Corrigé - Théorie de Galois

Chapitre 1 - Groupes

Questions de cours

Q1. Si e et e' sont neutres, $e = ee' = e'$. Si y et y' sont symétriques de x, l'associativité donne $y = y(xy') = (yx)y' = y'$.

Q2. Voir la proposition 1.3. L'ensemble $\mathfrak{A}_n$ contient id, et si σ, τ sont paires, $\varepsilon(\sigma\tau^{-1}) = \varepsilon(\sigma)\varepsilon(\tau)^{-1} = 1$. Les permutations impaires ne forment pas un sous-groupe : elles ne contiennent pas id.

Q3. Voir la proposition 1.8. Le point clé : si $\operatorname{Ker} f = \{e\}$ et $f(x) = f(y)$, alors $f(xy^{-1}) = e$, donc $x = y$.

Q4. Voir la proposition 1.9 : si $G = \langle x \rangle$ est d'ordre n, l'application $\overline{k} \mapsto x^k$ est bien définie, et c'est un isomorphisme de $\mathbb{Z}/n\mathbb{Z}$ sur G. Un groupe d'ordre p premier est engendré par tout élément non neutre, d'ordre p par le théorème de Lagrange : il est cyclique, donc isomorphe à $\mathbb{Z}/p\mathbb{Z}$.

Q5. Les cycles disjoints commutent, donc $\sigma^k = c_1^k \cdots c_r^k$, qui vaut id si et seulement si chaque $c_i^k = \mathrm{id}$, c'est-à-dire si chaque longueur divise k.

Q6. Voir la propriété 1.15 : l'ordre de x divise $|G|$ par le théorème de Lagrange. Appliquée au groupe $(\mathbb{Z}/p\mathbb{Z})^*$, d'ordre $p-1$, elle donne $a^{p-1} \equiv 1\ [p]$ pour $p \nmid a$.

Exercice 1 ⋆

1. (a) Non : aucun élément non nul n'a de symétrique. **(b)** Non : 2 n'est pas inversible. **(c)** Oui. **(d)** Oui : μ_n est stable par produit et par inverse. **(e)** Oui. **(f)** Non : $2 \times 3 = 0$, donc la loi n'est même pas interne, et 2 n'est pas inversible.

$$\boxed{\text{Seuls } \mathbb{Q}^*,\ \mu_n \text{ et } \mathbb{Z}/6\mathbb{Z} \text{ sont des groupes.}}$$

2. L'ordre de $\overline{k}$ dans $\mathbb{Z}/12\mathbb{Z}$ vaut $\dfrac{12}{\operatorname{pgcd}(k\,;12)}$:

k	0	1	2	3	4	5	6	7	8	9	10	11
ordre	1	12	6	4	3	12	2	12	3	4	6	12

Les générateurs sont les $\overline{k}$ avec $\operatorname{pgcd}(k\,;12) = 1$, au nombre de $\varphi(12) = 4$.

3. L'ordre d'un cycle est sa longueur, et deux cycles à supports disjoints commutent, donc l'ordre d'un produit de tels cycles est le PPCM de leurs longueurs :

$$\boxed{3 \qquad 2 \qquad 5 \qquad \operatorname{ppcm}(3\,;2) = 6}$$

Exercice 2 ⋆⋆

D'après le théorème de Lagrange, un sous-groupe de $G = (\mathbb{Z}/p\mathbb{Z})^2$ est d'ordre 1, p ou p^2. Les ordres extrêmes ne donnent que $\{0\}$ et G. Un sous-groupe d'ordre p est cyclique, engendré par n'importe lequel de ses $p-1$ éléments non nuls, puisque tout élément non nul de G est d'ordre p. Deux sous-groupes d'ordre p distincts ont une intersection d'ordre divisant p et strictement inférieur à p, donc triviale. Les sous-groupes d'ordre p réalisent donc une partition des p^2-1 éléments non nuls en paquets de $p-1$ éléments :

$$\frac{p^2-1}{p-1} = p+1 \qquad \text{d'où} \qquad \boxed{G \text{ possède } p+3 \text{ sous-groupes.}}$$

Le même raisonnement, appliqué aux $p^n - 1$ éléments non nuls de $(\mathbb{Z}/p\mathbb{Z})^n$, donne :

$$\boxed{\frac{p^n-1}{p-1} = 1 + p + \cdots + p^{n-1} \text{ sous-groupes d'ordre } p}$$

Pour $p = 2$, on retrouve les trois sous-groupes d'ordre 2 du groupe de Klein, et les cinq sous-groupes au total.

Remarque. Le groupe $(\mathbb{Z}/p\mathbb{Z})^n$ est un $\mathbb{F}_p$-espace vectoriel dont les sous-groupes sont les sous-espaces : on vient de compter les droites de $\mathbb{F}_p^n$.

Exercice 3 ⋆

1. On suit les orbites : $1 \to 3 \to 7 \to 1$, puis $2 \to 5 \to 2$, puis $4 \to 9 \to 8 \to 4$, et 6 est fixe.

$$\boxed{\sigma = (1\ 3\ 7)(2\ 5)(4\ 9\ 8)}$$

2. L'ordre est le PPCM des longueurs, et la signature vaut $(-1)^{\sum(\ell_i - 1)}$:

$$\boxed{\text{ordre}(\sigma) = \text{ppcm}(3\,;2\,;3) = 6 \qquad \varepsilon(\sigma) = (+1)(-1)(+1) = -1}$$

3. Par exemple $(1\ 2\ 3\ 4) = (1\ 4)(1\ 3)(1\ 2) = (1\ 2)(2\ 3)(3\ 4)$.

$$\boxed{\text{Le nombre de facteurs n'est pas déterminé, mais sa } \textit{parité} \text{ l'est (théorème 1.3).}}$$

