $K(u) \neq K(u^p) = K$, $u \notin K$ et donc, $[K(u) : K] = p$ d'après (a). Réciproquement, si $[K(u) : K] = p$, $u \notin K$ et donc, $K(u) \neq K = K(u^p)$.

8. Extensions cyclotomiques

Exercice 1. Si $i+n\mathbb{Z}$ est inversible dans $\mathbb{Z}/n$, il existe $j \in \mathbb{Z}$ tel que $(i+n\mathbb{Z})(j+n\mathbb{Z}) = 1+n\mathbb{Z}$ et donc, $ij-1 \in n\mathbb{Z}$, disons $ij-1 = -nk$. Alors $ij+nk = 1$, ce qui montre que i et n sont premiers entre eux. Réciproquement, si $ij+nk = 1$ alors $ij-1 \in n\mathbb{Z}$ et donc $(i+n\mathbb{Z})(j+n\mathbb{Z}) = 1+n\mathbb{Z}$, ce qui termine la première partie de l'exercice.

Nous avons alors $(\mathbb{Z}/n)^\times = \{i + n\mathbb{Z} \mid 1 \leq i \leq n \text{ et } (i, n) = 1\} = \varphi(n)$.

Exercice 2. (a) D'après l'exercice précédent, $k + p^n\mathbb{Z}$ est non inversible dans $\mathbb{Z}/p^n$ si $(k, p^n) \neq 1$. Les éléments non inversibles de $\mathbb{Z}/p^n$ sont donc de la forme $kp + n\mathbb{Z}$ avec $0 \leq k \leq p^{n-1}-1$. Il y en a donc p^{n-1}. Dès lors, $\varphi(p^n) = p^n - p^{n-1} = p^n(1 - 1/p)$.

(b) Comme $\mathbb{Z}/mn \cong \mathbb{Z}/m \times \mathbb{Z}/n \iff (m, n) = 1$, si $(m, n) = 1$ alors

$$(\mathbb{Z}/mn)^\times \cong (\mathbb{Z}/m)^\times \times (\mathbb{Z}/n)^\times.$$

L'exercice 1 implique alors que $\varphi(mn) = \varphi(m)\varphi(n)$ dès que $(m, n) = 1$.

(c) D'après (a) et (b),

$$\varphi(n) = \prod_{i=1}^{r} \varphi(p_i^{k_i}) = \prod_{i=1}^{r} p_i^{k_i}(1-\frac{1}{p_i}) = \left(\prod_{i=1}^{r} p_i^{k_i}\right)\left(\prod_{i=1}^{r}(1-\frac{1}{p_i})\right) = n\prod_{i=1}^{r}(1-\frac{1}{p_i}).$$

(d) Montrons d'abord le résultat pour $n = p^k$. Par (a),

$$\begin{aligned}\sum_{d|p^k} \varphi(d) &= \varphi(1) + \varphi(p) + \cdots + \varphi(p^k) \\ &= 1 + (p-1) + (p^2 - p) + \cdots + (p^k - p^{k-1}) \\ &= p^k.\end{aligned}$$

Si $n = \prod_{i=1}^r p_i^{k_i}$ alors par l'exercice 2 (b)

$$\begin{aligned}\sum_{d|n} \varphi(d) &= \sum_{\substack{d_1,\ldots,d_r \\ \forall i \;\; d_i | p_i^{k_i}}} \varphi(d_1 \cdots d_r) \\ &= \sum_{\substack{d_1,\ldots,d_r \\ \forall i \;\; d_i | p_i^{k_i}}} \varphi(d_1) \cdots \varphi(d_k) \\ &= \left(\sum_{d_1 | p_1^{k_1}} \varphi(d_1) \right) \cdots \left(\sum_{d_r | p_r^{k_r}} \varphi(d_r) \right) \\ &= p_1^{k_1} \cdots p_r^{k_r} = n\end{aligned}$$

