

Corps et extensions

Corrigé de l'exercice 1 : Caractéristique et morphisme de Frobenius

1. Le noyau du morphisme $\mathbb{Z} \rightarrow K, n \rightarrow n \cdot 1_K$, vaut $p\mathbb{Z}$ avec $p > 0$. D'abord, $p \neq 1$ car $1_K \neq 0$. Ensuite, si $p = ab$ avec $1 < a, b < p$, on a $(a \cdot 1_K)(b \cdot 1_K) = p \cdot 1_K = 0$. Or un corps est intègre, donc $a \cdot 1_K = 0$ ou $b \cdot 1_K = 0$, ce qui contredit la minimalité de p . **Ainsi, p est premier.**
2. Pour $1 \leq k \leq p-1$, on a $k \binom{p}{k} = p \binom{p-1}{k-1}$. Donc p divise $k \binom{p}{k}$. Or p est premier et ne divise pas k , donc il est premier avec k . Le lemme de Gauss donne alors $p \mid \binom{p}{k}$. Par conséquent, dans K , la formule du binôme devient

$$(x + y)^p = x^p + \sum_{k=1}^{p-1} \binom{p}{k} x^k y^{p-k} + y^p = x^p + y^p.$$

De plus, $F(xy) = (xy)^p = x^p y^p = F(x)F(y)$ par commutativité, et $F(1) = 1$.
Donc F est un morphisme de corps.

3. Le noyau de F est un idéal de K qui ne contient pas 1 , puisque $F(1) = 1$. Or les seuls idéaux d'un corps sont $\{0\}$ et K . Donc $\ker F = \{0\}$ et F est injectif. Si K est fini, une application injective de K dans lui-même est bijective. **Le Frobenius d'un corps fini est donc un automorphisme.**
4. Soit $a \geq 0$ un entier. Dans $\mathbb{F}_p$, on écrit $\bar{a} = 1 + 1 + \dots + 1$ (a termes). Comme F est additif, $\bar{a}^p = 1^p + \dots + 1^p = \bar{a}$. Ensuite, un entier négatif est congru modulo p à un entier positif, et la relation ne dépend que de la classe. **On retrouve $a^p \equiv a \pmod{p}$ pour tout $a \in \mathbb{Z}$.**
5. Si p est impair, $(-y)^p = -y^p$. Si $p = 2$, alors $-1 = 1$ dans K , donc $(-y)^2 = y^2 = -y^2$. Dans les deux cas, $F(x - y) = F(x) + F(-y) = x^p - y^p$.

Enfin, $F^n: x \rightarrow x^{p^n}$ est une composée de morphismes, donc un morphisme. **Ainsi,**
 $(x - y)^{p^n} = x^{p^n} - y^{p^n}$.

Corrigé de l'exercice 2 : Sous-corps premier et morphismes de corps

1. Le noyau de σ est un idéal de K . Il ne contient pas 1, car $\sigma(1) = 1 \neq 0$. Donc $\ker \sigma = \{0\}$, et σ est injectif. Ensuite, pour tout $n \in \mathbb{Z}$, on a $\sigma(n \cdot 1_K) = n \cdot 1_L$. Par injectivité, $n \cdot 1_K = 0$ si et seulement si $n \cdot 1_L = 0$. **Les deux corps ont donc la même caractéristique.**
2. On a $\text{car}(\mathbb{Q}) = 0$, $\text{car}(\mathbb{F}_3) = 3$ et $\text{car}(\mathbb{F}_5) = 5$. Les caractéristiques diffèrent. **D'après la question 1, aucun des deux morphismes n'existe.**
3. Le corps $\mathbb{Q}(\sqrt{2})$ contient $\mathbb{Q}$ et il est de caractéristique nulle : son sous-corps premier est $\mathbb{Q}$. De même pour $\mathbb{R}$. Ensuite, $\mathbb{F}_3[X]/(X^2 + 1)$ est de caractéristique 3 : son sous-corps premier est formé des classes des constantes $\{0\bar{1}, \overline{\alpha 2}\}$, isomorphe à $\mathbb{F}_3$. Enfin, $\mathbb{F}_7(T)$ est de caractéristique 7. **Les sous-corps premiers sont $\mathbb{Q}$, $\mathbb{Q}$, $\mathbb{F}_3$ et $\mathbb{F}_7$.**
4. Soit $\sigma: \mathbb{Q} \rightarrow L$ un morphisme de corps. D'abord, $\sigma(1) = 1_L$, donc $\sigma(n) = n \cdot 1_L$ pour tout $n \in \mathbb{Z}$ par additivité. Ensuite, pour $b \neq 0$, $\sigma(b)\sigma(\frac{a}{b}) = \sigma(a)$, donc $\sigma(\frac{a}{b}) = (a \cdot 1_L)(b \cdot 1_L)^{-1}$. **Ainsi, σ est l'injection canonique de $\mathbb{Q}$ sur le sous-corps premier de L .**

Corrigé de l'exercice 3 : Degré d'une extension biquadratique

1. Supposons $\sqrt{3} = a + b\sqrt{2}$ avec $a, b \in \mathbb{Q}$. En élevant au carré, $3 = a^2 + 2b^2 + 2ab\sqrt{2}$. Comme $(1, \sqrt{2})$ est libre sur $\mathbb{Q}$, on obtient $ab = 0$. Si $b = 0$, alors $\sqrt{3} = a$ est rationnel : c'est faux. Si $a = 0$, alors $3 = 2b^2$, donc $(2b)^2 = 6$, et $\sqrt{6}$ serait rationnel : c'est faux aussi. **Donc $\sqrt{3} \notin \mathbb{Q}(\sqrt{2})$.**
2. Le polynôme $X^2 - 3$ est de degré 2 et n'a pas de racine dans $\mathbb{Q}(\sqrt{2})$. Il y est donc irréductible, et c'est le polynôme minimal de $\sqrt{3}$ sur $\mathbb{Q}(\sqrt{2})$. Ainsi, $[\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}(\sqrt{2})] = 2$,

de base $(1, \sqrt{3})$. Par le théorème de la base télescopique, avec la base $(1, \sqrt{2})$ de $\mathbb{Q}(\sqrt{2})$ sur $\mathbb{Q}$, on obtient les produits $1, \sqrt{2}, \sqrt{3}, \sqrt{6}$. **Donc** $[\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}] = 4$, **de base** $(1, \sqrt{2}, \sqrt{3}, \sqrt{6})$.

3. D'une part, $\sqrt{6} = \sqrt{2}\sqrt{3} \in \mathbb{Q}(\sqrt{2}, \sqrt{3})$. D'autre part, $\sqrt{3} = \frac{\sqrt{6}}{\sqrt{2}} \in \mathbb{Q}(\sqrt{2}, \sqrt{6})$. Chaque corps contient donc les générateurs de l'autre. **Par double inclusion**, $\mathbb{Q}(\sqrt{2}, \sqrt{3}) = \mathbb{Q}(\sqrt{2}, \sqrt{6})$.
4. On a vu que $X^2 - 3$ est de degré 2 sans racine dans $\mathbb{Q}(\sqrt{2})$. **Il est donc irréductible sur** $\mathbb{Q}(\sqrt{2})$. En revanche, $18 = (3\sqrt{2})^2$, donc $X^2 - 18 = (X - 3\sqrt{2})(X + 3\sqrt{2})$ **est réductible sur** $\mathbb{Q}(\sqrt{2})$, bien qu'il soit irréductible sur $\mathbb{Q}$.

Corrigé de l'exercice 4 : Calculs dans un corps de rupture de X^3 - 2

1. Le polynôme $X^3 - 2$ est unitaire, et 2 divise tous ses coefficients non dominants sans que 4 divise le terme constant. Le critère d'Eisenstein en 2 montre donc qu'il est irréductible sur $\mathbb{Q}$. Par conséquent, l'idéal $(X^3 - 2)$ est maximal dans $\mathbb{Q}[X]$, et K est un corps. La division euclidienne par $X^3 - 2$ montre enfin que tout élément s'écrit de façon unique $a + b\alpha + c\alpha^2$. **Ainsi**, $[K : \mathbb{Q}] = 3$ **et** $(1, \alpha, \alpha^2)$ **est une base**.
2. On utilise l'identité $(\alpha + 1)(\alpha^2 - \alpha + 1) = \alpha^3 + 1$. Or $\alpha^3 = 2$, donc ce produit vaut 3. **Par conséquent**, $(1 + \alpha)^{-1} = \frac{1}{3}\alpha^2 - \frac{1}{3}\alpha + \frac{1}{3}$.
3. On a $\alpha^2 + \alpha = \alpha(1 + \alpha)$. D'abord, $\alpha \cdot \alpha^2 = 2$, donc $\alpha^{-1} = \frac{\alpha^2}{2}$. Ensuite,