4. On dresse la liste exhaustive des 24 permutations, regroupées par ordre.

ordre	**éléments**	**nombre**
1	id	1
2	$(1\ 2)$, $(1\ 3)$, $(1\ 4)$, $(2\ 3)$, $(2\ 4)$, $(3\ 4)$	6
2	$(1\ 2)(3\ 4)$, $(1\ 3)(2\ 4)$, $(1\ 4)(2\ 3)$	3
3	$(1\ 2\ 3)$, $(1\ 3\ 2)$, $(1\ 2\ 4)$, $(1\ 4\ 2)$ $(1\ 3\ 4)$, $(1\ 4\ 3)$, $(2\ 3\ 4)$, $(2\ 4\ 3)$	8
4	$(1\ 2\ 3\ 4)$, $(1\ 2\ 4\ 3)$, $(1\ 3\ 2\ 4)$ $(1\ 3\ 4\ 2)$, $(1\ 4\ 2\ 3)$, $(1\ 4\ 3\ 2)$	6

Contrôle du dénombrement. Les transpositions sont les $\binom{4}{2} = 6$ paires. Une double transposition est déterminée par le partenaire de 1, soit 3 possibilités. Les 3-cycles sont au nombre de $\binom{4}{3} \times 2 = 8$, trois éléments donnés se cyclant de deux façons. Enfin tout 4-cycle s'écrit $(1\ a\ b\ c)$ en démarrant par 1, soit $3! = 6$ possibilités.

$$\boxed{1 + 6 + 3 + 8 + 6 = 24 \quad \checkmark}$$

Remarque. Les cinq lignes du tableau sont exactement les cinq classes de conjugaison de $\mathfrak{S}_4$, que l'exercice 11 retrouvera par la structure de cycles. L'ordre seul ne les sépare pas : les transpositions et les doubles transpositions sont toutes d'ordre 2 sans être conjuguées.

Exercice 4 ⋆⋆

1. Si G contient un élément d'ordre 4, alors $G \simeq \mathbb{Z}/4\mathbb{Z}$. Sinon tout élément $\neq e$ est d'ordre 2, donc G est abélien (question 2) et, en choisissant $a \neq b$ non triviaux, $G = \{e\,; a\,; b\,; ab\} \simeq (\mathbb{Z}/2\mathbb{Z})^2$.

2. De $(xy)^2 = e$ on tire $xy = (xy)^{-1} = y^{-1}x^{-1} = yx$.

$$\boxed{G \text{ est abélien, et si } G \text{ est fini son ordre est une puissance de 2.}}$$

En effet G est alors un $\mathbb{F}_2$-espace vectoriel.

3. *Un exemple.* Le groupe $\mathfrak{S}_3$ est d'ordre $3! = 6$, et il n'est pas abélien :

$$(1\ 2)(1\ 3) = (1\ 3\ 2) \qquad \text{tandis que} \qquad (1\ 3)(1\ 2) = (1\ 2\ 3)$$

Unicité. Soit G un groupe non abélien d'ordre 6. On procède par étapes, en n'utilisant que le théorème de Lagrange.

Étape 1 — les ordres possibles sont 1, 2 et 3. L'ordre d'un élément divise $|G| = 6$, donc appartient à $\{1\,;2\,;3\,;6\}$. Un élément d'ordre 6 engendrerait G, qui serait cyclique donc abélien : ce cas est exclu.

Étape 2 — il existe un élément a d'ordre 3. Sinon, tout $x \neq e$ serait d'ordre 2, donc $x^2 = e$ pour tout $x \in G$, et la question 2 rendrait G abélien. On pose $H = \langle a\rangle = \{e\,;a\,;a^2\}$, d'ordre 3.

Étape 3 — H est stable par conjugaison. Son indice vaut $[G : H] = \dfrac{6}{3} = 2$. Il n'y a donc que deux classes à gauche, H et $G \setminus H$, et de même à droite. Pour $b \notin H$ on a ainsi $bH = G \setminus H = Hb$, c'est-à-dire $bHb^{-1} = H$.

Étape 4 — tout élément hors de H est d'ordre 2. Soit $b \notin H$. Les deux classes à gauche étant H et bH, la classe b^2H est l'une des deux ; si $b^2H = bH$, alors $bH = H$ et $b \in H$, ce qui est exclu. Donc $b^2 \in H$.

Si b était d'ordre 3, on aurait $b^3 = e$, donc $b = b^4 = \left(b^2\right)^2$; or $b^2 \in H$ et H est un sous-groupe, donc $\left(b^2\right)^2 \in H$, d'où $b \in H$: absurde. L'ordre de b est donc 2.

Étape 5 — G possède exactement les six éléments e, a, a^2, b, ab, a^2b. Les trois premiers forment H. Les trois suivants forment Hb, et ils sont distincts, car $a^ib = a^jb$ entraîne $a^i = a^j$. Comme H et Hb sont disjointes et de cardinal 3, elles épuisent G.

Étape 6 — la seule relation possible est $bab^{-1} = a^2$. L'étape 3 donne $bab^{-1} \in H$. La conjugaison préserve l'ordre, puisque $\left(bab^{-1}\right)^k = ba^kb^{-1}$: l'élément bab^{-1} est donc d'ordre 3, ce qui exclut e et laisse $bab^{-1} \in \{a\,;a^2\}$.