(e) Soient $n = p_1^{k_1} \cdots p_r^{k_r}$ et $n' = p_1 \cdots p_r$. Par hypothèse, nous savons que si $d \mid n$ et $p_i^2 \mid d$ pour un certain i alors $\mu(d) = 0$. Par conséquent,

$$\sum_{d|n} \mu(d) = \sum_{d|n'} \mu(d).$$

Montrons que $\sum_{d|n'} \mu(d) = 0$ si $n' \neq 1$. Remarquons que si $d \mid p_1 \cdots p_{r-1}$ alors $\mu(dp_r) = -\mu(d)$ par hypothèse. Ceci implique que

$$\begin{aligned}\sum_{d|n'} \mu(d) &= \sum_{d|p_1 \cdots p_{r-1}} \mu(d) + \sum_{dp^r | p_1 \cdots p_r} \mu(dp_r) \\ &= \sum_{d|p_1 \cdots p_{r-1}} \mu(d) - \sum_{d|p_1 \cdots p_{r-1}} \mu(d) \\ &= 0.\end{aligned}$$

Nous sommes prêt pour terminer l'exercice:

$$\begin{aligned}
\sum_{d|n} d\mu(\frac{n}{d}) &= \sum_{d|n}\left(\sum_{e|d}\varphi(e)\mu(\frac{n}{d})\right)\\
&= \sum_{e|n}\left(\varphi(e)\sum_{\substack{d|n\\ e|d}}\mu(\frac{n}{d})\right)\\
&= \sum_{e|n}\left(\varphi(e)\sum_{d|\frac{n}{e}}\mu(d)\right)\\
&= \sum_{\substack{e|n\\ e\neq n}}\left(\varphi(e)\sum_{d|\frac{n}{e}}\mu(d)\right)+\varphi(n)\mu(1)\\
&= \sum_{\substack{e|n\\ e\neq n}}(\varphi(e)\cdot 0)+\varphi(n)\\
&= \varphi(n).
\end{aligned}$$

Exercice 3. (a) Si $n > 2$, soit $n = 2^k$ avec $k > 1$ et donc, $\varphi(n) = 2^{k-1}(2-1)$ est paire, soit il existe un naturel premier $p > 2$ tel que $p \mid n$. Ecrivons $n = mp^k$ avec $(p, m) = 1$. Alors, par 2 (a) et (b),

$$\varphi(n) = \varphi(mp^k) = \varphi(m)\varphi(p^k) = \varphi(m)p^{k-1}(p-1)$$

est paire puisque $p - 1$ l'est.

(b) Supposons que $\varphi(n) = 2$. D'après 2(a) et (b), si $n = p_1^{k_1}\cdots p_r^{k_r}$ alors

$$2 = \varphi(n) = \varphi(p_1^{k_1})\cdots\varphi(p_r^{k_r}) = p_1^{k_1-1}(p_1-1)\cdots p_r^{k_r-1}(p_r-1).$$

S'il existe i tel que $p_i > 3$ alors $p_i - 1 > 2$ et donc, $\varphi(n) > 2$. Ceci implique que n est de la forme 2^k3^ℓ. Si $k > 2$ ou $\ell > 1$, $\varphi(n) = 2^{k-1}3^{\ell-1}2 > 2$. De même, si $k = 2$ et $\ell = 1$, $\varphi(n) = 4 > 2$. Donc, $n = 3, 4$ ou 6.

(c) Notons d'abord que $1 = \varphi(1) \neq 1/p$ pour tout naturel premier p. Supposons alors que $n > 1$. L'exercice 2 (c) montre que

$$\varphi(n) = n(1 - 1/p_1)\cdots(1 - 1/p_r).$$

Alors, de $\varphi(n) = n/p$, on déduit que

$$\frac{1}{p} = (1 - \frac{1}{p_1}) \cdots (1 - \frac{1}{p_r}) = \frac{(p_1 - 1) \cdots (p_r - 1)}{p_1 \cdots p_r}.$$

