Extensions de corps I : correction

Exercice 1. Si $e+\pi$ et $e\pi$ étaient algébriques sur $\mathbf{Q}$, les réels e et π, racines du polynôme $\mathrm{X}^2-(e+\pi)\mathrm{X}+e\pi$, seraient algébriques sur $\overline{\mathbf{Q}}$. Ils seraient donc dans $\overline{\overline{\mathbf{Q}}}=\overline{\mathbf{Q}}$, c'est-à-dire algébriques sur $\mathbf{Q}$, ce qui contredirait les théorèmes de Hermite et Lindemann.

Exercice 2.

1. Soit $\mathrm{L}/\mathbf{F}_p$ une extension telle que $|\mathrm{L}|=q$. Puisque $|\mathrm{L}^\times|=q-1$, on a d'après le théorème de Lagrange $\forall x\in\mathrm{L}^\times, x^{q-1}=1$ et donc $\forall x\in\mathrm{L}, x^q=x$. Le polynôme $\mathrm{X}^q-\mathrm{X}$ est donc scindé sur L : $\mathrm{X}^q-\mathrm{X}=\prod_{a\in\mathrm{L}}(\mathrm{X}-a)$. En outre, L est évidemment engendré par les racines de $\mathrm{X}^q-\mathrm{X}$, qui sont exactement les éléments de L. Le corps L est donc bien un corps de décomposition de $\mathrm{X}^q-\mathrm{X}$.
2. Réciproquement, soit L un corps de décomposition de $\mathrm{X}^q-\mathrm{X}\in\mathbf{F}_p[\mathrm{X}]$. On y a donc $\mathrm{X}^q-\mathrm{X}=\prod_{i=1}^q(\mathrm{X}-a_i)$ et L est engendré par les $a_1,\dots,a_q$. Mais l'ensemble
$$\mathrm{E}=\{a_i\,|\,1\leq i\leq q\}.$$
est l'ensemble des $x\in\mathrm{L}$ tels que $x^q=q$. Puisque $x\mapsto x^q$ est un morphisme de corps de L dans L (c'est une puissance du morphisme de Frobenius), l'ensemble E est un sous-corps de L. Comme par hypothèse L est engendré par E, on a bien $\mathrm{L}=\mathrm{E}$, et L est un corps de cardinal q.

Exercice 3.

1. Le critère d'Eisenstein pour $p=2$ implique que le polynôme X^3-2 est irréductible sur $\mathbf{Z}$ et donc sur $\mathbf{Q}$. Le corps $\mathbf{Q}(\sqrt[3]{2})$ est bien un corps de rupture pour ce polynôme. Ce n'est pas un corps de décomposition pour X^3-2 car les autres racines (dans $\mathbf{C}$) de ce polynôme, $\zeta_3\sqrt[3]{2}$ et $\zeta_3^2\sqrt[3]{2}$, ne sont pas réelles et donc pas dans $\mathbf{Q}(\sqrt[3]{2})$. Un corps de décomposition pour ce polynôme est donc $\mathbf{Q}(\sqrt[3]{2},\zeta_3\sqrt[3]{2},\zeta_3^2\sqrt[3]{2})$ et il s'agit de montrer que ce corps coïncide avec $\mathbf{Q}(\sqrt[3]{2},\zeta_3)$. L'inclusion $\mathbf{Q}(\sqrt[3]{2},\zeta_3\sqrt[3]{2},\zeta_3^2\sqrt[3]{2})\subset\mathbf{Q}(\sqrt[3]{2},\zeta_3)$ est claire ; l'inclusion réciproque vient simplement du fait que $\zeta_3=(\zeta_3^2\sqrt[3]{2})/(\zeta_3\sqrt[3]{2})$.
2. Le corps $\mathbf{Q}(\zeta_n)$ est clairement un corps de rupture du polynôme (irréductible d'après le cours) $\Phi_n\in\mathbf{Q}[\mathrm{X}]$. C'en est également un corps de décomposition car les racines de Φ_n sont exactement les ζ_n^k pour $1\leq k<n$ premier avec n, qui sont bien dans le corps $\mathbf{Q}(\zeta_n)$. Ce corps est appelé n-ième *corps cyclotomique*.

Exercice 4.