$$(\alpha^2 + \alpha)^{-1} = \frac{\alpha^2}{2} \cdot \frac{\alpha^2 - \alpha + 1}{3} = \frac{\alpha^4 - \alpha^3 + \alpha^2}{6} = \frac{2\alpha - 2 + \alpha^2}{6},$$
 car $\alpha^4 = 2\alpha$. Vérifions :

$$(\alpha^2 + \alpha)(\alpha^2 + 2\alpha - 2) = \alpha^4 + 3\alpha^3 - 2\alpha = 2\alpha + 6 - 2\alpha = 6. \text{ Donc } (\alpha^2 + \alpha)^{-1} = \frac{1}{6}(\alpha^2 + 2\alpha - 2).$$
4. D'abord, $(\alpha^2)^3 = \alpha^6 = 4$, donc α^2 annule $X^3 - 4$. Ensuite, $\alpha^2 \notin \mathbb{Q}$, car ses coordonnées dans la base sont $(0, 0, 1)$. Son degré divise $[K : \mathbb{Q}] = 3$ et ne vaut pas 1 : il vaut 3. Le polynôme $X^3 - 4$, unitaire de degré 3, est donc son polynôme minimal. De même, $\beta = 1 + \alpha$ vérifie $(\beta - 1)^3 = 2$, c'est-à-dire $\beta^3 - 3\beta^2 + 3\beta - 3 = 0$. Or $\mathbb{Q}(\beta) = \mathbb{Q}(\alpha)$ est de degré 3. **Les polynômes minimaux sont** $X^3 - 4$ **et** $X^3 - 3X^2 + 3X - 3$. Ce dernier est d'ailleurs d'Eisenstein en 3.

Corrigé de l'exercice 5 : Polynôme minimal de $\sqrt{2} + \sqrt{3}$

1. On a $\gamma^2 = 2 + 3 + 2\sqrt{6} = 5 + 2\sqrt{6}$. Donc $(\gamma^2 - 5)^2 = 24$, soit $\gamma^4 - 10\gamma^2 + 1 = 0$. **Le polynôme $P = X^4 - 10X^2 + 1$ convient.**

2. Par la formule du binôme,

$$\gamma^3 = 2\sqrt{2} + 3 \cdot 2 \cdot \sqrt{3} + 3\sqrt{2} \cdot 3 + 3\sqrt{3} = 11\sqrt{2} + 9\sqrt{3}.$$

Ainsi, $\gamma^3 - 9\gamma = 2\sqrt{2}$ et $\gamma^3 - 11\gamma = -2\sqrt{3}$. **Donc $\sqrt{2} = \frac{\gamma^3 - 9\gamma}{2}$ et $\sqrt{3} = \frac{11\gamma - \gamma^3}{2}$ appartiennent à $\mathbb{Q}(\gamma)$.**

3. D'une part, $\gamma \in \mathbb{Q}(\sqrt{2}, \sqrt{3})$. D'autre part, la question 2 donne l'inclusion réciproque. Donc $\mathbb{Q}(\gamma) = \mathbb{Q}(\sqrt{2}, \sqrt{3})$, de degré 4 d'après l'exercice 3. Le polynôme minimal de γ est donc de degré 4. Or il divise P , unitaire de degré 4. **Ainsi, $\mu_\gamma = X^4 - 10X^2 + 1$, irréductible sur $\mathbb{Q}$.** Ses racines sont les $\pm\sqrt{2} \pm \sqrt{3}$: en effet, leur carré vaut $5 \pm 2\sqrt{6}$, et $(5 \pm 2\sqrt{6} - 5)^2 = 24$.

4. Les trois identités se vérifient en développant : $X^4 - 2X^2 + 1 - 8X^2$, $X^4 + 2X^2 + 1 - 12X^2$ et $X^4 - 10X^2 + 25 - 24$ valent toutes P . Soit p premier impair et g un générateur de $\mathbb{F}_p^*$, d'ordre pair $p-1$. Les carrés non nuls sont exactement les puissances paires de g . Si 2 ou 3 est un carré (y compris $3 = 0$ lorsque $p = 3$), c'est gagné. Sinon, $2 = g^a$ et $3 = g^b$ avec a, b impairs, donc $6 = g^{a+b}$ avec $a+b$ pair : 6 est un carré. Ensuite :

◦ si $2 = s^2$, alors

$$P = (X^2 - 1)^2 - (2sX)^2 = (X^2 - 2sX - 1)(X^2 + 2sX - 1) ;$$

◦ si $3 = t^2$, alors $P = (X^2 - 2tX + 1)(X^2 + 2tX + 1)$;

◦ si $6 = u^2$, alors $P = (X^2 - 5 - 2u)(X^2 - 5 + 2u)$.

Dans tous les cas, P est réductible dans $\mathbb{F}_p[X]$. Pour $p = 2$, on a

$P = X^4 + 1 = (X + 1)^4$ par le Frobenius. Ainsi, **P est irréductible sur $\mathbb{Q}$ mais réductible modulo tout nombre premier.**

Point de méthode : la réduction modulo $\mathcal{P}$ prouve l'irréductibilité seulement quand elle réussit. Cet exemple montre qu'elle peut échouer pour tous les $\mathcal{P}$; il faut alors revenir à un calcul de degré.

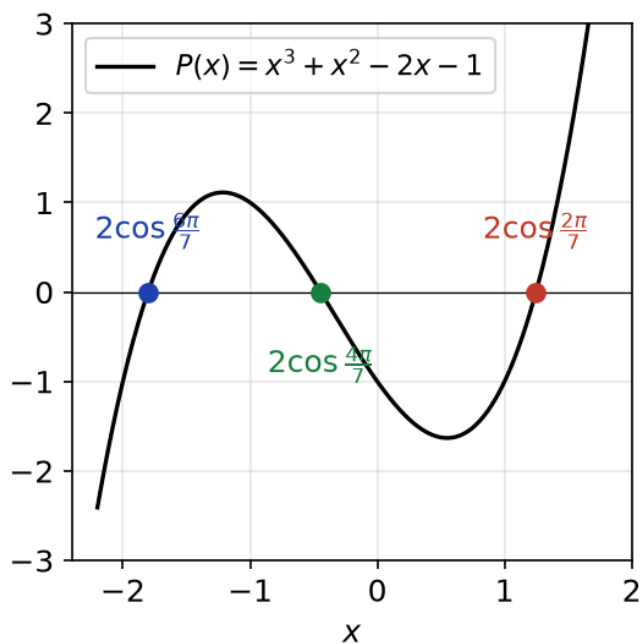
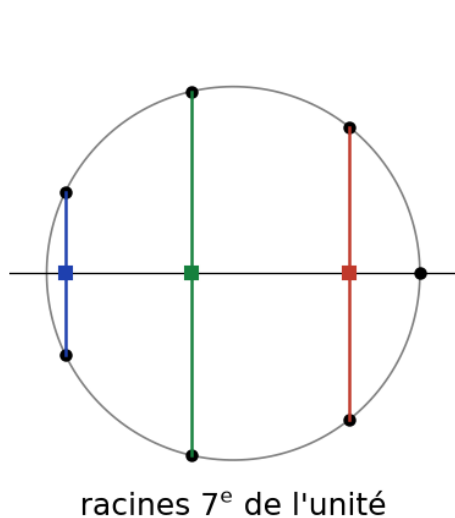
Corrigé de l'exercice 6 : Polynôme minimal de $2\cos(2\pi/7)$

- On a $\zeta^7 = 1$ et $\zeta \neq 1$. Or $(\zeta - 1)(1 + \zeta + \dots + \zeta^6) = \zeta^7 - 1 = 0$. Comme $\zeta - 1 \neq 0$, la somme est nulle.
- D'abord, $\theta^2 = \zeta^2 + 2 + \zeta^{-2}$, donc $\zeta^2 + \zeta^{-2} = \theta^2 - 2$. Ensuite, $\theta^3 = \zeta^3 + 3\zeta + 3\zeta^{-1} + \zeta^{-3}$, donc $\zeta^3 + \zeta^{-3} = \theta^3 - 3\theta$. Divisons alors la relation de la question 1 par ζ^3 :

$$\zeta^{-3} + \zeta^{-2} + \zeta^{-1} + 1 + \zeta + \zeta^2 + \zeta^3 = 0.$$

En regroupant, $1 + \theta + (\theta^2 - 2) + (\theta^3 - 3\theta) = 0$. Donc $\theta^3 + \theta^2 - 2\theta - 1 = 0$.