Par conséquent,

$$p_1 \cdots p_r = (p_1 - 1) \cdots (p_r - 1)p. \tag{5.1}$$

Remarquons que 2 divise $p_1 \cdots p_r$ puisque $(p_i - 1)$ est pair lorsque $p_i > 2$. Posons $p_1 = 2$. Notons aussi que si $r \geq 3$ alors il existe $i \neq j$ tels que $p_i, p_j > 2$. Comme $(p_i - 1)$ et $(p_j - 1)$ sont pairs, 4 diviserait $p_1 \cdots p_r$, ce qui est impossible puisque $p_1, \ldots, p_r$ sont des premiers distincts. Par conséquent, $r = 1$ ou 2. Si $r = 1$ alors $n = 2^k$ avec $k \geq 1$ et $p = 2$. Si $r = 2$, en posant $p_1 = 2$, légalité (5.1) montre que $2p_2 = (2 - 1)(p_2 - 1)p$. Ceci implique que $2 = p_2 - 1$ et $p = p_2$ et donc, $p_2 = p = 3$. Finallement, nous obtenons $(2^k, 2)$ avec $k \geq 1$ et $(2^k 3^\ell, 3)$ avec $k, \ell \geq 1$.

Exercice 4. (a) L'exercice 1 montre que $|(\mathbb{Z}/p^n)^\times| = \varphi(p^n) = p^{n-1}(p - 1)$ par l'exercice 2 (a). Il suffit donc de montrer que $(\mathbb{Z}/p^n)^\times$ est cyclique. Procédons par induction sur n et soit $n = 1$. Alors $(\mathbb{Z}/p)^\times = (\mathbb{F}_p)^\times$ est cyclique puisque $\mathbb{F}_p$ est un corps et le groupe multiplicatif d'un corps fini est cyclique d'après le Théorème 5.3. Traitons alors le cas $n > 1$. Soit S_p un p-Sylow de $(\mathbb{Z}/p^n)^\times$. Comme $|S_p| = p^{n-1}$, S_p est cyclique par hypothèse d'induction. Afin de conclure, il suffit alors de trouver un élément h d'ordre $p-1$ dans $(\mathbb{Z}/p^n)^\times$: en effet, puisque $(|S_p|, \langle h \rangle) = (p^{n-1}, p - 1) = 1$, $S_p \times \langle h \rangle$ est un sous-groupe cyclique[4] d'ordre $p^{n-1}(p - 1)$ de $(\mathbb{Z}/p^n)^\times$. Mais $|(\mathbb{Z}/p^n)^\times| = p^{n-1}(p - 1)$, par conséquent, $(\mathbb{Z}/p^n)^\times = S_p \times \langle h \rangle$ et donc, $(\mathbb{Z}/p^n)^\times$ est cyclique.
Montrons alors qu'il existe un élément d'ordre $p - 1$ dans $(\mathbb{Z}/p^n)^\times$. Soit $i \in \mathbb{N}$ tel que $(i, p) = 1$. Alors $(i^{p-1}, p^n) = 1$ et donc, par l'exercice 1, $i^{p-1} + p^n \in (\mathbb{Z}/p^n)^\times$. Comme $|i^{p-1} + p^n\mathbb{Z}|$ divise $p^{n-1}p - 1$, $|i^{p-1} + p^n\mathbb{Z}| = p^k$ pour un certain $k \in \{0, \ldots, n - 1\}$. Il suit alors

$$(i^{p^k} + p^n\mathbb{Z})^{p-1} = i^{p^k(p-1)} + p^n\mathbb{Z} = (i^{p-1} + p^n\mathbb{Z})^{p^k} = 1 + p^n\mathbb{Z}.$$

Donc, $i^{p^k} + p^n\mathbb{Z}$ est d'ordre $p - 1$.
(b) Comme $|(\mathbb{Z}/2)^\times| = \varphi(2) = 2^0(2-1) = 1$ et $|(\mathbb{Z}/2^2)^\times| = \varphi(2^2) = 2^1(2-1) = 2$, $(\mathbb{Z}/2)^\times$ et $(\mathbb{Z}/2^2)^\times$ sont cycliques.