Si $bab^{-1} = a$, alors a et b commutent ; or tout élément de G s'écrit a^ib^j d'après l'étape 5, donc G serait abélien : contradiction.

$$\boxed{a^3 = e, \qquad b^2 = e, \qquad bab^{-1} = a^2 = a^{-1}}$$

Étape 7 — conclusion. Ces trois relations déterminent entièrement le produit de deux éléments quelconques a^ib^j, donc la table de G. Or $\mathfrak{S}_3$ les vérifie avec $a = (1\ 2\ 3)$ et $b = (1\ 2)$:

$$(1\ 2)(1\ 2\ 3)(1\ 2) = (1\ 3\ 2) = a^2 \quad \checkmark$$

L'application $a^ib^j \mapsto (1\ 2\ 3)^i(1\ 2)^j$ est donc un isomorphisme de G sur $\mathfrak{S}_3$.

$$\boxed{\text{Il y a exactement deux groupes d'ordre 6 : } \mathbb{Z}/6\mathbb{Z} \text{ et } \mathfrak{S}_3.}$$

Remarque. On invoque souvent le théorème de Cauchy pour produire d'emblée les éléments a et b. C'est légitime, mais inutile ici : ce théorème n'est établi qu'au chapitre 2, alors que les étapes 1 et 2 ci-dessus ne demandent que Lagrange. On notera d'ailleurs que $\mathfrak{S}_3 = D_3$ est le groupe diédral du triangle, et que les relations encadrées sont exactement celles de D_4 à l'exercice 5, avec 4 remplacé par 3.

Exercice 5 ⋆⋆

1. La rotation d'angle $\dfrac{\pi}{2}$ est d'ordre 4, une symétrie axiale est involutive, et srs^{-1} est la rotation d'angle $-\dfrac{\pi}{2}$, soit r^{-1}. Tout élément s'écrit alors r^is^j avec $0 \leqslant i \leqslant 3$ et $j \in \{0\,;1\}$:

$$\boxed{|D_4| = 8}$$

2. On classe les huit éléments par ordre :

élément	id	r	r^2	r^3	s	rs	r^2s	r^3s
ordre	1	4	2	4	2	2	2	2

3. On trouve dix sous-groupes :

$$\boxed{\begin{array}{l}\text{ordre } 1 : \{\mathrm{id}\}\\ \text{ordre } 2 : \langle r^2\rangle,\ \langle s\rangle,\ \langle rs\rangle,\ \langle r^2s\rangle,\ \langle r^3s\rangle \quad \text{(cinq)}\\ \text{ordre } 4 : \langle r\rangle,\ \{\mathrm{id}, r^2, s, r^2s\},\ \{\mathrm{id}, r^2, rs, r^3s\} \quad \text{(trois)}\\ \text{ordre } 8 : D_4\end{array}}$$

Exercice 6 ⋆⋆

1. Un endomorphisme f de $\mathbb{Z}/n\mathbb{Z}$ est déterminé par $f(\overline{1}) = \overline{a}$, et f est bijectif si et seulement si $\overline{a}$ engendre, c'est-à-dire $\mathrm{pgcd}(a\,;n) = 1$. L'application $f \mapsto \overline{a}$ est un morphisme multiplicatif :

$$\boxed{\mathrm{Aut}(\mathbb{Z}/n\mathbb{Z}) \simeq (\mathbb{Z}/n\mathbb{Z})^*,\ \text{d'ordre } \varphi(n).}$$

2. $(\mathbb{Z}/8\mathbb{Z})^* = \{\overline{1};\overline{3};\overline{5};\overline{7}\}$, et $3^2 = 5^2 = 7^2 = 1$ modulo 8 : tous les éléments non triviaux sont d'ordre 2.

$$\boxed{\mathrm{Aut}(\mathbb{Z}/8\mathbb{Z}) \simeq (\mathbb{Z}/2\mathbb{Z})^2 \qquad \mathrm{Aut}(\mathbb{Z}/7\mathbb{Z}) \simeq \mathbb{Z}/6\mathbb{Z},\ \text{engendré par } \overline{3}.}$$

3. Un sous-groupe d'ordre 4 est cyclique — engendré par un 4-cycle, et il y en a trois — ou de type Klein. Les Klein sont : le groupe $V = \{\mathrm{id}\,;(1\,2)(3\,4)\,;(1\,3)(2\,4)\,;(1\,4)(2\,3)\}$, et les trois groupes $\{\mathrm{id}\,;(a\ b)\,;(c\ d)\,;(a\ b)(c\ d)\}$.

$$\boxed{\text{Sept sous-groupes d'ordre 4 : trois cycliques et quatre de type Klein.}}$$

Chapitre 2 - Quotients, actions et résolubilité

Questions de cours

Q1. Voir la proposition 2.1. Si $[G : H] = 2$, les classes à gauche comme à droite sont H et $G \setminus H$, donc $gH = Hg$ pour tout g.

Q2. Voir le théorème 2.2 : $\overline{x} \mapsto f(x)$ est bien défini et injectif sur $G/\mathrm{Ker}\, f$. Appliqué à la signature, surjective de noyau $\mathfrak{A}_n$, il donne $\mathfrak{S}_n/\mathfrak{A}_n \simeq \{\pm 1\} \simeq \mathbb{Z}/2\mathbb{Z}$.

Q3. Voir la proposition 2.3 : on évalue $\sigma c \sigma^{-1}$ en $\sigma(a_i)$. La conjugaison préserve donc le type, et deux permutations de même type sont conjuguées par toute bijection envoyant les cycles de l'une sur ceux de l'autre.

Q4. Voir le théorème 2.4 et l'équation aux classes du paragraphe 2.4. Pour un p-groupe, chaque orbite non réduite à un point a un cardinal multiple de p, donc p divise $|Z(G)|$.

Q5. Voir la proposition 2.5. Pour $D(\mathfrak{S}_n)$: les commutateurs sont pairs, donc $D(\mathfrak{S}_n) \subseteq \mathfrak{A}_n$; réciproquement, tout 3-cycle est un commutateur, $(a\ b\ c) = [(a\ b)\,;(a\ c)]$, et les 3-cycles engendrent $\mathfrak{A}_n$ (proposition 2.7).