- Soit $P = X^3 + X^2 - 2X - 1$. Une racine rationnelle de ce polynôme unitaire à coefficients entiers serait un entier divisant 1. Or $P(1) = -1$ et $P(-1) = 1$. Ainsi, P n'a pas de racine dans $\mathbb{Q}$. Comme il est de degré 3, il est irréductible sur $\mathbb{Q}$. **C'est donc le polynôme minimal de θ , et $[\mathbb{Q}(\theta) : \mathbb{Q}] = 3$.**
- Pour $k \in \{2, 3\}$, ζ^k vérifie encore $(\zeta^k)^7 = 1$ et $\zeta^k \neq 1$. Le calcul précédent s'applique donc mot pour mot à ζ^k : $2\cos\frac{2k\pi}{7}$ est racine de P . Ces trois réels sont distincts, car $\cos$ est strictement décroissante sur $[0, \pi]$. Ce sont donc les trois racines de P . De plus, $2\cos\frac{4\pi}{7} = \zeta^2 + \zeta^{-2} = \theta^2 - 2$. La somme des racines vaut -1 , donc $2\cos\frac{6\pi}{7} = -1 - \theta - (\theta^2 - 2) = 1 - \theta - \theta^2$. **Les trois racines sont dans $\mathbb{Q}(\theta)$, qui est donc le corps de décomposition de P , de degré 3.** La figure ci-dessous montre les trois racines, projections des racines septièmes de l'unité, et le graphe de P .



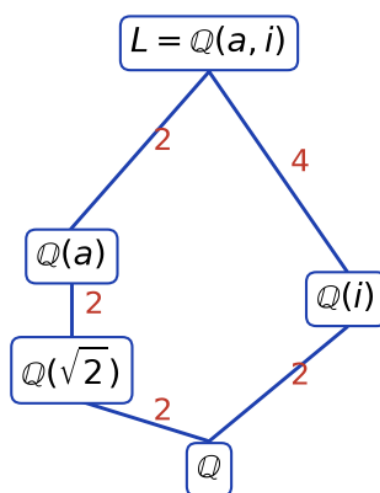
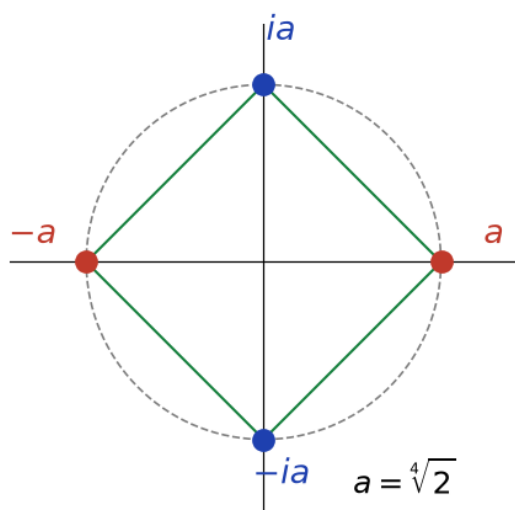
Corrigé de l'exercice 7 : Corps de décomposition de $X^3 - 2$

1. Le critère d'Eisenstein en 2 montre que $X^3 - 2$ est irréductible sur $\mathbb{Q}$. Ses racines complexes z vérifient $z^3 = 2 = a^3$, donc $(\frac{z}{a})^3 = 1$. **Les racines sont a , ja et j^2a .**
2. Le corps L contient a , ja et j^2a . Réciproquement, tout sous-corps contenant les trois racines contient a et $j = \frac{ja}{a}$. Donc $L = \mathbb{Q}(a, ja, j^2a)$ est bien le corps de décomposition. Ensuite, $[\mathbb{Q}(a) : \mathbb{Q}] = 3$. Le nombre j est racine de $X^2 + X + 1$, et $j \notin \mathbb{Q}(a)$ car $\mathbb{Q}(a) \subset \mathbb{R}$. Ce polynôme de degré 2 sans racine dans $\mathbb{Q}(a)$ y est irréductible, donc $[L : \mathbb{Q}(a)] = 2$. **La base télescopique donne $[L : \mathbb{Q}] = 6$.**
3. Chacun des trois corps est un corps de rupture de $X^3 - 2$, irréductible sur $\mathbb{Q}$. Par unicité du corps de rupture, ils sont isomorphes, et chacun est de degré 3. Montrons qu'ils sont distincts. Si $\mathbb{Q}(ja) = \mathbb{Q}(a)$, alors $j = \frac{ja}{a} \in \mathbb{Q}(a) \subset \mathbb{R}$: c'est absurde. De même, $\mathbb{Q}(j^2a) \neq \mathbb{Q}(a)$, car $j^2 \notin \mathbb{R}$. Enfin, si $\mathbb{Q}(ja) = \mathbb{Q}(j^2a)$, alors $j = \frac{j^2a}{ja}$ et $a = \frac{ja}{j}$ appartiennent à $\mathbb{Q}(ja)$. Ce corps contiendrait L , de degré $6 > 3$: c'est impossible. **Les trois corps sont deux à deux distincts et isomorphes.**
4. On a $[\mathbb{Q}(j) : \mathbb{Q}] = 2$ et $L = \mathbb{Q}(j)(a)$. Par la base télescopique, $[L : \mathbb{Q}(j)] = \frac{6}{2} = 3$. Le

polynôme minimal de α sur $\mathbb{Q}(j)$ est donc de degré 3 et divise $X^3 - 2$. **Ainsi, $X^3 - 2$ est irréductible sur $\mathbb{Q}(j)$.**

Corrigé de l'exercice 8 : Corps de décomposition de $X^4 - 2$

1. Le critère d'Eisenstein en 2 donne l'irréductibilité de $X^4 - 2$ sur $\mathbb{Q}$. Si $z^4 = 2$, alors $(\frac{z}{\alpha})^4 = 1$, donc $\frac{z}{\alpha} \in \{1, i, -1, -i\}$. **Les racines sont $\alpha, -\alpha, i\alpha$ et $-i\alpha$.**
2. Le corps de décomposition est $\mathbb{Q}(\alpha, -\alpha, i\alpha, -i\alpha)$. Il contient α et $i = \frac{i\alpha}{\alpha}$, et il est contenu dans $\mathbb{Q}(\alpha, i)$. Donc il vaut $L = \mathbb{Q}(\alpha, i)$. Ensuite, $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 4$. Comme $\mathbb{Q}(\alpha) \subset \mathbb{R}$, on a $i \notin \mathbb{Q}(\alpha)$, et $X^2 + 1$ est irréductible sur $\mathbb{Q}(\alpha)$. Ainsi, $[L : \mathbb{Q}(\alpha)] = 2$. **Par la base télescopique, $[L : \mathbb{Q}] = 8$.**
3. On a $\alpha^2 = \sqrt{2}$, donc $\mathbb{Q}(\sqrt{2}) \subset \mathbb{Q}(\alpha)$. Par la base télescopique, $[\mathbb{Q}(\alpha) : \mathbb{Q}(\sqrt{2})] = \frac{4}{2} = 2$. Le polynôme $X^2 - \sqrt{2}$ est unitaire, de degré 2, et annule α . **C'est le polynôme minimal de α sur $\mathbb{Q}(\sqrt{2})$.**
4. On a $[\mathbb{Q}(i) : \mathbb{Q}] = 2$ et $L = \mathbb{Q}(i)(\alpha)$. Donc $[\mathbb{Q}(i)(\alpha) : \mathbb{Q}(i)] = \frac{8}{2} = 4$. Le polynôme minimal de α sur $\mathbb{Q}(i)$ est de degré 4 et divise $X^4 - 2$. **Ainsi, $X^4 - 2$ est irréductible sur $\mathbb{Q}(i)$.**
5. Les corps $\mathbb{Q}(\alpha)$ et $\mathbb{Q}(i\alpha)$ sont deux corps de rupture de $X^4 - 2$: ils sont isomorphes. Cependant, $i\alpha \notin \mathbb{R}$, donc $i\alpha \notin \mathbb{Q}(\alpha)$: ils sont distincts. Ensuite, $i\sqrt{2} = i\alpha^2 \in L$ et $(i\sqrt{2})^2 = -2$. Le polynôme $X^2 + 2$ n'a pas de racine rationnelle, donc $[\mathbb{Q}(i\sqrt{2}) : \mathbb{Q}] = 2$. Ce corps n'est pas réel, donc il diffère de $\mathbb{Q}(\sqrt{2})$. Enfin, si $\mathbb{Q}(i\sqrt{2}) = \mathbb{Q}(i)$, alors $\sqrt{2} = \frac{i\sqrt{2}}{i} \in \mathbb{Q}(i)$. Par égalité des degrés, on aurait $\mathbb{Q}(\sqrt{2}) = \mathbb{Q}(i)$, ce qui est faux car l'un est réel et l'autre non. **Ainsi, $\mathbb{Q}(i\sqrt{2})$ est un troisième sous-corps quadratique de L .** La figure ci-dessous récapitule les racines et la tour de corps obtenue.