[4]rappelons que si G, H sont deux groupes cycliques finis tels que $(|G|, |H|) = 1$ alors $G \times H$ est cyclique (exercice I 8.5).

(c) Voir Abstract Algebra, David S. Dummit and Richard M. Foote.

Exercice 5. (a) Comme $g_p(x) = x^{p-1} + \cdots + 1$ et $x^{p^{k-1}} - 1 = \prod_{\substack{d|p^k \\ d<p^k}} g_d$,

$$\begin{aligned} g_{p^k}(x) &= \frac{x^{p^k}-1}{\prod_{\substack{d|p^k \\ d<p^k}} g_d} = \frac{(x^{p^{k-1}})^p - 1}{(x^{p^{k-1}}-1)} \\ &= \frac{(x^{p^{k-1}}-1)((x^{p^{k-1}})^{p-1} + \cdots + 1)}{(x^{p^{k-1}}-1)} \\ &= (x^{p^{k-1}})^{p-1} + \cdots + 1 \\ &= g_p(x^{p^{k-1}}). \end{aligned}$$

(e) Rappelons que $\sum_{d|n} \mu(d) = 0$ si $n > 1$ et $\mu(1) = 1$. Alors,

$$\begin{aligned} \prod_{d|n}(x^{n/d}-1)^{\mu(d)} &= \prod_{d|n}\left(\prod_{e|\frac{n}{d}} g_e(x)\right)^{\mu(d)} \\ &= \prod_{e|n} g_e(x)^{\sum\limits_{\substack{d|n \\ e|\frac{n}{d}}} \mu(d)} \\ &= \prod_{e|n} g_e(x)^{\sum\limits_{d|\frac{n}{e}} \mu(d)} \\ &= \prod_{\substack{e|n \\ e\neq n}} g_e(x)^{\sum\limits_{d|\frac{n}{e}} \mu(d)} g_n(x)^{\mu(1)} \\ &= \prod_{\substack{e|n \\ e\neq n}} g_e(x)^0 g_n(x) \\ &= g_n(x). \end{aligned}$$

(b) Soit $n = p_1^{k_1} \cdots p_r^{k_r}$. Puisque $\mu(d) = 0$ si p^2 divise d pour un certain naturel

premier p,

$$\begin{aligned} g_n(x) &= g_{p_1^{k_1}\cdots p_r^{k_r}}(x) \\ &= \prod_{d|p_1^{k_1}\cdots p_r^{k_r}} (x^{p_1^{k_1}\cdots p_r^{k_r}/d} - 1)^{\mu(d)} \\ &= \prod_{d|p_1\cdots p_r} ((x^{p_1^{k_1-1}\cdots p_r^{k_r-1}})^{p_1\cdots p_r/d} - 1)^{\mu(d)} \\ &= g_{p_1\cdots p_r}(x^{p_1^{k_1-1}\cdots p_r^{k_r-1}}). \end{aligned}$$

(c) Rappelons que $\mu(pd) = -\mu(d)$ lorsque p est un naturel premier, $\mu(d) = 0$ si p^2 divise d et $\sum_{d|n} \mu(d) = 0$ si $n > 1$. Notons aussi que $(x^{2n/d} - 1)^{\mu(d)}((x^{n/d} - 1)^{-\mu(d)} = (x^{n/d} + 1)^{\mu(d)}$. Aussi, comme n est impair et $n > 2$, n/d est impair lorsque d divise n et donc, $-x^{n/d} = (-x)^{n/d}$. Par conséquent,

