Extensions de corps

I. Extensions de corps, [Perrin], [Chambert-Loir]

Exercice 1. — Montrer qu'un morphisme de corps est toujours injectif.

Exercice 2. — Montrer qu'on a l'égalité $\mathbf{Q}[\sqrt{2},\sqrt{3}] = \mathbf{Q}[\sqrt{2}+\sqrt{3}]$.

Exercice 3. — Soit k un corps et $P \in k[X]$ un polynôme.
Montrer que $K := k[X]/(P)$ est un corps ssi P est irréductible. Dans ce cas, comment calcule-t-on explicitement l'inverse d'un élément non nul ?

Exercice 4. — Soient K un corps et L une extension finie de K.

a) Soient x, y deux éléments de L. Montrer que x et y sont algébriques sur K.

On note Π_x, Π_y leurs polynômes minimaux respectifs.

b) Montrer que Π_x est irréductible sur $K(y)$ si et seulement si Π_y est irréductible sur $K(x)$.

Exercice 5. — Soient k un corps et $P \in k[X]$ un polynôme irréductible de degré n. Soit également K une extension finie de k de degré m.

a) Si $n \not| m$, montrer que P n'a pas de racines dans K.
Application : Montrer que $X^3 - 2 \in \mathbf{Q}[i][X]$ est irréductible.

b) Si m est premier à n, montrer que P est irréductible sur K.
Application : Montrer que $X^7 - 2 \in \mathbf{Q}[i][X]$ est irréductible.

Exercice 6. — Soit $P \in k[X]$ un polynôme de degré $n > 0$. Montrer que P est irréductible dans $k[X]$ ssi P n'a aucune racine dans toute extension $k \subset L$ de degré $[L : k] \leqslant \frac{n}{2}$.

Exercice 7. — **[Extensions de degré 2.]**
Soient K un corps de caractéristique différente de 2 et L une extension de K de degré 2.Montrer qu'il existe $x \in L \setminus K$ tel que $L = K(x)$ et $\alpha := x^2 \in K$.
Donner un exemple où ce n'est pas le cas en caractéristique 2.

Exercice 8. — **[Extensions de degré 3.]**
Soient K un corps, $P \in K[X]$ un polynôme unitaire de degré 3 et L un corps de décomposition de P.

a) Montrer que les seules valeurs possibles pour $[L : K]$ sont $1, 2, 3, 6$.

b) Montrer que P est irréductible ssi $[L : K] \in \{3, 6\}$.

c) Soit α, β, γ les trois racines de P dans L. Montrer que le discriminant de P, c'est-à-dire
$\Delta := (\alpha-\beta)^2(\beta-\gamma)^2(\gamma-\alpha)^2$ appartient à K.

d) Si P est irréductible, montrer que l'on a $[L : K] = 3$ ssi Δ est un carré dans K.
[**Indication:** Si Δ n'est pas un carré, noter que $[K[\sqrt{\Delta}] : K]$ divise $[L : K]$.]

e) Application : montrer qu'un polynôme $P \in \mathbf{R}[X]$ de degré 3 a toutes ses racines réelles ssi $\Delta(P) \geqslant 0$.

Exercice 9. — **[Théorème de Wantzel]**

a) Montrer que l'ensemble $\mathcal{C}$ des réels constructibles à la règle et au compas est un sous-corps de $\mathbf{R}$.

b) Montrer que si $x > 0$ et $x \in \mathcal{C}$, alors $\sqrt{x} \in \mathcal{C}$.

c) Montrer que si x est constructible, il existe une suite finie d'extensions $Q =: E_0 \subset E_1 \subset \dots E_n$ quadratiques (*i.e.* $[E_{i+1} : E_i] = 2$) telle que $x \in E_n$.

d) En utilisant l'Ex. **7**, montrer que la réciproque est vraie.

e) **Application :** Montrer que si $x \in \mathbf{R}$ est constructible, alors x est algébrique et de degré une puissance de 2. En déduire l'impossibilité de la quadrature du cercle et de la trisection de l'angle.

Exercice 10. — Montrer qu'une extension finie de $\mathbf{Q}$ ne contient qu'un nombre fini de racines de l'unité.

Exercice 11. — Pour $n \geqslant 1$ un entier, on note $\Phi_n = \sum_{k=0}^{\varphi(n)} a_k X^k$ le n-ème polynôme cyclotomique.

a) Rappeler la définition de Φ_n, déterminer son degré $\varphi(n)$ et montrer que $\Phi_n \in \mathbf{Z}[X]$.

b) Quel est le degré de l'extension $\mathbf{Q} \subset \mathbf{Q}[e^{\frac{2i\pi}{n}}]$?

c) Pour $n > 2$, montrer que le degré de l'extension $\mathbf{Q}[\cos(\frac{2\pi}{n})] \subset \mathbf{Q}[e^{\frac{2i\pi}{n}}]$ vaut 2.
[**Indication:** Noter que pour $n > 2$, $e^{\frac{2i\pi}{n}} \notin \mathbf{R}$.]