Q6. Les classes de conjugaison de $\mathfrak{A}_5$ ont pour cardinaux 1, 15, 20, 12 et 12, les 5-cycles formant deux classes. Un sous-groupe distingué est une réunion de classes contenant l'identité, de cardinal divisant 60 ; aucune somme autre que 1 et 60 ne convient.

Exercice 7 ⋆⋆⋆

1. $|\mathfrak{A}_4| = \dfrac{4!}{2} = 12$, et $6 \mid 12$.

2. Les douze éléments se répartissent selon leur ordre :

$$\boxed{\mathfrak{A}_4 = \{\mathrm{id}\} \cup \underbrace{\{\text{trois doubles transpositions}\}}_{\text{ordre } 2} \cup \underbrace{\{\text{huit 3-cycles}\}}_{\text{ordre } 3}}$$

3. Un tel H serait d'indice $\dfrac{12}{6} = 2$, donc distingué, et $\mathfrak{A}_4/H$ serait d'ordre 2.

4. Dans un groupe d'ordre 2, tout carré est trivial : $\overline{x}^2 = \overline{e}$, donc $x^2 \in H$ pour tout $x \in \mathfrak{A}_4$. Or si c est un 3-cycle, $c^2 = c^{-1}$ est encore un 3-cycle, et les huit 3-cycles sont ainsi tous des carrés. Donc H contiendrait $8 + 1 = 9 > 6$ éléments.

$\boxed{\mathfrak{A}_4 \text{ n'a pas de sous-groupe d'ordre 6 : la réciproque de Lagrange est fausse.}}$

5. Les trois doubles transpositions, avec id, forment déjà un sous-groupe :

$\boxed{V \text{ est d'ordre 4, et c'est le plus petit convenant.}}$

Exercice 8 ⋆⋆

1. On part de ij = k et l'on multiplie à gauche par j, puis on utilise $\mathrm{j}^2 = -1$:

$$\mathrm{j(ij)} = \mathrm{jk} = \mathrm{i} \qquad \text{donc} \qquad \mathrm{(ji)j} = \mathrm{i}$$

En multipliant à droite par j : $\mathrm{(ji)j}^2 = \mathrm{ij}$, soit $-\mathrm{ji} = \mathrm{k}$.

$\boxed{\mathrm{ji} = -\mathrm{k} \neq \mathrm{k} = \mathrm{ij} \text{ : le groupe } Q_8 \text{ n'est pas abélien.}}$

2. On a $\mathrm{i}^2 = -1$ et $\mathrm{i}^4 = 1$, donc i est d'ordre 4, et de même pour les six éléments ±i, ±j, ±k.

élément	1	−1	i	−i	j	−j	k	−k
ordre	1	2	4	4	4	4	4	4

$\boxed{Q_8 \text{ possède un } \textit{unique} \text{ élément d'ordre 2, à savoir } -1.}$

3. Le groupe $\mathbb{Z}/8\mathbb{Z}$ possède un élément d'ordre 8, ce qui n'est pas le cas ici. Et D_4 possède *cinq* éléments d'ordre 2 d'après l'exercice 5, contre un seul pour Q_8.

$\boxed{\text{Les trois groupes } \mathbb{Z}/8\mathbb{Z},\ D_4 \text{ et } Q_8 \text{ sont deux à deux non isomorphes.}}$

Le nombre d'éléments de chaque ordre est un invariant d'isomorphisme : c'est l'outil le plus économique pour séparer deux groupes de même ordre.

4. Un sous-groupe propre non trivial a pour ordre 2 ou 4. Celui d'ordre 2 est engendré par l'unique élément d'ordre 2 ; ceux d'ordre 4 sont cycliques, engendrés par un élément d'ordre 4, et $\langle x \rangle = \langle -x \rangle$.

$\boxed{\{1\}\ ,\ \{\pm 1\}\ ,\ \langle \mathrm{i} \rangle\ ,\ \langle \mathrm{j} \rangle\ ,\ \langle \mathrm{k} \rangle\ ,\ Q_8 \quad \text{soit six sous-groupes.}}$

5. Les sous-groupes $\{1\}$ et Q_8 sont distingués. Les trois sous-groupes d'ordre 4 sont d'indice 2, donc distingués. Enfin $\{\pm 1\}$ est le centre, donc distingué.

$\boxed{\text{Tous les sous-groupes de } Q_8 \text{ sont distingués, bien que } Q_8 \text{ ne soit pas abélien.}}$

À retenir : « tout sous-groupe distingué » n'entraîne donc *pas* « abélien ». C'est la différence entre Q_8 et D_4, qui possède quatre sous-groupes non distingués.

6. Un élément central commute avec i et j ; les six éléments d'ordre 4 sont exclus, puisque ij ≠ ji et que les relations sont symétriques.

$$\boxed{Z(Q_8) = \{\pm 1\} \qquad \text{et} \qquad Q_8/Z(Q_8) \simeq (\mathbb{Z}/2\mathbb{Z})^2}$$

Le quotient est d'ordre 4 et tous ses éléments non triviaux sont d'ordre 2, puisque i^2, j^2 et k^2 valent $-1 \in Z$. On retrouve au passage que Q_8/Z n'est pas cyclique, conformément à l'exercice 10.