$$\begin{aligned} g_{2n}(x) &= \prod_{d|2n}(x^{2n/d} - 1)^{\mu(d)} \\ &= \prod_{d|n}(x^{2n/d} - 1)^{\mu(d)} \prod_{2d|2n} (x^{2n/2d} - 1)^{\mu(2d)} \\ &= \prod_{d|n}(x^{2n/d} - 1)^{\mu(d)} \prod_{d|n}(x^{n/d} - 1)^{-\mu(d)} \\ &= \prod_{d|n}(x^{2n/d} - 1)^{\mu(d)}(x^{n/d} - 1)^{-\mu(d)} \\ &= \prod_{d|n}(x^{n/d} + 1)^{\mu(d)} \\ &= (-1)^{\sum_{d|n}\mu(d)} \prod_{d|n}(x^{n/d} + 1)^{\mu(d)} \\ &= \prod_{d|n}(-1)^{\mu(d)}(x^{n/d} + 1)^{\mu(d)} \\ &= \prod_{d|n}(-(x^{n/d} + 1))^{\mu(d)} \\ &= \prod_{d|n}((-x)^{n/d} - 1)^{\mu(d)} \\ &= g_n(-x). \end{aligned}$$

(d) Nous avons

$$\begin{aligned} g_{pn}(x) &= \prod_{d|pn}(x^{pn/d}-1)^{\mu(d)} \\ &= \prod_{d|n}(x^{pn/d}-1)^{\mu(d)} \prod_{pd|pn}(x^{pn/pd}-1)^{\mu(pd)} \\ &= \prod_{d|n}((x^p)^{n/d}-1)^{\mu(d)} \prod_{d|n}(x^{n/d}-1)^{-\mu(d)} \\ &= \prod_{d|n}((x^p)^{n/d}-1)^{\mu(d)} \left(\prod_{d|n}(x^{n/d}-1)^{\mu(d)}\right)^{-1} \\ &= g_n(x^p)/g_n(x). \end{aligned}$$

Exercice 6.

$$\begin{array}{ll} g_1(x) = x-1 & g_{11}(x) = x^{10}+\cdots+1 \\ g_2(x) = x+1 & g_{12}(x) = g_6(x^2) \\ g_3(x) = x^2+x+1 & g_{13}(x) = x^{12}+\cdots+1 \\ g_4(x) = g_2(x^2) = x^2+1 & g_{14}(x) = g_7(-x) \\ g_5(x) = x^4+x^3+x^2+x+1 & g_{15}(x) = g_3(x^5)/g_3(x) \\ g_6(x) = g_3(-x) = x^2-x+1 & g_{16}(x) = g_2(x^8) \\ g_7(x) = x^6+\cdots+1 & g_{17}(x) = x^{16}+\cdots+1 \\ g_8(x) = g_2(x^4) = x^4+1 & g_{18}(x) = g_9(-x) \\ g_9(x) = g_3(x^3) = x^6+x^3+1 & g_{19}(x) = x^{18}+\cdots+1 \\ g_{10}(x) = g_5(-x) = x^4-x^3+x^2-x+1 & g_{20}(x) = g_{10}(x^2). \end{array}$$

Exercice 7. Si $n = p_1^{n_1}\cdots p_r^{n_r}$, alors $\mathbb{Z}/n = \mathbb{Z}/p_1^{n_1} \times \cdots \times \mathbb{Z}/p_r^{n_r}$ en tant que groupe additif et donc,

$$\mathrm{Aut}_{\mathbb{Q}}F_n \cong (\mathbb{Z}/n)^\times = (\mathbb{Z}/p_1^{n_1})^\times \times \cdots \times (\mathbb{Z}/p_r^{n_r})^\times.$$

Exercice 8. (a) Calculons $\mathrm{Aut}_{\mathbb{Q}}F_5$. Soit ξ une racine primitive $5^{\text{ième}}$ de 1. Notons que le polynôme minimal de ξ sur $\mathbb{Q}$ est $g_5(x) = 1+x+\cdots+x^4$ car $g_5(x)$ est irréductible d'après la Proposition 8.3 et donc,