d) En déduire le degré de l'extension $\mathbf{Q} \subset \mathbf{Q}[\cos(\frac{2\pi}{n})]$ lorsque $n > 2$.
Cela montre en particulier que pour $n > 2$, $\varphi(n)$ est pair. Est-ce une surprise ?

e) En déduire que les seules valeurs entières de n telles que $\cos(\frac{2\pi}{n})$ soit rationnel sont $1, 2, 3, 4$ et 6.

f) De même, montrer qu'il n'y qu'un nombre fini d'entiers que l'on précisera tels que $\cos(\frac{2\pi}{n})$ s'écrive de la forme $a + b\sqrt{d}$, avec $a, b, d \in \mathbf{Q}$ et d non carré.

g) Étendre les résultats de **e)** et **f)** aux nombres $\cos(\frac{2k\pi}{n})$.

h) **Digression :** Montrer que pour $n \geqslant 2$, les coefficients a_k de Φ_n vérifient $a_{\varphi(n)-k} = a_k$.
[**Indication:** Comparer $\Phi_n(X)$ et $\Phi_n(\frac{1}{X})$. Attention au cas $n = 1$.]
Expliciter alors le polynôme minimal de $2\cos(\frac{2\pi}{n})$.

i) En notant que $\sin(\frac{2\pi}{n}) = \cos(\frac{\pi}{2} - \frac{2\pi}{n})$, montrer que $\sin(\frac{2\pi}{n})$ est algébrique de degré :

$$\begin{cases} \varphi(n) & \text{si } \operatorname{pgcd}(n,8) < 4 \\ \frac{\varphi(n)}{2} & \text{si } \operatorname{pgcd}(n,8) = 4 \\ \frac{\varphi(n)}{4} & \text{si } \operatorname{pgcd}(n,8) = 8 \end{cases}.$$

II. Corps finis, [Demazure]

Exercice 12. — Soit $\mathbf{F}_q$ un corps fini à $q := p^n$ éléments.

a) Quel est le groupe $(\mathbf{F}_q, +)$?

b) Quel est le groupe $(\mathbf{F}_q^\times, \times)$?

c) Pour $m \geqslant 1$, combien de racines m-ème de l'unité y a-t-il dans $\mathbf{F}_q$?

d) Combien y a-t-il de carrés dans $\mathbf{F}_q$? de cubes ?

Exercice 13. — Soit $q = p^n$ une puissance d'un nombre premier et $\mathbf{F}_q$ "le" corps à q éléments. Soit $A = X^{q-1} - 1 \in \mathbf{F}_q[X]$. En utilisant les relations coefficients racines pour le polynôme A, calculer $\prod_{\alpha \in \mathbf{F}_q^*} \alpha$ et $\sum_{\alpha \in \mathbf{F}_q} \alpha^2$.

Exercice 14. — Soit K un corps fini à p^m éléments.

a) Montrer que K admet un sous-corps à p^n éléments ssi $n|m$.
Dans ce cas, montrer que ce sous-corps à p^n éléments est unique.

b) Montrer que le polynôme $X^2 + X + 1$ est irréductible sur $\mathbf{F}_2$ et sur $\mathbf{F}_{32}$.

Exercice 15. — Soit $\mathbf{F}_q$ un corps fini et $M \in \mathrm{M}_n(\mathbf{F}_q)$. Montrer que M est diagonalisable ssi $M^q = M$.

Exercice 16. — Soient $A, B \in \mathrm{M}_n(\mathbf{Z})$ et p un nombre premier.

a) Montrer que l'on a la congruence $\mathrm{Tr}(A^p) \equiv \mathrm{Tr}(A)\ [p]$.
[**Indication:** Considérer la réduction $\overline{A} \in \mathrm{M}_n(\mathbf{F}_p)$ et commencer par traiter le cas où $\overline{A}$ est trigonalisable.]

b) En déduire que l'on a $\mathrm{Tr}(A + B)^p \equiv \mathrm{Tr}(A^p) + \mathrm{Tr}(B^p)\ [p]$.

Exercice 17. — Soit $\alpha := \sqrt{2} + \sqrt{3} \in \mathbf{R}$.

a) Montrer que α est algébrique de degré 4 sur $\mathbf{Q}$ et expliciter son polynôme minimal $P \in \mathbf{Z}[X]$.

b) Montrer que P a une racine dans tout corps k dans lequel 2 et 3 sont des carrés.

c) Pour tout premier p, montrer que tous les éléments de $\mathbf{F}_p$ sont des carrés dans $\mathbf{F}_{p^2}$.

d) En déduire que P est réductible sur $\mathbf{F}_p$ pour tout p.

Exercice 18. — Soit $n \geqslant 1$ et $P \in \mathbf{F}_p[X]$ un polynôme irréductible de degré n. On note K le corps fini $\mathbf{F}_p[X]/(P)$.

a) Soit $\varphi : K \to K$, $x \mapsto x^p$ le morphisme de Frobenius. Montrer que φ est un automorphisme de corps $\mathbf{F}_p$-linéaire et qu'il est d'ordre n.

b) En déduire que $\overline{P}$ a n racines distinctes dans K qui sont $\alpha := \overline{X}, \varphi(\alpha), \ldots, \varphi^{n-1}(\alpha)$.