Corrigé de l'exercice 9 : Extensions de degré 2

1. Soit $\alpha \in L \setminus K$. On a $K \subset K(\alpha) \subset L$, donc $[K(\alpha):K]$ divise $[L:K] = 2$. Or ce degré ne vaut pas 1, puisque $\alpha \notin K$. Donc $[K(\alpha):K] = 2 = [L:K]$. Un sous-espace de même dimension finie est l'espace entier. **Ainsi, $L = K(\alpha)$.**

2. Soit $X^2 + bX + c$ le polynôme minimal de α . Comme $2 \neq 0$ dans K , on peut poser $\delta = \alpha + \frac{b}{2}$. Alors

$$\delta^2 = \alpha^2 + b\alpha + \frac{b^2}{4} = -c + \frac{b^2}{4} \in K.$$

De plus, $\delta \notin K$, sinon $\alpha = \delta - \frac{b}{2}$ serait dans K . **D'après la question 1, $L = K(\delta)$ avec $\delta^2 \in K$.**

3. Ici, $L = \mathbb{Q}(\delta)$ avec $r = \delta^2 \in \mathbb{Q}$ et $\delta \notin \mathbb{Q}$. Écrivons $r = \frac{u}{v}$ avec $u > 0$. Alors $r = \frac{uv}{v^2}$, et l'on écrit $uv = s^2 d$ avec d sans facteur carré. Donc $\delta = \pm \frac{s}{v} \sqrt{d}$, où $\sqrt{d}$ désigne une racine carrée complexe de d . Ainsi, $\mathbb{Q}(\delta) = \mathbb{Q}(\sqrt{d})$. Enfin, $d \neq 1$ (et $d \neq 0$), car $\delta \notin \mathbb{Q}$. **Toute extension quadratique de $\mathbb{Q}$ dans $\mathbb{C}$ est un $\mathbb{Q}(\sqrt{d})$, avec $d \neq 1$ sans facteur carré.**

4. Supposons $(x + y\sqrt{3})^2 = 2$ avec $x, y \in \mathbb{Q}$. Alors $x^2 + 3y^2 + 2xy\sqrt{3} = 2$, donc

$xy = 0$. Si $y = 0$, alors $x^2 = 2$: impossible dans $\mathbb{Q}$. Si $x = 0$, alors $3y^2 = 2$, soit $(3y)^2 = 6$: impossible aussi. Donc 2 n'est pas un carré dans $\mathbb{Q}(\sqrt{3})$. Or un isomorphisme $\sigma : \mathbb{Q}(\sqrt{2}) \rightarrow \mathbb{Q}(\sqrt{3})$ fixe $\mathbb{Q}$ (exercice 2), donc $\sigma(\sqrt{2})^2 = \sigma(2) = 2$. **Un tel isomorphisme n'existe donc pas.**

Corrigé de l'exercice 10 : Nombres transcendants

1. L'ensemble $\mathbb{Q}_n[X]$ est en bijection avec $\mathbb{Q}^{n+1}$, qui est dénombrable. Donc $\mathbb{Q}[X] = \bigcup_n \mathbb{Q}_n[X]$ est dénombrable, comme réunion dénombrable d'ensembles dénombrables. Ensuite, tout polynôme non nul a un nombre fini de racines. L'ensemble des nombres algébriques est la réunion, indexée par $\mathbb{Q}[X] \setminus \{0\}$, de ces ensembles finis. Il est donc dénombrable. **Comme $\mathbb{R}$ n'est pas dénombrable, il existe des réels transcendants.**
2. Le noyau du morphisme d'évaluation $\text{ev}_\alpha : \mathbb{Q}[X] \rightarrow \mathbb{C}$ est réduit à $\{0\}$, par définition de la transcendance. Donc ev_α induit un isomorphisme $\mathbb{Q}[X] \simeq \mathbb{Q}[\alpha]$. Or X n'est pas inversible dans $\mathbb{Q}[X]$, pour une raison de degré. Donc α n'est pas inversible dans $\mathbb{Q}[\alpha]$. En revanche, $\alpha \neq 0$ est inversible dans le corps $\mathbb{Q}(\alpha)$. **Ainsi, $\mathbb{Q}[\alpha] \neq \mathbb{Q}(\alpha)$.**
3. Une relation $\sum_{k=0}^n c_k \alpha^k = 0$ non triviale fournirait un polynôme non nul annulant α . Donc la famille $(\alpha^k)_{k \geq 0}$ est libre sur $\mathbb{Q}$. **Par conséquent, $[\mathbb{Q}(\alpha) : \mathbb{Q}] = +\infty$.**
4. Supposons $\alpha^2 + 1$ algébrique, racine de $P \neq 0$ de degré m . Alors $Q = P(X^2 + 1)$ est un polynôme de degré $2m$, donc non nul, et $Q(\alpha) = 0$. C'est absurde. Ensuite, si $\beta^2 = \alpha$ avec β algébrique, l'extension $\mathbb{Q}(\beta)/\mathbb{Q}$ est finie. Elle contient $\alpha = \beta^2$, qui serait donc algébrique : c'est absurde. **Ainsi, $\alpha^2 + 1$ et toute racine carrée de α sont transcendants.**

Corrigé de l'exercice 11 : Les nombres algébriques forment un corps

1. Le polynôme minimal μ_β de β sur $\mathbb{Q}$ est à coefficients dans $\mathbb{Q}(\alpha)$. Donc le polynôme minimal de β sur $\mathbb{Q}(\alpha)$ divise μ_β , et $[\mathbb{Q}(\alpha, \beta) : \mathbb{Q}(\alpha)] \leq n$. La base télescopique donne

$[\mathbb{Q}(\alpha, \beta) : \mathbb{Q}] \leq mn$. Cette extension finie est algébrique. Elle contient $\alpha + \beta$, $\alpha\beta$, $-\alpha$ et, si $\alpha \neq 0$, α^{-1} . **Donc $\bar{\mathbb{Q}}$ est un sous-corps de $\mathbb{C}$.**

2. Notons $D = [\mathbb{Q}(\sqrt{2}, \sqrt[3]{3}) : \mathbb{Q}]$. D'une part, $D \leq 2 \times 3 = 6$. D'autre part, $[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2$ et $[\mathbb{Q}(\sqrt[3]{3}) : \mathbb{Q}] = 3$, car $X^3 - 3$ est d'Eisenstein en 3. Ces deux degrés divisent D , donc $6 \mid D$. **Ainsi, $D = 6$.**

3. En développant,

$$(\gamma - \sqrt{2})^3 = \gamma^3 - 3\sqrt{2}\gamma^2 + 6\gamma - 2\sqrt{2} = 3.$$

Donc $\sqrt{2}(3\gamma^2 + 2) = \gamma^3 + 6\gamma - 3$. Comme γ est réel, $3\gamma^2 + 2 > 0$, et $\sqrt{2} = \frac{\gamma^3 + 6\gamma - 3}{3\gamma^2 + 2} \in \mathbb{Q}(\gamma)$. Ensuite, $\sqrt[3]{3} = \gamma - \sqrt{2} \in \mathbb{Q}(\gamma)$. Donc $\mathbb{Q}(\gamma) = \mathbb{Q}(\sqrt{2}, \sqrt[3]{3})$. **Le degré de γ vaut 6.**

4. Élevons au carré la relation $\gamma^3 + 6\gamma - 3 = \sqrt{2}(3\gamma^2 + 2)$. D'abord, $(\gamma^3 + 6\gamma - 3)^2 = \gamma^6 + 12\gamma^4 - 6\gamma^3 + 36\gamma^2 - 36\gamma + 9$. Ensuite, $2(3\gamma^2 + 2)^2 = 18\gamma^4 + 24\gamma^2 + 8$. La différence est nulle, soit

$$\gamma^6 - 6\gamma^4 - 6\gamma^3 + 12\gamma^2 - 36\gamma + 1 = 0.$$

Ce polynôme est unitaire, de degré 6, et annule γ , qui est de degré 6. **Le polynôme minimal de γ est $X^6 - 6X^4 - 6X^3 + 12X^2 - 36X + 1$.**

5. Soit z racine de $\sum_{k=0}^n a_k X^k \neq 0$, avec $a_k \in \bar{\mathbb{Q}}$. Le corps $M = \mathbb{Q}(a_0, \dots, a_n)$ est de degré fini sur $\mathbb{Q}$, par récurrence à partir de la question 1. Ensuite, z est algébrique sur M , donc $[M(z) : M]$ est fini. Par la base télescopique, $[M(z) : \mathbb{Q}]$ est fini. **Donc z est algébrique sur $\mathbb{Q}$: le corps $\bar{\mathbb{Q}}$ est algébriquement clos.**

Corrigé de l'exercice 12 : Duplication du cube et racines non constructibles

1. D'après le théorème des tours quadratiques, un réel constructible x appartient à un corps K_r avec $[K_r : \mathbb{Q}] = 2^r$. Or $\mathbb{Q} \subset \mathbb{Q}(x) \subset K_r$. **Donc $[\mathbb{Q}(x) : \mathbb{Q}]$ divise 2^r : c'est une puissance de 2.**