$$1+\xi+\xi^2+\xi^3+\xi^4 = 0.$$

Le Théorème 8.1 montre que $F_5 = \mathbb{Q}(\xi)$ est une extension cyclique, et la Proposition 8.3 implique que $\mathrm{Aut}_{\mathbb{Q}} F_5 \cong (\mathbb{Z}/5)^\times \cong \mathbb{Z}/4$. Ce groupe ne posséde qu'un seul sous-groupe propre et donc, il n'exixte qu'un seul corps intermédiaire entre $\mathbb{Q}$ et F_5. Considérons le $\mathbb{Q}$-automorphisme σ de F_5 tel que $\xi \mapsto \xi^2$. Alors $\sigma^4 = \mathrm{id}$ et

$$\mathrm{Aut}_{\mathbb{Q}} F_5 = \{\mathrm{id}, \sigma, \sigma^2, \sigma^3\}.$$

Le seul sous-groupe propre de $\mathrm{Aut}_{\mathbb{Q}} F_5$ est $\{\mathrm{id}, \sigma^2\}$ est. La correspondance de Galois entraîne alors que le seul corps intermédiaire entre $\mathbb{Q}$ et F_5 est

$$\{\mathrm{id}, \sigma^2\}' = \{x \in F_5 \mid \sigma^2(x) = x\}.$$

Exprimons $x = a + b\xi + c\xi^2 + d\xi^3 + e\xi^4$ dans la base $\{1, \xi, \xi^2, \xi^3, \xi^4\}$ de F_5 sur $\mathbb{Q}$. Alors de

$$\begin{aligned} a + b\xi + c\xi^2 + d\xi^3 + e\xi^4 &= \sigma^2(a + b\xi + c\xi^2 + d\xi^3 + e\xi^4) \\ &= a + b\xi^4 + c\xi^3 + d\xi^2 + e\xi \end{aligned}$$

on d'eduit que $b = e, c = d$ et donc,

$$\{\mathrm{id}, \sigma^2\}' = \{a + b(\xi + \xi^4) + c(\xi^2 + \xi^3) \mid a, b, c \in \mathbb{Q}\}.$$

Comme $\xi^2 + \xi^3 = -1 - (\xi + \xi^4)$,

$$\{\mathrm{id}, \sigma^2\}' = \{a + b(\xi + \xi^4) \mid a, b \in \mathbb{Q}\} = \mathbb{Q}(\xi + \xi^4) = \mathbb{Q}(\xi + \xi^{-1}).$$

Autre solution: Puisque $\mathrm{Aut}_{\mathbb{Q}} F_5 \cong (\mathbb{F}_5)^\times \cong \mathbb{Z}/4$, $\mathrm{Aut}_{\mathbb{Q}} F_5$ ne possède qu'un seul sous-groupe propre et donc, par la correspondance de Galois, il n'y a qu'un seul corps intermédiaire entre $\mathbb{Q}$ et F_5. Notons que $\mathbb{Q} \subsetneq \mathbb{Q}(\xi + \xi^4)$ car sinon $\xi^2 + \xi^3 = -1 - (\xi + \xi^4) \in \mathbb{Q}$ et donc, ξ serait une racine d'un polynôme de degré trois sur $\mathbb{Q}$, ce qui est faux. D'autre part, $\mathbb{Q}(\xi + \xi^4) \subsetneq F_5$ puisque $\xi \in \mathbb{C} \setminus \mathbb{R}$ et $\xi + \xi^4 = \xi + \xi^{-1}\xi + \overline{\xi} \in \mathbb{R}$ car ξ est de module 1. Par conséquent,

$$\mathbb{Q}(\xi + \xi^4) = \mathbb{Q}(\xi + \overline{\xi}) = \mathbb{Q}(\xi + \xi^{-1})$$

est le corps intermédiaire recherché.