Exercice 9 ⋆⋆⋆

1. Le produit de deux matrices unitriangulaires supérieures est unitriangulaire supérieure, et l'on vérifie :

$$M(a\,;b\,;c)^{-1} = M(-a\,;\,-b\,;\,ab-c)$$

Comme $(a\,;b\,;c)$ décrit $\mathbb{F}_p^3$:

$$\boxed{|H(\mathbb{F}_p)| = p^3}$$

2. Le produit matriciel donne directement :

$$\boxed{M(a\,;b\,;c)\,M(a'\,;b'\,;c') = M(a+a'\,;\,b+b'\,;\,c+c'+ab')}$$

Le terme ab' n'est pas symétrique en les deux facteurs : avec $M(1\,;0\,;0)$ et $M(0\,;1\,;0)$, on obtient $M(1\,;1\,;1)$ dans un sens et $M(1\,;1\,;0)$ dans l'autre.

$$\boxed{H(\mathbb{F}_p) \text{ n'est pas abélien.}}$$

3. L'élément $M(a\,;b\,;c)$ est central si et seulement si $ab' = a'b$ pour tous a', b', c'est-à-dire $a = b = 0$.

$$\boxed{Z = \{M(0\,;0\,;c)\} \simeq \mathbb{Z}/p\mathbb{Z} \qquad \text{et} \qquad H(\mathbb{F}_p)/Z \simeq (\mathbb{Z}/p\mathbb{Z})^2}$$

Le quotient s'identifie à $(a\,;b\,)$ par la question 2, avec addition composante par composante.

4. On a $N = M(a\,;b\,;c) - I_3$, matrice nilpotente : $N^2 = ab\,E_{1,3}$ et $N^3 = 0$. Comme I_3 et N commutent, le binôme donne :

$$M^p = (I_3+N)^p = I_3 + pN + \frac{p(p-1)}{2}N^2$$

Pour p impair, p divise $\dfrac{p(p-1)}{2}$, donc les deux derniers termes sont nuls dans $\mathbb{F}_p$.

$$\boxed{M(a\,;b\,;c)^p = I_3 \text{ pour } p \text{ impair.}}$$

5.

$$\boxed{\text{Pour } p \text{ impair, } H(\mathbb{F}_p) \text{ est non abélien et vérifie } x^p = e \text{ pour tout } x.}$$

Il n'y a aucune contradiction avec la question 2 de l'exercice 4 : celle-ci concerne l'exposant 2, et sa démonstration repose sur $x^{-1} = x$, ce qui n'a plus lieu pour $p \geqslant 3$. Le calcul $(xy)^2 = e \Rightarrow xy = yx$ n'a pas d'analogue en exposant impair.

$$\boxed{\text{« Exposant » p « premier » n'entraîne « abélien » que pour } p = 2.}$$

6. Pour $p = 2$, le coefficient $\dfrac{p(p-1)}{2} = 1$ n'est plus divisible par 2, et $M(1\,;1\,;c)^2 = M(0\,;0\,;1) \neq I_3$: l'exposant vaut 4.

$$\boxed{H(\mathbb{F}_2) \text{ est d'ordre 8, non abélien, d'exposant 4 : c'est } D_4.}$$

Il possède en effet cinq éléments d'ordre 2 et deux d'ordre 4, ce qui l'écarte de Q_8 (exercice 8).

Exercice 10 ⋆

1. Le sous-groupe $\langle\overline{4}\rangle = \{\overline{0};\overline{4};\overline{8}\}$ est d'ordre 3, donc le quotient est d'ordre 4 ; il est cyclique, engendré par la classe de $\overline{1}$:

$$\boxed{\mathbb{Z}/12\mathbb{Z}/\langle\overline{4}\rangle \simeq \mathbb{Z}/4\mathbb{Z}}$$

2. Chaque quotient est d'ordre 2 ou 4 :

$$\boxed{\mathfrak{S}_3/\mathfrak{A}_3 \simeq \mathbb{Z}/2\mathbb{Z} \qquad D_4/\langle r^2\rangle \simeq (\mathbb{Z}/2\mathbb{Z})^2}$$

Pour le second, le quotient est d'ordre 4 et tous ses éléments non triviaux sont d'ordre 2, puisque r^2, s^2 et $(rs)^2$ appartiennent à $\langle r^2\rangle$.

3. Si G est abélien, $\overline{x}\,\overline{y} = \overline{xy} = \overline{yx} = \overline{y}\,\overline{x}$. La réciproque est fausse : $\mathfrak{S}_3/\mathfrak{A}_3$ est abélien sans que $\mathfrak{S}_3$ le soit.

4. Soit $G/Z(G) = \langle \overline{a}\rangle$. Tout $x \in G$ s'écrit $x = a^i z$ avec $z \in Z(G)$, et deux tels éléments commutent :

$$(a^i z)(a^j z') = a^{i+j} z z' = (a^j z')(a^i z)$$

Si $|G| = p^2$, le centre est non trivial, d'après l'équation aux classes du paragraphe 2.4 du cours, donc $G/Z(G)$ est d'ordre 1 ou p, donc cyclique.

$$\boxed{\text{Tout groupe d'ordre } p^2 \text{ est abélien.}}$$

Exercice 11 ⋆⋆

1. Les cinq partitions de 4 donnent cinq classes :

structure	1^4	$2\,1^2$	2^2	$3\,1$	4
cardinal	1	6	3	8	6

$$\boxed{1+6+3+8+6 = 24 \quad \checkmark}$$

2. Les sept partitions de 5 donnent sept classes, de cardinaux :

$$\boxed{1\ (1^5)\ ,\ 10\ (2\,1^3)\ ,\ 15\ (2^2 1)\ ,\ 20\ (3\,1^2)\ ,\ 20\ (3\,2)\ ,\ 30\ (4\,1)\ ,\ 24\ (5)}$$

dont la somme vaut 120.

3. Les réunions de classes contenant id dont le cardinal divise 24 sont 1, $1+3=4$, $1+3+8=12$ et 24 :

$$\boxed{\{\mathrm{id}\} \trianglelefteq V \trianglelefteq \mathfrak{A}_4 \trianglelefteq \mathfrak{S}_4}$$

Exercice 12 ⋆⋆

1. *Cauchy :* si p premier divise $|G|$, alors G contient un élément d'ordre p. Comme $15 = 3 \times 5$, on obtient un élément d'ordre 3 et un d'ordre 5.