1. (a) Soit $\mathrm{P}\in\mathrm{K}[\mathrm{X}]$ un polynôme unitaire de degré 2. On peut l'écrire $\mathrm{P}=\mathrm{X}^2-p_1\mathrm{X}+p_2$ avec p_1, $p_2\in\mathrm{K}$. En posant $a=p_1/2$ et $b=p_1^2/4-p_2$ (ce qui est licite car K n'est pas de caractéristique 2), on a bien $\mathrm{P}=(\mathrm{X}-a)^2+b$.
   (b) Soit $\widetilde{\alpha}\in\mathrm{L}\setminus\mathrm{K}$. La famille $(1,\widetilde{\alpha})$ est donc une famille K-libre de L. C'en est donc une base. On peut ainsi écrire $\widetilde{\alpha}^2=\mu\widetilde{\alpha}+\lambda$ pour un certain couple $(\lambda,\mu)\in\mathrm{K}^2$. Le polynôme minimal de $\widetilde{\alpha}$ est alors $\mu_{\mathrm{K}}^{\widetilde{\alpha}}(\mathrm{X})=\mathrm{X}^2-\mu\mathrm{X}-\lambda$ (ce polynôme est en effet annulateur, et il est clairement de degré minimal pour cette propriété). D'après la question précédente, il existe a et b dans K tels que $\mu_{\mathrm{K}}^{\widetilde{\alpha}}(\mathrm{X})=(\mathrm{X}-a)^2-b$. Soit $\alpha=\widetilde{\alpha}-a$. On a évidemment $\mathbf{Q}(\alpha)=\mathbf{Q}(\widetilde{\alpha})=\mathrm{L}$, et $\alpha^2=(\widetilde{\alpha}-a)^2=b\in\mathrm{K}$.

(c) Soit $\beta \in \mathrm{L}$ tel que $\mathrm{L} = \mathbf{Q}(\beta)$ et $\beta^2 \in \mathrm{K}$. On peut alors écrire $\beta = \lambda\alpha + \mu$, pour $(\lambda, \mu) \in \mathrm{K}^2$. On obtient alors $\beta^2 = (\lambda^2\alpha^2 + \mu)^2 + 2\lambda\mu\alpha$. L'hypothèse $\beta^2 \in \mathrm{K}$ entraîne donc que $\lambda = 0$ ou que $\mu = 0$. Mais le premier cas est impossible car il entraînerait $\beta \in \mathrm{K}$; on a donc $\mu = 0$, c'est-à-dire que $\beta/\alpha \in \mathrm{K}$.

2. (a) L'extension $\mathbf{Q}(\sqrt{p})/\mathbf{Q}$ est de degré 2. Le réel $\sqrt{q}$ est une racine de $\mathrm{X}^2 - q \in \mathbf{Q}(\sqrt{p})[\mathrm{X}]$. On a donc $[\mathbf{Q}(\sqrt{p}, \sqrt{q}) : \mathbf{Q}(\sqrt{p})] \leq 2$. Plus précisément, soit $\sqrt{q} \in \mathbf{Q}(\sqrt{p})$, soit $[\mathbf{Q}(\sqrt{p}, \sqrt{q}) : \mathbf{Q}(\sqrt{p})] = 2$. Mais le premier cas est impossible : il entraînerait $\mathbf{Q}(\sqrt{p}) = \mathbf{Q}(\sqrt{q})$ et, d'après la question précédente, $\sqrt{p/q} \in \mathbf{Q}$, ce qui n'est pas (par exemple, si p/q était le carré d'un rationnel, sa valuation p-adique serait paire). On a donc bien $[\mathbf{Q}(\sqrt{p}, \sqrt{q}) : \mathbf{Q}(\sqrt{p})] = 2$. La formule de multiplicativité des degrés entraîne donc que $\mathbf{Q}(\sqrt{p}, \sqrt{q})/\mathbf{Q}$ est de degré 4.