- Le polynôme $X^3 - 2$ est irréductible (Eisenstein en 2), donc $[\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = 3$. Ce n'est pas une puissance de 2. **Ainsi, $\sqrt[3]{2}$ n'est pas constructible.** Géométriquement, un cube de volume double de celui d'un cube d'arête 1 a pour arête $\sqrt[3]{2}$: on ne peut pas la construire à la règle et au compas.
- Le réel 2 est constructible, donc $\sqrt{2}$ aussi, puis $\sqrt{\sqrt{2}} = \sqrt[4]{2}$. Enfin, $X^4 - 2$ est d'Eisenstein en 2. **Ainsi, $\sqrt[4]{2}$ est constructible, de degré 4.**
- Le polynôme $X^6 - 2$ est d'Eisenstein en 2, donc $\sqrt[6]{2}$ est de degré 6, qui n'est pas une puissance de 2. Ensuite, si $1 + \sqrt[3]{2}$ était constructible, $\sqrt[3]{2} = (1 + \sqrt[3]{2}) - 1$ le serait aussi, car les constructibles forment un corps. **Aucun des deux n'est constructible.**
- On calcule $(1 + \sqrt{2})^3 = 1 + 3\sqrt{2} + 3 \times 2 + 2\sqrt{2} = 7 + 5\sqrt{2}$. La racine cubique réelle étant unique, $\sqrt[3]{7 + 5\sqrt{2}} = 1 + \sqrt{2}$. **Ce réel est constructible**, bien qu'il s'écrive avec une racine cubique.

Point de méthode : une écriture avec des racines cubiques ne prouve pas la non-constructibilité. Seul le degré sur $\mathbb{Q}$ compte.

Corrigé de l'exercice 13 : Trisection de l'angle

- Par la formule de Moivre, $\cos 3\theta = \operatorname{Re}((\cos\theta + i\sin\theta)^3) = \cos^3\theta - 3\cos\theta\sin^2\theta$. En remplaçant $\sin^2\theta$ par $1 - \cos^2\theta$, **on obtient** $\cos 3\theta = 4\cos^3\theta - 3\cos\theta$.
- Avec $\theta = 20^\circ$ et $c = \cos 20^\circ$, on a $4c^3 - 3c = \cos 60^\circ = \frac{1}{2}$. Posons $x = 2c$. Alors $4c^3 = \frac{x^3}{2}$ et $3c = \frac{3x}{2}$. En multipliant par 2, **on obtient** $x^3 - 3x - 1 = 0$.
- Une racine rationnelle de ce polynôme unitaire à coefficients entiers serait ± 1 . Or $1 - 3 - 1 = -3$ et $-1 + 3 - 1 = 1$. Ce polynôme de degré 3 n'a pas de racine rationnelle, donc il est irréductible sur $\mathbb{Q}$. Ainsi, x est de degré 3 et n'est pas constructible. Par conséquent, $\cos 20^\circ = \frac{x}{2}$ non plus. Pourtant, l'angle de 60° est constructible, car $\cos 60^\circ = \frac{1}{2}$. **Il n'existe donc pas de méthode générale de trisection à la règle et au compas.**
- Le tiers de 90° est 30° , et $\cos 30^\circ = \frac{\sqrt{3}}{2}$. Ce réel est constructible, car $\sqrt{3}$ l'est. **L'angle droit se trisecte donc.**

- ## Corrigé de l'exercice 15 : Construction de F4 et F8

- $$\begin{array}{c|cccc} + & 0 & 1 & \alpha & \alpha+1 \\ \hline 0 & 0 & 1 & \alpha & \alpha+1 \\ 1 & 1 & 0 & \alpha+1 & \alpha \\ \alpha & \alpha & \alpha+1 & 0 & 1 \\ \alpha+1 & \alpha+1 & \alpha & 1 & 0 \end{array} \quad \begin{array}{c|ccc} \times & 1 & \alpha & \alpha+1 \\ \hline 1 & 1 & \alpha & \alpha+1 \\ \alpha & \alpha & \alpha+1 & 1 \\ \alpha+1 & \alpha+1 & 1 & \alpha \end{array}$$

3. Le polynôme $X^3 + X + 1$ vaut 1 en 0 et en 1. De degré 3 sans racine, il est irréductible. Avec $\beta^3 = \beta + 1$, on calcule successivement :

$$\beta^4 = \beta^2 + \beta, \beta^5 = \beta^3 + \beta^2 = \beta^2 + \beta + 1, \beta^6 = \beta^3 + \beta^2 + \beta = \beta^2 + 1, \beta^7 = \beta^3 + \beta = 1.$$

Les puissances $\beta^0, \dots, \beta^6$ décrivent les sept éléments non nuls, et $\beta^7 = 1$.

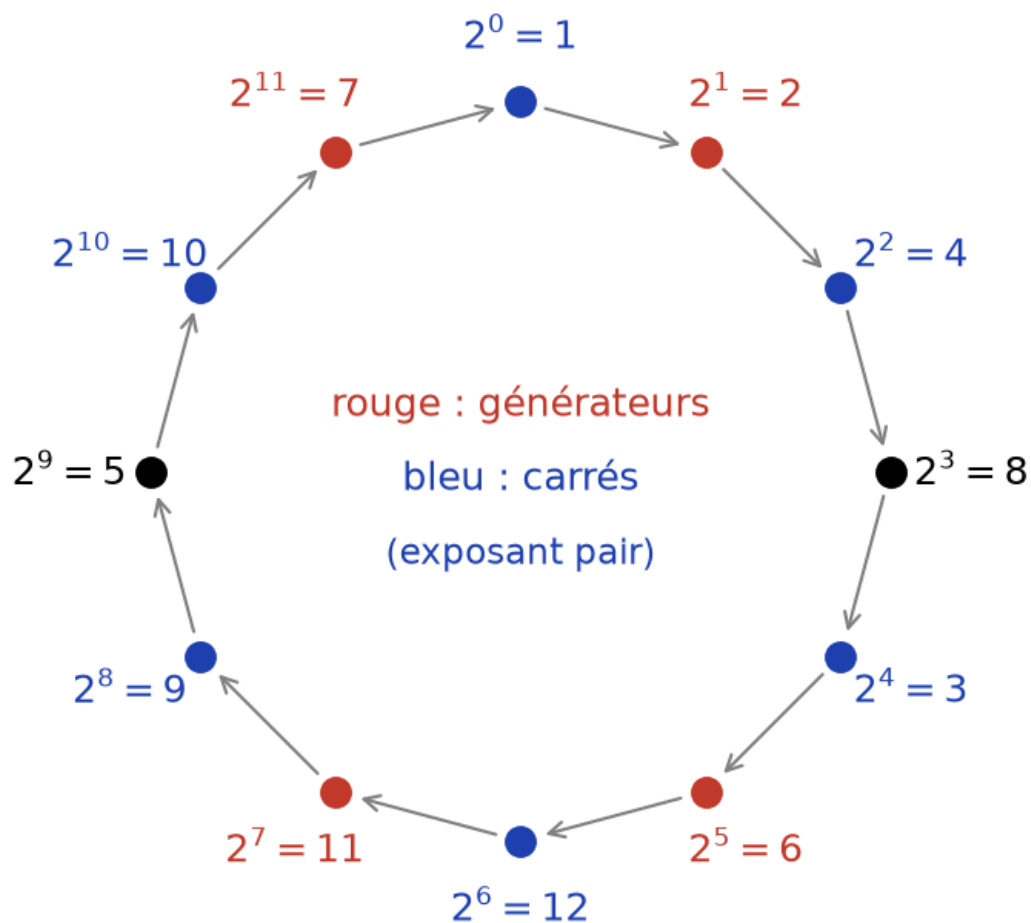
4. On a $\beta^2 + 1 = \beta^6$, donc son inverse est $\beta^{7-6} = \beta$. Vérification :
 $\beta(\beta^2 + 1) = \beta^3 + \beta = 1$. De même, $\beta^2 + \beta = \beta^4$, d'inverse $\beta^3 = \beta + 1$. **Les inverses sont β et $\beta + 1$.**
5. Un sous-corps à 4 éléments serait de degré 2 sur $\mathbb{F}_2$. Par la base télescopique, 2 diviserait $[\mathbb{F}_8 : \mathbb{F}_2] = 3$. **C'est impossible.**