2. Notons n_3 et n_5 les nombres de 3- et 5-Sylow. On a $n_3 \equiv 1\ [3]$ et $n_3 \mid 5$, donc $n_3 = 1$; de même $n_5 \equiv 1\ [5]$ et $n_5 \mid 3$, donc $n_5 = 1$. Ces deux sous-groupes P et Q sont donc distingués, d'intersection triviale, et PQ est d'ordre 15 :

$$\boxed{G \simeq \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z} \simeq \mathbb{Z}/15\mathbb{Z}}$$

3. Ici $12 = 2^2 \times 3$. On a $n_3 \in \{1\,;4\}$. Si $n_3 = 1$, le 3-Sylow est distingué. Si $n_3 = 4$, les quatre 3-Sylow fournissent $4 \times 2 = 8$ éléments d'ordre 3 ; il reste $12 - 8 = 4$ éléments, qui forment nécessairement l'unique 2-Sylow, lequel est alors distingué.

$$\boxed{\text{Aucun groupe d'ordre 12 n'est simple.}}$$

4. On a $n_q \equiv 1\ [q]$ et $n_q \mid p < q$, donc $n_q = 1$; et $n_p \equiv 1\ [p]$ avec $n_p \mid q$, donc $n_p \in \{1\,;q\}$, mais $q \not\equiv 1\ [p]$ par hypothèse, donc $n_p = 1$. Les deux Sylow sont distingués, d'intersection triviale :

$$\boxed{G \simeq \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/q\mathbb{Z} \simeq \mathbb{Z}/pq\mathbb{Z}}$$

Exercice 13 ⋆⋆⋆

Le cas d'un p-groupe. Supposons $|G| = p^n$, et soit g un élément d'ordre maximal p^m. Tout $h \in G$ a un ordre p^k avec $k \leqslant m$. Le groupe cyclique $\langle g \rangle$ possède un sous-groupe d'ordre p^k, à savoir $\langle g^{p^{m-k}} \rangle$; or $\langle h \rangle$ est aussi d'ordre p^k, et l'hypothèse d'unicité impose $\langle h \rangle = \langle g^{p^{m-k}} \rangle \subseteq \langle g \rangle$. Ainsi $G = \langle g \rangle$ est cyclique.

Le cas général. Écrivons $|G| = p_1^{a_1} \cdots p_r^{a_r}$. Pour chaque i, les p_i-Sylow sont tous de même ordre, donc il n'y en a qu'un, P_i : il est distingué, puisque ses conjugués sont encore des p_i-Sylow. Les sous-groupes de P_i étant des sous-groupes de G, le groupe P_i hérite de l'hypothèse, et il est cyclique d'après le premier cas ; soit g_i un générateur.

Pour $i \neq j$, les éléments de P_i et de P_j commutent : si $x \in P_i$ et $y \in P_j$, le commutateur $xyx^{-1}y^{-1}$ appartient à P_i, puisque $yx^{-1}y^{-1} \in P_i$, et à P_j, puisque $xyx^{-1} \in P_j$; or $P_i \cap P_j = \{e\}$, les ordres étant premiers entre eux. L'élément $g = g_1 \cdots g_r$ est alors un produit d'éléments qui commutent deux à deux et d'ordres premiers entre eux : son ordre est le produit de ces ordres, c'est-à-dire $|G|$.

$$\boxed{G = \langle g_1 \cdots g_r \rangle \text{ est cyclique.}}$$

La réciproque est vraie : un groupe cyclique d'ordre n possède exactement un sous-groupe de chaque ordre divisant n.

Exercice 14 ⋆⋆⋆⋆

Les 5-Sylow sont en nombre $n_5 \equiv 1\ [5]$ divisant 12, donc $n_5 \in \{1\,;6\}$, et l'hypothèse impose $n_5 = 6$. Deux 5-Sylow distincts se coupant trivialement, G contient $6 \times 4 = 24$ éléments d'ordre 5. Supposons l'existence d'un sous-groupe distingué N avec $\{e\} \neq N \neq G$.

Un lemme. Tout groupe H d'ordre 30 possède un unique 5-Sylow. En effet $n_5(H) \in \{1\,;6\}$ et $n_3(H) \in \{1\,;10\}$, et l'on ne peut avoir à la fois $n_5 = 6$ et $n_3 = 10$, ce qui ferait $24 + 20 > 30$ éléments. Si $n_3(H) = 1$, le 3-Sylow Q est distingué, QP est un sous-groupe d'ordre 15 pour tout 5-Sylow P, donc d'indice 2 et distingué. Ce sous-groupe d'ordre 15 est cyclique (exercice 12) et contient tous les 5-Sylow de H, puisque l'image de l'un d'eux dans le quotient d'ordre 2 est triviale : il n'en contient qu'un, donc $n_5(H) = 1$.

Si 5 divise $|N|$. Alors N contient un 5-Sylow de G, donc tous ses conjugués, c'est-à-dire les six. Ainsi $|N| \geqslant 1 + 24 = 25$, et $|N|$ est un diviseur strict de 60 multiple de 5 : c'est 30. Le lemme contredit alors la présence de six 5-Sylow dans N.

Si 5 ne divise pas $|N|$. On a $|N| \in \{2\,;3\,;4\,;6\,;12\}$. Si $|N| = 6$ ou 12, le groupe N possède un sous-groupe de Sylow qui y est unique : pour l'ordre 6 c'est le 3-Sylow, pour l'ordre 12 l'un des deux d'après l'exercice 12. Ce sous-groupe N' est distingué dans G, car $gN'g^{-1}$ est un sous-groupe de $gNg^{-1} = N$ de même ordre, donc égal à N'. Quitte à remplacer N par N', on peut supposer $|N| \in \{2\,;3\,;4\}$.