(b) Soit $\beta \in \mathbf{Q}(\sqrt{p}, \sqrt{q})$ tel que $\beta^2 \in \mathbf{Q}$. Si $\beta \in \mathbf{Q}(\sqrt{p})$, la question 1.(c) appliquée à l'extension $\mathbf{Q}(\sqrt{p})/\mathbf{Q}$ entraîne $\beta \in \mathbf{Q}$ ou $\beta/\sqrt{p} \in \mathbf{Q}$. Dans le cas contraire, la même question appliquée à $\mathbf{Q}(\sqrt{p}, \sqrt{q})/\mathbf{Q}(\sqrt{p})$ entraîne que $\beta/\sqrt{q} \in \mathbf{Q}(\sqrt{p})$. On obtient donc (car $(\beta/\sqrt{q})^2 \in \mathbf{Q}$) que $\beta/\sqrt{q}$ est un multiple rationnel de 1 ou $\sqrt{p}$.

(c) D'après la formule de multiplicativité des degrés, une sous-extension $\mathbf{Q} \subset \mathrm{K} \subset \mathrm{Q}(\sqrt{p}, \sqrt{q})$ est de degré 1, 2 ou 4. Évidemment, la seule sous-extension de degré 1 est $\mathbf{Q}/\mathbf{Q}$ et la seule de degré 4 est $\mathbf{Q}(\sqrt{p}, \sqrt{q})/\mathbf{Q}$. Si le degré est 2, la première partie entraîne l'existence de $\beta \in \mathbf{Q}(\sqrt{p}, \sqrt{q})$ tel que $\mathrm{K} = \mathbf{Q}(\beta)$ et $\beta^2 \in \mathrm{K}$. D'après la première question, β est un multiple rationnel de $\sqrt{p}$, $\sqrt{q}$ ou $\sqrt{pq}$ (le cas $\beta \in \mathbf{Q}$ est exclu car il entraînerait $[\mathbf{Q}(\beta) : \mathbf{Q}] = 1$). Les sous-extensions de degré 2 sont donc $\mathbf{Q}(\sqrt{p})/\mathbf{Q}$, $\mathbf{Q}(\sqrt{q})/\mathbf{Q}$ et $\mathbf{Q}(\sqrt{pq})/\mathbf{Q}$.

(d) $(\sqrt{p} + \sqrt{q})^2 = p + q + 2\sqrt{pq}$ donc $\sqrt{p} + \sqrt{q}$ annule $\mathrm{P} = (\mathrm{X}^2 - (p+q))^2 - 4pq = \mathrm{X}^4 - 2(p+q)\mathrm{X}^2 + (p-q)^2$. D'après la preuve de la formule de multiplicativité des degrés, la famille $(1, \sqrt{p}, \sqrt{q}, \sqrt{pq})$ est une $\mathbf{Q}$-base de $\mathbf{Q}(\sqrt{p}, \sqrt{q})$. Cette base est en outre adaptée aux trois sous-extensions quadratiques de $\mathbf{Q}(\sqrt{p}, \sqrt{q})$:

$$\mathbf{Q}(\sqrt{p}) = \mathrm{Vect}_{\mathbf{Q}}(1, \sqrt{p}) \qquad \mathbf{Q}(\sqrt{q}) = \mathrm{Vect}_{\mathbf{Q}}(1, \sqrt{q}) \qquad \mathbf{Q}(\sqrt{pq}) = \mathrm{Vect}_{\mathbf{Q}}(1, \sqrt{pq}).$$

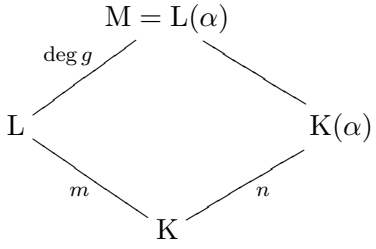
L'élément $\sqrt{p} + \sqrt{q}$ n'appartient donc à aucune de ces extensions quadratiques, ce qui entraîne $\mathbf{Q}(\sqrt{p} + \sqrt{q}) = \mathbf{Q}(\sqrt{p}, \sqrt{q})$. Cela entraîne que $\deg \mu_{\mathbf{Q}}^{\sqrt{p}+\sqrt{q}} = [\mathbf{Q}(\sqrt{p} + \sqrt{q}) : \mathbf{Q}] = 4$. On a donc $\mu_{\mathbf{Q}}^{\sqrt{p}+\sqrt{q}} = \mathrm{P} = \mathrm{X}^4 - 2(p+q)\mathrm{X}^2 + (p-q)^2$.

Exercice 5.