(b) Par la Proposition 8.3, $\mathrm{Aut}_{\mathbb{Q}} F_8 \cong (\mathbb{Z}/8)^\times \cong \mathbb{Z}/2 \oplus \mathbb{Z}/2$ d'après l'exercice 4. Comme $\mathbb{Z}/2 \oplus \mathbb{Z}/2$ possède trois sous-groupes propres (tous d'ordre 2), il existe trois corps intermédiaire entre $\mathbb{Q}$ et F_8. Les racines de

$$x^8 - 1 = g_1(x)g_2(x)g_4(x)g_8(x) = (x-1)(x+1)(x^2+1)(x^4+1)$$

sont

$$\pm 1, \pm i, \sqrt{2}/2 \pm i\sqrt{2}/2, -\sqrt{2}/2 \pm i\sqrt{2}/2.$$

Alors $F_8 = \mathbb{Q}(i, \sqrt{2})$. Considérons les $\mathbb{Q}$-automorphismes σ, δ de F_8 tels que $\sigma(\sqrt{2}) = -\sqrt{2}$, $\sigma(i) = i$ et $\delta(\sqrt{2}) = \sqrt{2}, \delta(i) = -i$. On vérifie que $\sigma^2 = \delta^2 = \mathrm{id}$ et que $\langle \sigma, \delta \rangle$ est d'ordre 4 et donc,

$$\mathrm{Aut}_{\mathbb{Q}} F_8 = \{\mathrm{id}, \sigma, \delta, \sigma\delta\}.$$

Les trois sous-groupes de $\mathrm{Aut}_{\mathbb{Q}} F_8$ sont

$$\{\mathrm{id}, \sigma\}, \{\mathrm{id}, \delta\}\{\mathrm{id}, \sigma\delta\}.$$

Un calcul similaire à celui fait au point (a) montre alors que

$$\begin{aligned} \{\mathrm{id}, \sigma\}' &= \mathbb{Q}(i), \\ \{\mathrm{id}, \delta\}' &= \mathbb{Q}(\sqrt{2}), \\ \{\mathrm{id}, \sigma\delta\}' &= \mathbb{Q}(\sqrt{2}i). \end{aligned}$$

(c) Nous savons que $\mathrm{Aut}_{\mathbb{Q}} F_7 \cong (\mathbb{F}_7)^\times \cong \mathbb{Z}/6$ (Proposition 8.3) et donc, il n'existe que deux sous-groupes propres de $\mathrm{Aut}_{\mathbb{Q}} F_7$, l'un d'ordre 2 et l'autre d'ordre 3. Le $\mathbb{Q}$-automorphisme σ de F_7 défini par $\xi \mapsto \xi^5$ est d'ordre 6 et donc,

$$\mathrm{Aut}_{\mathbb{Q}} F_7 = \{\mathrm{id}, \sigma, \ldots, \sigma^5\}.$$

Ses sous-groupes d'ordre 2 et 3 sont respectivement $\{\mathrm{id}, \sigma^3\}$ et $\{\mathrm{id}, \sigma^2, \sigma^4\}$. On montre alors que

$$\begin{aligned} \{\mathrm{id}, \sigma^3\}' &= \mathbb{Q}(\xi + \xi^{-1}), \\ \{\mathrm{id}, \sigma^2, \sigma^4\}' &= \mathbb{Q}(\xi + \xi^2 + \xi^4). \end{aligned}$$

Exercice 9. Rappelons que $F_n = \mathbb{Q}(\xi)$ et que $[\mathbb{Q}(\xi) : \mathbb{Q}] = \varphi(n)$ d'après la Proposition 8.3. Comme $\xi \in \mathbb{C}\backslash\mathbb{R}$ et $\overline{\xi} = \xi^{-1}$ car ξ est de module 1, $\xi + \xi^{-1} \in \mathbb{R}$ et donc,

$$[\mathbb{Q}(\xi) : \mathbb{Q}(\xi + \xi^{-1})] > 1.$$

Puisque ξ est une racine de $x^2 - (\xi + \xi^{-1})x + 1 \in \mathbb{Q}(\xi + \xi^{-1})$,

$$[\mathbb{Q}(\xi) : \mathbb{Q}(\xi + \xi^{-1})] = 2.$$

Dès lors, de la chaîne $\mathbb{Q} \subset \mathbb{Q}(\xi + \xi^{-1}) \subset \mathbb{Q}(\xi)$, on déduit que

$$[\mathbb{Q}(\xi + \xi^{-1}) : \mathbb{Q}] = [\mathbb{Q}(\xi) : \mathbb{Q}]/[\mathbb{Q}(\xi) : \mathbb{Q}(\xi + \xi^{-1})] = \varphi(n)/2.$$