Corrigé de l'exercice 16 : Le corps $\mathbb{F}_9$ et ses générateurs

1. Dans $\mathbb{F}_3$, $X^2 + 1$ prend les valeurs 1, 2, 2 en 0, 1, 2. Sans racine et de degré 2, **il est irréductible, et $\mathbb{F}_9$ est un corps à 9 éléments.**
2. On a $\alpha^2 = -1 \neq 1$ et $\alpha^4 = 1$. **L'ordre de α vaut 4, donc α n'engendre pas $\mathbb{F}_9^*$, qui est d'ordre 8.**
3. D'abord, $(1 + \alpha)^2 = 1 + 2\alpha + \alpha^2 = 2\alpha$. Ensuite, $(1 + \alpha)^4 = 4\alpha^2 = -4 = -1$ dans $\mathbb{F}_3$. L'ordre de $1 + \alpha$ divise 8 mais ne divise pas 4. **Il vaut donc 8 : $1 + \alpha$ est un générateur.**
4. Il y a $\varphi(8) = 4$ générateurs : les $(1 + \alpha)^k$ avec k impair. On calcule
 $(1 + \alpha)^3 = 2\alpha(1 + \alpha) = 2\alpha - 2 = 1 + 2\alpha$. Ensuite,
 $(1 + \alpha)^5 = -(1 + \alpha) = 2 + 2\alpha$ et $(1 + \alpha)^7 = -(1 + 2\alpha) = 2 + \alpha$. **Les générateurs sont $1 + \alpha$, $1 + 2\alpha$, $2 + 2\alpha$ et $2 + \alpha$.** Les quatre autres éléments non nuls, 1, 2, α , 2α , sont d'ordres 1, 2, 4, 4.
5. Posons $\beta = 1 + \alpha$. Alors $(\beta - 1)^2 = -1$, soit $\beta^2 - 2\beta + 2 = 0$, c'est-à-dire
 $\beta^2 + \beta + 2 = 0$ dans $\mathbb{F}_3$. Comme $\beta \notin \mathbb{F}_3$, son degré vaut 2. **Le polynôme minimal est $X^2 + X + 2$, et $\mathbb{F}_9 \simeq \mathbb{F}_3[X]/(X^2 + X + 2)$, présentation dans laquelle la classe de X est un générateur.**

Corrigé de l'exercice 17 : Générateurs et racines dans $\mathbb{F}_{13}$

1. On a $12 = 2^2 \times 3$. D'après la méthode du cours, il suffit de vérifier $2^{12/2} \neq 1$ et $2^{12/3} \neq 1$. Or $2^4 = 16 = 3$ et $2^6 = 64 = 12 = -1$ dans $\mathbb{F}_{13}$. **Donc 2 est d'ordre 12 : il engendre $\mathbb{F}_{13}^*$.**
2. Les puissances $2^0, \dots, 2^{11}$ valent successivement 1, 2, 4, 8, 3, 6, 12, 11, 9, 5, 10, 7. Les générateurs sont les 2^k avec k premier à 12, soit $k \in \{1, 5, 7, 11\}$. **Les générateurs sont 2, 6, 11 et 7.**
3. Les carrés non nuls sont les puissances paires de 2 : $2^0, 2^2, \dots, 2^{10}$. **Ce sont 1, 4, 3, 12, 9, 10.** En particulier, $-1 = 12 = 2^6 = (2^3)^2 = 8^2$. **Donc -1 est un carré**, conformément au fait que $13 \equiv 1 \pmod{4}$. La figure ci-dessous place les douze puissances de 2 sur un cycle et distingue les générateurs et les carrés.



4. Posons $x = 2^k$, l'élément 0 n'étant pas solution. On a $10 = 2^{10}$, donc $x^2 = 10$ équivaut à $2^k \equiv 10 \pmod{12}$, soit $k \equiv 5 \pmod{6}$. Ainsi, $k \in \{5, 11\}$ et $x \in \{6, 7\}$.
 Vérification : $6^2 = 36 = 10$ et $7^2 = 49 = 10$. Ensuite, $5 = 2^9$, donc $x^3 = 5$ équivaut à $3^k \equiv 9 \pmod{12}$, soit $k \equiv 3 \pmod{4}$. D'où $k \in \{3, 7, 11\}$ et $x \in \{8, 11, 7\}$. Vérification : $8^3 = 512 = 39 \times 13 + 5$. **Les solutions sont $\{6, 7\}$ pour $x^2 = 10$ et $\{7, 8, 11\}$ pour $x^3 = 5$.**

Point de méthode : un générateur transforme les équations multiplicatives en congruences sur les exposants, exactement comme un logarithme.

Corrigé de l'exercice 18 : Deux constructions de $\mathbb{F}_{16}$

- On a $P(0) = 1$ et $P(1) = 1 + 1 + 1 = 1$, donc P n'a pas de facteur de degré 1. S'il était réductible, il serait produit de deux irréductibles de degré 2. Or le seul est $X^2 + X + 1$, et $(X^2 + X + 1)^2 = X^4 + X^2 + 1 \neq P$. **Donc P est irréductible.**
- L'ordre de α divise $15 = 3 \times 5$. D'une part, $\alpha^3 \neq 1$, car $(1, \alpha, \alpha^2, \alpha^3)$ est une base. D'autre part, $\alpha^4 = \alpha + 1$, donc $\alpha^5 = \alpha^2 + \alpha \neq 1$. **Ainsi, α est d'ordre 15 : c'est un générateur.**
- On a $Q(0) = 1$, $Q(1) = 5 = 1$, et $Q \neq X^4 + X^2 + 1$. Le même raisonnement montre que Q est irréductible. Cependant, $(X - 1)Q = X^5 - 1$, donc $\beta^5 = 1$ avec $\beta \neq 1$. **L'ordre de β vaut 5, et β n'engendre pas le groupe multiplicatif.** Les deux quotients sont pourtant des corps à 16 éléments, donc isomorphes.
- Le sous-corps à 4 éléments est formé de 0 et des racines de $x^3 = 1$ dans $\mathbb{F}_{16}^*$. Ce sont 1, α^5 et α^{10} . On a $\alpha^5 = \alpha^2 + \alpha$, puis $\alpha^{10} = (\alpha^2 + \alpha)^2 = \alpha^4 + \alpha^2 = \alpha^2 + \alpha + 1$. Vérification : $(\alpha^2 + \alpha)^2 + (\alpha^2 + \alpha) + 1 = \alpha^4 + \alpha + 1 = 0$. **Le sous-corps est $\{0, 1, \alpha^2 + \alpha, \alpha^2 + \alpha + 1\}$.**

Corrigé de l'exercice 19 : Sous-corps de $\mathbb{F}_{4096}$

1. Les diviseurs de 12 sont 1, 2, 3, 4, 6, 12. **Les sous-corps sont $\mathbb{F}_2, \mathbb{F}_4, \mathbb{F}_8, \mathbb{F}_{16}, \mathbb{F}_{64}$ et K .** De plus, $\mathbb{F}_{2^d} \subset \mathbb{F}_{2^e}$ si et seulement si $d \mid e$. Ainsi, $\mathbb{F}_4 \subset \mathbb{F}_{16}$, $\mathbb{F}_4 \subset \mathbb{F}_{64}$ et $\mathbb{F}_8 \subset \mathbb{F}_{64}$, mais $\mathbb{F}_8 \not\subset \mathbb{F}_{16}$.
2. Le corps $\mathbb{F}_2(x)$ est un sous-corps de K . Il est égal à K si et seulement si x n'est dans aucun sous-corps strict. Or tout diviseur strict de 12 divise 6 ou 4. Donc tout sous-corps strict est inclus dans $\mathbb{F}_{64}$ ou dans $\mathbb{F}_{16}$. **Ainsi, $\mathbb{F}_2(x) = K$ si et seulement si $x \notin \mathbb{F}_{64} \cup \mathbb{F}_{16}$.**
3. L'intersection $\mathbb{F}_{64} \cap \mathbb{F}_{16}$ est un sous-corps de $\mathbb{F}_{16}$ et de $\mathbb{F}_{64}$. Son degré divise 4 et 6, donc 2 : c'est $\mathbb{F}_4$. Par la formule du crible, $|\mathbb{F}_{64} \cup \mathbb{F}_{16}| = 64 + 16 - 4 = 76$. **Il y a donc $4096 - 76 = 4020$ éléments tels que $\mathbb{F}_2(x) = K$.**
4. Pour un tel x , le polynôme minimal est irréductible de degré $[\mathbb{F}_2(x) : \mathbb{F}_2] = 12$. Réciproquement, soit Q unitaire irréductible de degré 12. Son corps de rupture a 2^{12} éléments, donc il est isomorphe à K , et Q a une racine y dans K . Comme $y^{4096} = y$, $Q = \mu_y$ divise $X^{4096} - X$, qui est scindé à racines simples sur K . Donc Q a 12 racines distinctes dans K , toutes de degré 12. L'application $x \rightarrow \mu_x$ est ainsi exactement 12 pour 1. **Il y a $\frac{4020}{12} = 335$ polynômes unitaires irréductibles de degré 12 sur $\mathbb{F}_2$.**