Le quotient G/N est alors d'ordre 30, 20 ou 15, et possède un unique 5-Sylow : par le lemme pour l'ordre 30, et parce que n_5 divise 4 ou 3 dans les autres cas. Si P est un 5-Sylow de G, son image PN/N est ce 5-Sylow, qui est distingué dans G/N ; d'après le théorème de correspondance, PN est distingué dans G. Il contient alors les six 5-Sylow, donc au moins 25 éléments, alors que $|PN| = 5\,|N| \leqslant 20$: c'est absurde.

$$\boxed{G \text{ est simple.}}$$

On peut montrer qu'un groupe simple d'ordre 60 est isomorphe à $\mathfrak{A}_5$: cet exercice est ainsi la première étape d'une caractérisation de $\mathfrak{A}_5$ par son ordre.

Exercice 15 ⋆⋆⋆

1. La composée vérifie $\varphi_{a,b} \circ \varphi_{a',b'} = \varphi_{aa',\,ab'+b}$, ce qui montre la stabilité ; l'inverse est $\varphi_{a^{-1},\,-a^{-1}b}$. Le couple $(a\,;b)$ décrit $\mathbb{F}_p^* \times \mathbb{F}_p$:

$$\boxed{|\mathrm{Aff}(\mathbb{F}_p)| = p(p-1)}$$

La formule ci-dessus n'est pas symétrique dès que $p \geqslant 3$: avec $\varphi_{2,0}$ et $\varphi_{1,1}$, on obtient $\varphi_{2,2}$ dans un sens et $\varphi_{2,1}$ dans l'autre.

2. On a $\varphi_{a,b} \circ \varphi_{1,t} \circ \varphi_{a,b}^{-1} = \varphi_{1,at}$, qui est encore une translation. L'application $\varphi_{a,b} \mapsto a$ est un morphisme surjectif sur $\mathbb{F}_p^*$, de noyau T :

$$\boxed{T \simeq \mathbb{Z}/p\mathbb{Z} \text{ est distingué, et } \mathrm{Aff}(\mathbb{F}_p)/T \simeq \mathbb{F}_p^* \simeq \mathbb{Z}/(p-1)\mathbb{Z}}$$

3. La suite $\{\mathrm{id}\} \trianglelefteq T \trianglelefteq \mathrm{Aff}(\mathbb{F}_p)$ a pour quotients successifs $\mathbb{Z}/p\mathbb{Z}$ et $\mathbb{Z}/(p-1)\mathbb{Z}$, tous deux abéliens.

$$\boxed{\mathrm{Aff}(\mathbb{F}_p) \text{ est résoluble.}}$$

4. Si $\varphi_{a,b}$ est central, il commute avec toute translation, ce qui impose $at = t$ pour tout t, donc $a = 1$; et il commute avec $\varphi_{c,0}$ pour $c \neq 1$, ce qui impose $b = cb$, donc $b = 0$.

$$\boxed{Z(\mathrm{Aff}(\mathbb{F}_p)) = \{\mathrm{id}\} \text{ pour } p \geqslant 3.}$$

5. Pour $p = 3$, l'ordre vaut $3 \times 2 = 6$, et le groupe n'est pas abélien.

$$\boxed{\mathrm{Aff}(\mathbb{F}_3) \simeq \mathfrak{S}_3, \text{ d'après l'unicité établie à l'exercice 4.}}$$

6. Pour x, $y \in \mathbb{F}_p$, la translation $\varphi_{1,y-x}$ envoie x sur y : l'action est transitive, l'orbite de 0 est $\mathbb{F}_p$ tout entier. Le stabilisateur de 0 est formé des $\varphi_{a,0}$, c'est-à-dire des homothéties.

$$\boxed{|\mathcal{O}(0)| \times |\mathrm{Stab}(0)| = p \times (p-1) = |\mathrm{Aff}(\mathbb{F}_p)| \quad \checkmark}$$

Exercice 16 ⋆⋆⋆

1. Une matrice de $\mathrm{GL}_2(\mathbb{F}_3)$ est déterminée par une base $(u\,;v)$ de $\mathbb{F}_3^2$: il y a $3^2 - 1 = 8$ choix pour u non nul, puis $3^2 - 3 = 6$ choix pour v hors de la droite engendrée par u, soit 48 matrices. Le déterminant est un morphisme surjectif de $\mathrm{GL}_2(\mathbb{F}_3)$ sur $\mathbb{F}_3^*$, d'ordre 2 :

$$\boxed{|\mathrm{SL}_2(\mathbb{F}_3)| = \frac{48}{2} = 24}$$

2. Soit $A \in G$ avec $A^2 = I_2$. Le polynôme $X^2 - 1 = (X-1)(X+1)$ annule A et est scindé à racines simples sur $\mathbb{F}_3$, donc A est diagonalisable de valeurs propres dans $\{\pm 1\}$. Comme $\det A = 1$, ces valeurs propres sont $(1\,;1)$ ou $(-1\,;-1)$, d'où $A = I_2$ ou $A = -I_2$.

$$\boxed{-I_2 \text{ est le seul élément d'ordre 2 de } \mathrm{SL}_2(\mathbb{F}_3).}$$

3. L'exercice 3 a dénombré $6 + 3 = 9$ éléments d'ordre 2 dans $\mathfrak{S}_4$.

$$\boxed{\mathrm{SL}_2(\mathbb{F}_3) \not\simeq \mathfrak{S}_4, \text{ bien que tous deux soient d'ordre 24.}}$$

À retenir : l'ordre ne détermine pas le groupe. Il existe en fait quinze groupes d'ordre 24 à isomorphisme près.