Soit $g \in \mathrm{L}[\mathrm{X}]$ un facteur irréductible de $f \in \mathrm{L}[\mathrm{X}]$ et M/L un corps de rupture de g sur L : on a $\mathrm{M} = \mathrm{L}(\alpha)$ et $g(\alpha) = 0$. Le corps $\mathrm{K}(\alpha)$ est alors un corps de rupture de f sur K. D'après la formule de multiplicativité des degrés, on a :

$$[\mathrm{M} : \mathrm{K}] = [\mathrm{M} : \mathrm{K}(\alpha)] \cdot \underbrace{[\mathrm{K}(\alpha) : \mathrm{K}]}_{=n} = \underbrace{[\mathrm{M} : \mathrm{L}]}_{=\deg g} \cdot \underbrace{[\mathrm{L} : \mathrm{K}]}_{=m}.$$

Le degré $[\mathrm{M} : \mathrm{K}]$ est donc un multiple à la fois de n et m. Puisque ces nombres sont premiers entre eux, il est divisible par leur produit mn. Mais $[\mathrm{M}, \mathrm{K}] = m \deg g$ et $\deg g \leq \deg f = n$. On a donc $\deg = n$ et $g = f$; f est irréductible sur $\mathrm{L}[\mathrm{X}]$.



Exercice 6.

1. Si K est un corps fini, L également. Son groupe multiplicatif est donc cyclique. Soit $\theta \in \mathrm{L}^\times$ générateur. On a alors évidemment $\mathrm{L} = \mathrm{K}(\theta)$.
2. L'existence de $\lambda \in \mathrm{F} \setminus \mathrm{S}$ est garantie car F est infini et S fini. Évidemment, on a pour tout $\lambda \in \mathrm{F}$, $\mathrm{F}(\alpha + \lambda\beta) \subset \mathrm{F}(\alpha, \beta)$. Pour avoir l'inclusion réciproque, il suffit d'avoir $\beta \in (\alpha + \lambda\beta)$. Nous allons montrer $\beta \notin \mathrm{F}(\alpha + \lambda\beta) \Rightarrow \lambda \in \mathrm{S}$. Supposons donc $\beta \notin \mathrm{F}(\gamma)$, avec $\gamma = \alpha + \lambda\beta$. Cela implique $\deg \mu^\beta_{\mathrm{F}(\gamma)} \geq 2$. Mais β est une racine commune à $\mu^\beta_{\mathrm{F}}(\mathrm{X}) \in \mathrm{F}[\mathrm{X}] \subset \mathrm{F}(\gamma)[\mathrm{X}]$ et $\mu^\alpha_{\mathrm{F}}(\gamma - \lambda\mathrm{X}) \in \mathrm{F}(\gamma)[\mathrm{X}]$. Son polynôme minimal $\mu^\beta_{\mathrm{F}(\gamma)}$ divise donc $\mathrm{pgcd}_{\mathrm{F}(\gamma)}(\mu^\beta_{\mathrm{F}}, \mu^\alpha_{\mathrm{F}}(\gamma - \lambda\mathrm{X}))$, qui est donc également de degré ≥ 2. Par hypothèse, L/F est séparable. Le polynôme irréductible μ^β_{F} a donc une racine $\beta' \neq \beta$. Si $\lambda \neq 0$, l'élément $\alpha' = \gamma - \lambda\beta' \neq \alpha$ est donc une racine $\neq \alpha$ de μ^α_{F} et $\lambda = (\alpha' - \alpha)/(\beta - \beta') \in \mathrm{S}$.
3. Si L/K est une extension séparable et finie, $\mathrm{L} = \mathrm{K}(\alpha_1, \ldots, \alpha_t)$ et chaque extension intermédiaire $\mathrm{K}(\alpha_1, \ldots, \alpha_r)/\mathrm{K}$ est séparable. En appliquant par récurrence la question précédente, on peut donc trouver $\theta \in \mathrm{L}$ tel que $\mathrm{L} = \mathrm{K}(\theta)$.
4. Si K est parfait, toute extension est séparable. La question précédente montre donc que toute extension finie de K est monogène.
5. Tout élément $\alpha \in \mathrm{L} = \mathrm{K}(\sqrt[p]{\mathrm{T}}, \sqrt[p]{\mathrm{U}})$ s'écrit $\alpha = f(\sqrt[p]{\mathrm{T}}, \sqrt[p]{\mathrm{U}})$, avec $f(\mathrm{X}, \mathrm{Y}) \in \mathrm{K}(\mathrm{X}, \mathrm{Y})$. Comme $x \mapsto x^p$ est un morphisme de corps, on a

$$\alpha^p = f(\sqrt[p]{\mathrm{T}}, \sqrt[p]{\mathrm{U}})^p = f((\sqrt[p]{\mathrm{T}})^p, (\sqrt[p]{\mathrm{U}})^p) = f(\mathrm{T}, \mathrm{U}) \in \mathbf{F}_p(\mathrm{T}, \mathrm{U}) = \mathrm{K}.$$