9. Extensions radicales

Exercice 1. Soient $u_1, \ldots, u_n \in F$ tels que $F = K(u_1, \ldots, u_n)$ avec $u_1^{k_1} \in K$ et pour tout $i > 1$, $u_i^{k_i} \in K(u_1, \ldots, u_{i-1})$. Comme $K \subset E$, $F = E(u_1, \ldots, u_n)$. De plus, $u_1^{k_1} \in K \subset E$ et pour tout $i > 1$, $u_i^{k_i} \in K(u_1, \ldots, u_{i-1}) \subset E(u_1, \ldots, u_{i-1})$, ce qui montre que F est une extension radicale de E.

Exercice 3. (a) Si $K(u)$ est Galois sur K alors $K(u)$ est un corps de rupture sur K. Comme f est le polynôme minimal de u sur K, $K(u)$ contiendrait toutes les racines de f et donc $F \subset K(u)$. Ceci entraîne la contradiction suivante:

$$n! = |S_n| = |\mathrm{Aut}_K F| = [F : K] < [K(u) : K] = n.$$

Montrons que $\mathrm{Aut}_K K(u) = \{\mathrm{id}\}$. Si $K(u)$ contient une autre racine v de f alors $f = (x - v)(x - u)g(x)$ avex $g(x) \in K(u)[x]$. Il est clair que F est un corps de rupture de $g(x)$ sur $K(u)$. De l'exercice 3.5, on déduit alors que $[F : K(u)] \mid \deg g! = (n - 2)!$. Mais alors

$$n! = [F : K] = [F : K(u)][K(u) : K] \leq (n - 2)!n < n!.$$

Donc, u est la seule racine de f dans $K(u)$, ce qui implique que $\mathrm{Aut}_K K(u) = \{\mathrm{id}\}$.
(b) Une clôture normale N de K contenant u contient toutes les racines de f par définition et donc, elle contient un corps de rupture E de f sur K. Comme $E \cong F$ (Corollair 3.9), N contient une copie de F.
(c) Supposons qu'il existe une extension radicale E de K telle que $K \subset K(u) \subset E$. Soit alors N une clôture normale de E sur K, N existe d'après le Théorème 3.16. Par (b), N contient une copie L de F et par le Lemme 9.3, N est une extension radicale de K. Le Théorème 9.4 montre alors que

$$\mathrm{Aut}_K L \cong \mathrm{Aut}_K F \cong S_n$$

est un groupe résoluble, ce qui est impossible pour $n \geq 5$.

Exercice 4. Soient $v_1, \ldots, v_n, w_1, \ldots, w_m \in F$ et $k_1, \ldots, k_n, \ell_1, \ldots, \ell_m \in \mathbb{N}$ tels que $F = E(v_1, \ldots, v_n)$, $E = K(w_1, \ldots, w_m)$, $v_1^{k_1} \in E$, $w_1^{\ell_1} \in K$, et $\forall i \in \{1, \ldots, n\}$, $\forall j \in \{1, \ldots, m\}$, $v_i^{k_i} \in E(v_1, \ldots, v_{i-1})$ et $w_j^{\ell_j} \in K(w_1, \ldots, w_{j-1})$. Alors $F = K(v_1, \ldots, v_n, w_1, \ldots, w_m)$. Posons $u_1 = w_1, \ldots, u_m = w_m, u_{m+1} = v_1, \ldots, u_{m+n} = v_n$ et $n_1 = \ell_1, \ldots, n_m = \ell_m, n_{m+1} = k_1, \ldots, n_{m+n} = k_n$. On

vérifie que $u_1^{n_1} \in K$ et $\forall i \in \{1, \ldots, m+n\}$, $u_i^{k_i} \in K(u_1, \ldots, u_{i-1})$. Donc, F est une extension radicale de K.