Exercice 19. — Soit $q = p^n$ une puissance d'un nombre premier et $\mathbf{F}_q$ un corps à q éléments. Pour tout $\alpha \in \mathbf{F}_q$, on pose $\mathrm{Tr}(\alpha) = \sum_{i=0}^{n-1} \alpha^{p^i}$.

a) Montrer que Tr est une application linéaire à valeur dans le sous-corps $\mathbf{F}_p \subset \mathbf{F}_q$.

b) Montrer qu'il existe $\alpha \in \mathbf{F}_q$ tel que $\mathrm{Tr}(\alpha) \neq 0$.

c) Pour $\alpha \in \mathbf{F}_q$, montrer qu'on a $\mathrm{Tr}(\alpha) = 0$ ss'il existe $\beta \in \mathbf{F}_q$, tel que $\alpha = \beta^p - \beta$.
[**Indication:** Noter que $\mathbf{F}_q \to \mathbf{F}_q$, $\beta \mapsto \beta^p - \beta$ est linéaire. Quelle est la dimension de son image ?]

Exercice 20. — Soient P_1 et $P_2 \in \mathbf{F}_p[X]$ deux polynômes irréductibles de même degré $n \geqslant 1$. Comment explicite-t-on un isomorphisme entre les corps finis $\mathbf{F}_p[X]/(P_1)$ et $\mathbf{F}_p[X]/(P_2)$?
Application numérique : $P_1 = X^2 + X + 2$, $P_2 = X^2 + 2X + 2 \in \mathbf{F}_3[X]$.

Exercice 21. — Donner un sens à l'énoncé suivant : "Soit p un nombre premier. Montrer que $\bigcup_{n=0}^{+\infty} \mathbf{F}_{p^{n!}}$ est une clôture algébrique de $\mathbf{F}_p$".

Exercice 22. — Soit $P \in \mathbf{F}_p[X]$ un polynôme. Montrer que le nombre de racines distinctes de P dans $\mathbf{F}_p$ (sans compter les multiplicités) est le degré du pgcd $P \wedge (X^p - X)$. Et pour compter les racines dans $\mathbf{F}_q$?

Exercice 23. — Soit $P \in \mathbf{F}_p[X]$ un polynôme irréductible de degré n.

a) Montrer que pour tout $k \geqslant 1$, $P | X^{p^{nk}} - X$ dans $\mathbf{F}_p[X]$.
[**Indication:** Dans le corps fini $\mathbf{F}_p[X]/(P)$, on a $\overline{X}^{p^n} - \overline{X} = 0$.]

b) Montrer que dans $\mathbf{F}_p[X]$, on a $X^{p^n} - X = \prod_{\substack{P \in \mathbf{F}_p[X] \text{ irréductible} \\ \text{unitaire de degré divisant } n}} P$.

c) En déduire le test d'irréductibilité de Rabin : un polynôme $P \in \mathbf{F}_p[X]$ de degré n est irréductible ss'il divise $X^{p^n} - X$ et, pour tout facteur premier $d|n$, P est premier à $X^{p^{\frac{n}{d}}} - X$.
Application : Montrer que pour pour $a \in \mathbf{F}_p^\times$, le polynôme $X^p - X - a \in \mathbf{F}_p[X]$ est irréductible.
[**Indication:** Montrer que pour tout i, $X^{p^i} \equiv X + ia \mod (X^p - X - a)$.]

d) En notant $\mathrm{I}_p(n)$ le nombre de polynômes de $\mathbf{F}_p[X]$ irréductibles unitaires de degré n, montrer que l'on a $p^n = \sum_{d|n} d\mathrm{I}_p(d)$.

e) En utilisant la formule d'inversion de Möbius, en déduire que l'on a $\mathrm{I}_p(n) = \frac{1}{n} \sum_{d|n} \mu(\frac{n}{d}) q^d$.

f) Montrer que $\mathrm{I}_p(n)$ est équivalent à $\frac{q^n}{n}$.

Exercice 24. — **[Algorithme de Berlekamp]**
Soit $P \in \mathbf{F}_p[X]$ un polynôme sans facteur carré ; on note $P = P_1 \ldots P_r$ la décomposition de P en facteurs irréductibles. Soit $E := \mathbf{F}_p[X]/(P)$.

a) Montrer que E est un produit de corps finis.

b) Soit $\varphi : E \to E$, $e \mapsto e^p$. Montrer que φ est une linéaire et que l'on a $\dim \ker(\varphi - \mathrm{id}) = r$.
En déduire un test d'irréductibilité dans $\mathbf{F}_p[X]$.

c) Si $r > 1$, justifier qu'il existe un élément $\overline{Q} \in \ker(\varphi - \mathrm{id})$ "non constant".
Montrer qu'il existe $\lambda \in \mathbf{F}_p$, tel que $\mathrm{pgcd}(P, Q - \lambda)$ soit un diviseur non trivial de P.

d) Programmer cet algorithme de factorisation. Comment traiter également les polynômes ayant éventuellement des facteurs irréductibles avec multiplicités ?