Corrigé de l'exercice 20 : Dénombrement des polynômes irréductibles

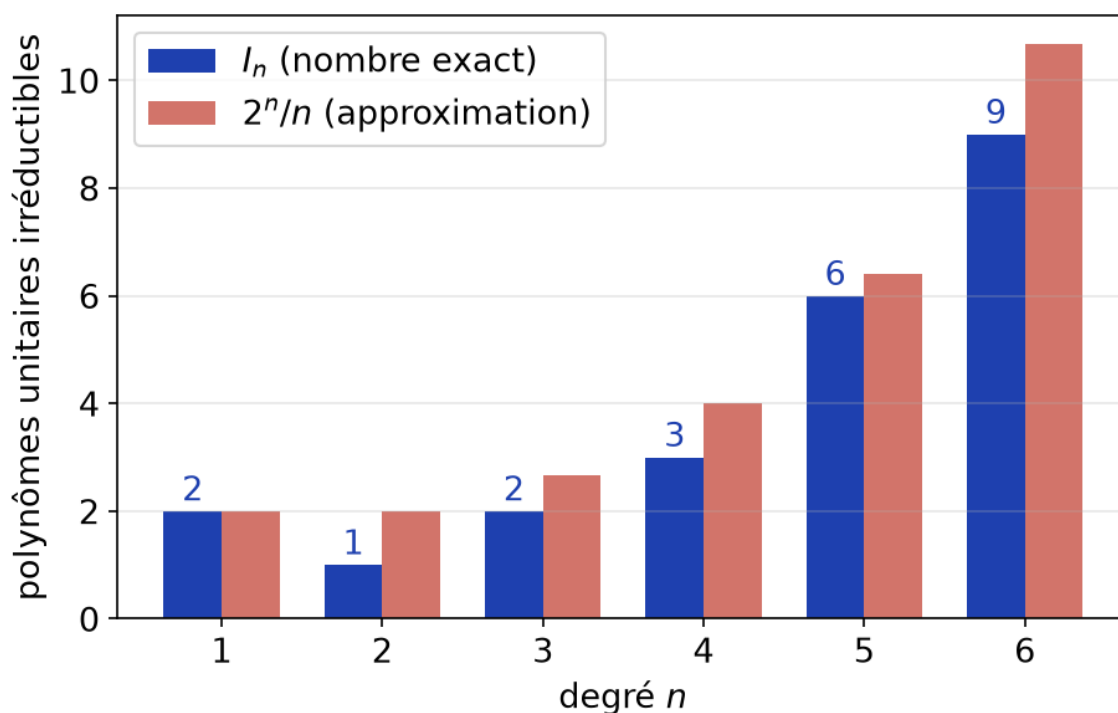
1. Soit $L = \mathbb{F}_p[X]/(Q)$, corps à p^d éléments, et $x = \overline{X}$. Supposons d'abord que Q divise $X^{p^n} - X$. Alors $x^{p^n} = x$. L'ensemble des $y \in L$ tels que $y^{p^n} = y$ est un sous-corps, car F^n est un morphisme. Il contient x , donc il vaut $\mathbb{F}_p(x) = L$. Soit g un générateur de L^* : on a $g^{p^n-1} = 1$, donc $p^d - 1$ divise $p^n - 1$. Écrivons $n = kd + r$ avec $0 \leq r < d$. Alors $p^n - 1 = p^r(p^{kd} - 1) + (p^r - 1)$, et $p^d - 1$ divise $p^{kd} - 1$. Donc $p^d - 1$ divise $p^r - 1 < p^d - 1$, ce qui impose $r = 0$. Réciproquement, si $d \mid n$, tout $y \in L$ vérifie $y^{p^d} = y$. En itérant $\frac{n}{d}$ fois, $y^{p^n} = y$. En particulier, x annule $X^{p^n} - X$, donc $Q = \mu_x$ le divise. **Ainsi, $Q \mid X^{p^n} - X$ si et seulement si $d \mid n$.**

2. La dérivée de $X^{p^n} - X$ vaut -1 . Ce polynôme est donc premier avec sa dérivée : il est sans facteur carré. Ses facteurs irréductibles unitaires apparaissent ainsi avec multiplicité 1. D'après la question 1, ce sont exactement les irréductibles unitaires de degré divisant n . En comparant les degrés, $p^n = \sum_{d|n} d I_d$.

3. Pour $p = 2$, la formule donne successivement :

$$\begin{aligned} 2 &= I_1, & 4 &= I_1 + 2I_2, & 8 &= I_1 + 3I_3, \\ 16 &= I_1 + 2I_2 + 4I_4, & 32 &= I_1 + 5I_5, & 64 &= I_1 + 2I_2 + 3I_3 + 6I_6. \end{aligned}$$

On obtient $I_1 = 2$, $I_2 = 1$, $I_3 = 2$, $I_4 = 3$, $I_5 = 6$, $I_6 = 9$. Pour $p = 3$, $9 = 3 + 2I_2$, donc $I_2 = 3$. Les polynômes unitaires de degré 2 sans racine dans $\mathbb{F}_3$ sont $X^2 + 1$, $X^2 + X + 2$ et $X^2 + 2X + 2$. La figure ci-dessous compare les I_n obtenus pour $p = 2$ à l'approximation $\frac{2^n}{n}$.



4. Pour $n = 1$, $I_1 = p \geq 1$. Soit $n \geq 2$ et $m = \lfloor n/2 \rfloor$. D'après la question 2 appliquée à d , on a $d I_d \leq p^d$. Les diviseurs stricts de n sont au plus égaux à m , donc

$$\sum_{\substack{d|n, \\ d < n}} d I_d \leq \sum_{k=1}^m p^k < \frac{p^{m+1} - 1}{p - 1} \leq p^{m+1} - 1 < p^n,$$

car $m+1 \leq n$. Par conséquent, $nI_n = p^n - \sum_{\substack{d|n, \\ d < n}} dI_d > 0$. Ainsi, $I_n \geq 1$ pour tout n . On en déduit une preuve constructive de l'existence de $\mathbb{F}_{p^n}$: c'est $\mathbb{F}_p[X]/(P)$ avec P irréductible de degré n .

Corrigé de l'exercice 21 : Carrés dans un corps fini

1. L'application $s: x \rightarrow x^2$ est un morphisme du groupe $\mathbb{F}_q^*$. Son noyau est formé des racines de $X^2 - 1$, soit $\{1, -1\}$, qui a deux éléments car $-1 \neq 1$ en caractéristique impaire. Donc l'image a $\frac{q-1}{2}$ éléments. Soit g un générateur et $x = g^m$. Les carrés sont les puissances paires de g . De plus, $x^{(q-1)/2} = g^{m(q-1)/2} = 1$ si et seulement si $q-1$ divise $m\frac{q-1}{2}$, c'est-à-dire si m est pair. **Ainsi, x est un carré si et seulement si $x^{(q-1)/2} = 1$.**
2. D'après le critère précédent, -1 est un carré si et seulement si $(-1)^{(q-1)/2} = 1$. Comme $-1 \neq 1$, cela équivaut à $\frac{q-1}{2}$ pair. **Donc -1 est un carré si et seulement si $q \equiv 1 \pmod{4}$.**
3. Soit $c \in \mathbb{F}_q$. L'ensemble $A = \left\{ \begin{matrix} a^2, \\ a \in \mathbb{F}_q \end{matrix} \right\}$ a $\frac{q-1}{2} + 1 = \frac{q+1}{2}$ éléments, en comptant 0 .
L'ensemble $B = \left\{ \begin{matrix} c - b^2, \\ b \in \mathbb{F}_q \end{matrix} \right\}$ en a autant, car $y \rightarrow c - y$ est injective. Or $|A| + |B| = q + 1 > q$. Donc $A \cap B \neq \emptyset$: il existe a, b tels que $a^2 = c - b^2$. **Tout élément est somme de deux carrés.**
4. On a $7 \equiv 3 \pmod{4}$, donc -1 n'est pas un carré dans $\mathbb{F}_7$. Les carrés de $\mathbb{F}_7$ sont $0, 1, 4, 2$, car $3^2 = 9 = 2$. Ainsi, $3 = 1 + 2$. **On a $3 = 1^2 + 3^2$ dans $\mathbb{F}_7$.**