Cette propriété entraîne que toute extension monogène $\mathrm{K}(\alpha) \subset \mathrm{L}$ est de degré 1 ou p. Or, la formule de multiplicativité des degrés entraîne facilement que $[\mathrm{L} : \mathrm{K}] = p^2$. En particulier, L ne s'écrit $\mathrm{K}(\alpha)$ pour aucun élément $\alpha \in \mathrm{L}$.

Exercice 7. Supposons P irréductible. P est alors le polynôme minimal de chacune de ses racines, qui sont donc dans K_d, et vérifient $x^{q^d} = x$. Donc P divise $\mathrm{X}^{q^d} - \mathrm{X}$. Si P n'était pas premier à $\mathrm{X}^{q^{\frac{d}{p}}} - \mathrm{X}$, pour p facteur premier de d, alors ces deux polynômes auraient une racine en commun, qui serait alors dans $\mathrm{K}_{\frac{d}{p}}$. Une telle racine aurait alors un degré divisant $\frac{d}{p}$, ce qui est impossible puisqu'on vient de dire que toutes les racines de P étaient de degré d.
Inversement, supposons que P vérifie les deux critères. Alors, puisque P divise $\mathrm{X}^{q^d} - \mathrm{X}$, toutes ses racines (dans $\overline{\mathrm{K}}$) sont dans K_d. On sait que les extensions intermédiaires de K_d/K sont précisément les K_n/K, pour n divisant d. Si P avait une racine dans une extension de K de degré inférieur ou égal à $d/2$, cette racine serait donc nécessairement dans un $\mathrm{K}_{\frac{d}{p}}$, pour p divisant d. Mais alors P et $\mathrm{X}^{q^{\frac{d}{p}}} - \mathrm{X}$ auraient une racine commune et donc un pgcd non trivial, ce qui est contraire aux hypothèses. Donc P n'a de racines dans aucune extension de degré plus petit que $d/2$, et donc est irréductible.

Exercice 8.

1. Soit $c_1, \ldots, c_n \in \mathrm{M}$ tels que $c_1\chi_1 + \cdots + c_n\chi_n = 0$ et qu'il n'existe aucune relation de liaison plus courte. En particulier, on a donc $n \geq 2$ et aucun c_i n'est nul. Puisque $\chi_1 \neq \chi_2$, on peut trouver $g_0 \in \mathrm{G}$ tel que $\chi_1(g_0) \neq \chi_2(g_0)$. On a alors

$$\begin{cases} \forall g \in \mathrm{G}, & c_1\chi_1(g) + c_2\chi_2(g) + \cdots + c_n(g)\chi_n(g) &= 0 \\ \forall g \in \mathrm{G}, & c_1\chi_1(g_0)\chi_1(g) + c_2\chi_2(g_0)\chi_2(g) + \cdots + c_n(g)\chi_n(g_0)\chi_n(g) &= 0. \end{cases}$$

On obtient donc une relation plus courte

$$c_2\left(\frac{\chi_2(g_0)}{\chi_1(g_0)}-1\right)\chi_2+\cdots+c_n\left(\frac{\chi_n(g_0)}{\chi_1(g_0)}-1\right)\chi_n=0,$$

ce qui contitue une contradiction.

2. Un plongement $\mathrm{L}\to\mathrm{M}$ induit par restriction un morphisme de groupes $\mathrm{L}^\times\to\mathrm{M}^\times$. Le résultat précédent montre donc leur indépendance linéaire.
3. Sous les hypothèses de l'énoncé (en supposant les α_i distincts), les applications $k\mapsto\alpha_i^k$ sont des caractères $\mathbf{N}\to\mathrm{M}^\times$ différents donc ils sont linéairement indépendants.