Corrigé de l'exercice 22 : Isomorphisme explicite entre deux corps à 8 éléments

1. Le polynôme $X^3 + X + 1$ vaut 1 en 0 et en 1. De même, $Y^3 + Y^2 + 1$ vaut 1 en 0 et en 1. De degré 3 sans racine, ils sont irréductibles sur $\mathbb{F}_2$. **Les quotients sont donc deux corps à $2^3 = 8$ éléments.**
2. On part de $\beta^3 + \beta + 1 = 0$ et l'on divise par β^3 : $1 + \beta^{-2} + \beta^{-3} = 0$. Donc β^{-1} est racine de $Y^3 + Y^2 + 1$. D'après l'exercice 15, $\beta^{-1} = \beta^6 = \beta^2 + 1$. **Ainsi, $\beta^2 + 1$ est racine de $Y^3 + Y^2 + 1$ dans K_1 .**
3. Considérons le morphisme d'évaluation $\mathbb{F}_2[Y] \rightarrow K_1, Y \rightarrow \beta^2 + 1$. Son noyau contient $Y^3 + Y^2 + 1$ et ne contient pas 1. Comme cet idéal contient un irréductible qui engendre un idéal maximal, il est égal à $(Y^3 + Y^2 + 1)$. Par passage au quotient, on obtient un morphisme injectif $\sigma : K_2 \rightarrow K_1$. Les deux corps ont 8 éléments, donc σ est bijectif. Enfin, $\sigma(\gamma^2) = (\beta^2 + 1)^2 = \beta^4 + 1 = \beta^2 + \beta + 1$. **L'isomorphisme vérifie $\sigma(\gamma) = \beta^2 + 1$ et $\sigma(\gamma^2) = \beta^2 + \beta + 1$.**
4. Un isomorphisme est déterminé par l'image de γ , qui doit être une racine de $Y^3 + Y^2 + 1$ dans K_1 . Or les racines de $X^3 + X + 1$ sont β , $\beta^2 = F(\beta)$ et $\beta^4 = F^2(\beta)$, trois éléments distincts. Leurs inverses $\beta^6, \beta^5, \beta^3$ sont les trois racines de $Y^3 + Y^2 + 1$, à savoir $\beta^2 + 1$, $\beta^2 + \beta + 1$ et $\beta + 1$. Chacune définit un isomorphisme par la construction précédente. **Il existe exactement trois isomorphismes de K_2 sur K_1 .**

Corrigé de l'exercice 23 : Problème : cyclicité du groupe multiplicatif

1. Classons les entiers $k \in \{1, \dots, n\}$ selon la valeur de $\frac{n}{\gcd(k, n)}$, qui est un diviseur d de n . On a $\gcd(k, n) = \frac{n}{d}$ si et seulement si $k = \frac{n}{d}k'$ avec $1 \leq k' \leq d$ et $\gcd(k', d) = 1$. Il y a donc $\varphi(d)$ tels entiers. En sommant sur les diviseurs, **on obtient**
$$\sum_{d|n} \varphi(d) = n.$$
2. Supposons $N(d) \neq 0$ et soit $x \in G$ d'ordre d . Les éléments $1, x, \dots, x^{d-1}$ sont distincts et racines de $X^d - 1$. Or ce polynôme a au plus d racines dans le corps K . Donc tout élément d'ordre d est une puissance x^k . Enfin, x^k est d'ordre d si et seulement si $\gcd(k, d) = 1$. **Ainsi, $N(d) \in \{0, \varphi(d)\}$.**
3. Par le théorème de Lagrange, l'ordre de tout élément divise n . Donc
$$\sum_{d|n} N(d) = n = \sum_{d|n} \varphi(d).$$
 Comme $N(d) \leq \varphi(d)$ pour tout d , chaque inégalité est

une égalité. En particulier, $N(n) = \varphi(n) \geq 1$. **Il existe un élément d'ordre n : G est cyclique.**

- On a $16 = 2^4$, donc il suffit de vérifier $3^8 \neq 1$ dans $\mathbb{F}_{17}$. Or $3^2 = 9$, $3^4 = 81 = 13$, puis $3^8 = 169 = 16 = -1$. **Donc 3 engendre $\mathbb{F}_{17}^*$, qui a $\varphi(16) = 8$ générateurs.** De même, $\mathbb{F}_{25}^*$ est cyclique d'ordre 24. **Il a $\varphi(24) = \varphi(8)\varphi(3) = 8$ générateurs.**
- Le corps $\mathbb{F}_p(g)$ contient 0 et toutes les puissances de g , donc tous les éléments de $\mathbb{F}_{p^n}$. Ainsi, $\mathbb{F}_{p^n} = \mathbb{F}_p(g)$ et $[\mathbb{F}_p(g) : \mathbb{F}_p] = n$. Le polynôme minimal μ_g est donc irréductible de degré n . **De plus, $\mathbb{F}_{p^n} = \mathbb{F}_p(g) \simeq \mathbb{F}_p[X]/(\mu_g)$.**
- Supposons $\mathbb{Q}^* = \langle r \rangle$. Alors $-1 = r^k$ pour un entier k , non nul car $r^0 = 1 \neq -1$. Donc $r^{2k} = 1$, et r est d'ordre fini. Le groupe $\mathbb{Q}^*$ serait fini, ce qui est absurde. **Le même argument s'applique mot pour mot à $\mathbb{R}^*$: aucun des deux n'est cyclique.**

Point de méthode : la preuve n'utilise que le fait qu'un polynôme de degré d a au plus d racines dans un corps. Elle s'applique donc à tout sous-groupe fini de K^* , par exemple aux racines n -ièmes de l'unité dans $\mathbb{C}$.

Corrigé de l'exercice 24 : Problème : polynômes d'Artin-Schreier

- Pour $x \in \mathbb{F}_p$, le petit théorème de Fermat donne $x^p = x$. **Donc $P(x) = -a \neq 0$: P n'a pas de racine dans $\mathbb{F}_p$.**
- Soit $k \in \mathbb{F}_p$. Par le Frobenius, $(\alpha + k)^p = \alpha^p + k^p = \alpha^p + k$. Donc

$$P(\alpha + k) = \alpha^p + k - \alpha - k - a = P(\alpha) = 0.$$

Les p éléments $\alpha + k$ sont distincts et racines du polynôme unitaire P de degré p . **Donc**

$$P = \prod_{k \in \mathbb{F}_p} (X - \alpha - k).$$

- L'anneau $L[X]$ est factoriel. Le facteur unitaire Q de P s'écrit donc

$$\prod_{k \in S} (X - \alpha - k) \text{ avec } S \subset \mathbb{F}_p \text{ et } |S| = d. \text{ Son coefficient de } X^{d-1} \text{ vaut } -\sum_{k \in S} (\alpha + k) = -(d\alpha + s), \text{ où } s = \sum_{k \in S} k \in \mathbb{F}_p. \text{ Or ce coefficient appartient à } \mathbb{F}_p,$$

puisque $Q \in \mathbb{F}_p[X]$. Ensuite, $1 \leq d \leq p-1$, donc d est inversible dans $\mathbb{F}_p$. On en déduit $\alpha \in \mathbb{F}_p$, ce qui contredit la question 1. **Ainsi, P est irréductible sur $\mathbb{F}_p$.**

4. Comme P est irréductible, $\mathbb{F}_p(\alpha)$ est un corps de rupture de degré p . Il contient toutes les racines $\alpha + k$. Donc $\mathbb{F}_p(\alpha)$ est engendré par les racines de P , et $L = \mathbb{F}_p(\alpha)$. **Par conséquent, $|L| = p^p$, et $\mathbb{F}_p[X]/(P) \simeq \mathbb{F}_p(\alpha)$ est un corps de décomposition de P .**

5. On a $F(\alpha) = \alpha^p = \alpha + a$, car $P(\alpha) = 0$. Par récurrence, $F^k(\alpha) = \alpha + ka$: en effet, $F(\alpha + ka) = \alpha^p + ka = \alpha + (k+1)a$. D'abord, F est un automorphisme de L , car L est fini. Ensuite, $F^p(\alpha) = \alpha + pa = \alpha$, et F^p fixe $\mathbb{F}_p$. Comme $L = \mathbb{F}_p[\alpha]$, on a $F^p = \text{id}_L$. Enfin, pour $1 \leq k \leq p-1$, $ka \neq 0$, donc $F^k(\alpha) \neq \alpha$. **Le Frobenius est un automorphisme d'ordre exactement p .**

6. Pour $p = 2$ et $a = 1$, on trouve $P = X^2 + X + 1$ et $L = \mathbb{F}_4$, avec $F(\alpha) = \alpha^2 = \alpha + 1$. Pour $p = 3$ et $a = 1$, on trouve $P = X^3 - X - 1 = X^3 + 2X + 2$. **Ainsi, $\mathbb{F}_{27} = \mathbb{F}_3[X]/(X^3 + 2X + 2)$, et les racines de P sont α , $\alpha + 1$ et $\alpha + 2$.**

Point de méthode : pour prouver qu'un polynôme est irréductible, il suffit parfois de connaître toutes ses racines dans une extension, puis de montrer qu'aucun produit partiel n'est à coefficients dans le corps de base.

[Revenir aux énoncés des exercices](#)

Pour aller plus loin en L3

- Le cours : [corps et extensions, cours de maths en L3](#)
- Les énoncés : [exercices de maths en L3 sur corps et extensions](#)
- À maîtriser avant : [Anneaux, idéaux et arithmétique](#)
- Chapitre précédent : [Anneaux, idéaux et arithmétique](#)

- Chapitre suivant : [Réduction de Jordan et décomposition de Dunford](#)
- Tester vos connaissances : [QCM de maths en L3 par chapitre](#)
- Le sommaire : [tous les chapitres de maths de L3](#) et la [licence de maths de L1 à L3](#)