4. Le sous-groupe $\{\pm I_2\}$ est le centre de G, donc distingué, et le quotient est d'ordre $\dfrac{24}{2} = 12$.

$$\boxed{\mathrm{SL}_2(\mathbb{F}_3)/\{\pm I_2\} \simeq \mathfrak{A}_4}$$

5. Le groupe $\mathfrak{A}_4$ est résoluble, avec la suite $\{\mathrm{id}\} \trianglelefteq V \trianglelefteq \mathfrak{A}_4$, et $\{\pm I_2\} \simeq \mathbb{Z}/2\mathbb{Z}$ l'est aussi. Le théorème 2.8 assure qu'une extension d'un groupe résoluble par un groupe résoluble est résoluble.

$$\boxed{\mathrm{SL}_2(\mathbb{F}_3) \text{ est résoluble.}}$$

6.

Deux groupes de même ordre peuvent différer par la répartition des ordres de leurs éléments, par leur centre, ou par leurs sous-groupes distingués.

Ici $Z(\mathrm{SL}_2(\mathbb{F}_3))$ est d'ordre 2 alors que $Z(\mathfrak{S}_4)$ est trivial : c'est une seconde façon, indépendante de la première, de séparer les deux groupes.

Exercice 17 ⋆⋆⋆

Notons B ce groupe et U le sous-groupe des matrices triangulaires supérieures à diagonale formée de 1. L'application qui à $A \in B$ associe sa diagonale est un morphisme surjectif de B sur $(\mathbb{F}^*)^n$, puisque la diagonale d'un produit de matrices triangulaires supérieures est le produit des diagonales. Son noyau est U, donc $U \trianglelefteq B$ et le premier théorème d'isomorphisme donne $B/U \simeq (\mathbb{F}^*)^n$, qui est abélien.

Pour $1 \leqslant k \leqslant n$, notons U_k l'ensemble des $I_n + N \in U$ tels que $N_{ij} = 0$ dès que $j - i < k$, de sorte que $U_1 = U$ et $U_n = \{I_n\}$. Si $I_n + N$ et $I_n + N'$ sont dans U_k, leur produit vaut $I_n + N + N' + NN'$, et NN' n'a de coefficients non nuls qu'à partir de la diagonale d'indice $2k \geqslant k+1$. L'application qui associe à un élément de U_k sa k-ième surdiagonale est donc un morphisme de U_k vers le groupe additif $\mathbb{F}^{n-k}$, de noyau U_{k+1}. Il en résulte que $U_{k+1} \trianglelefteq U_k$ et que U_k/U_{k+1} est abélien.

$$U = U_1 \trianglerighteq U_2 \trianglerighteq \cdots \trianglerighteq U_n = \{I_n\}$$

Le groupe U est donc résoluble, ainsi que B/U, et le théorème 2.8 conclut.

Le groupe des matrices triangulaires supérieures inversibles est résoluble.

La finitude de $\mathbb{F}$ ne sert pas : le résultat vaut sur tout corps. Pour $n = 3$ et $\mathbb{F} = \mathbb{F}_p$, le groupe U est le groupe de Heisenberg de l'exercice 9.

Chapitre 3 - Anneaux, corps et polynômes

Questions de cours

Q1. Voir la proposition 3.1. Pour les idéaux de $\mathbb{Z}$: un idéal non nul I contient un plus petit élément strictement positif n, et la division euclidienne de tout $a \in I$ par n fournit un reste dans I, donc nul par minimalité : $I = n\mathbb{Z}$.

Q2. Voir le théorème 3.2. Les idéaux de $\mathbb{Z}$ contenant $n\mathbb{Z}$ sont les $d\mathbb{Z}$ avec $d \mid n$: l'idéal $n\mathbb{Z}$ est maximal si et seulement si n est premier.

Q3. Voir les propositions 3.2 et 3.3. Si $\mathrm{car}(K) = ab$ avec $a, b > 1$, alors $(a \cdot 1)(b \cdot 1) = 0$ contredit l'intégrité. Pour le rêve du débutant, p divise $\binom{p}{k}$ pour $1 \leqslant k \leqslant p-1$.

Q4. Voir le théorème 3.4 : un idéal non nul est engendré par l'un de ses éléments non nuls de degré minimal, grâce à la division euclidienne. Pour la proposition 3.6 : si α est racine, $P = (X - \alpha)Q$, et l'intégrité de K permet la récurrence sur le degré.

Q5. Voir le théorème 3.6. Pour $\Phi_p(X+1) = \dfrac{(X+1)^p - 1}{X}$, les coefficients non dominants sont les $\binom{p}{k}$, tous divisibles par p, et le terme constant vaut p : Eisenstein s'applique en p.

Exercice 18 ⋆

1. On pose la division :

$$\boxed{X^4 + X^3 + 2X + 1 = (X^2+1)(X^2+X-1) + (X+2)}$$

2. L'algorithme d'Euclide donne $X^6 - 1 = X^2(X^4-1) + (X^2-1)$, puis $X^4 - 1 = (X^2+1)(X^2-1)$: le dernier reste non nul est $X^2 - 1$, et la première égalité fournit directement la relation de Bézout.

$$\boxed{\text{pgcd} = X^2 - 1 \qquad \text{avec} \qquad -X^2(X^4-1) + 1 \cdot (X^6 - 1) = X^2 - 1}$$

3. Le polynôme X^2-1 admet dans $\mathbb{Z}/8\mathbb{Z}$ les quatre racines $\overline{1}$, $\overline{3}$, $\overline{5}$, $\overline{7}$.

$$\boxed{\text{Aucune contradiction : } \mathbb{Z}/8\mathbb{Z} \text{ n'est pas intègre, car } \overline{2}\,\overline{4}=\overline{0}.}$$

Exercice 19 ⋆⋆

1. C'est la première question d'irréductibilité du document. Avant de traiter les six polynômes, on rassemble les quatre outils dont on aura besoin, chacun avec sa justification ; on verra ensuite comment choisir le plus économique.

Outil 1 : le degré 2 *ou* 3. Sur un corps K, un polynôme de degré 2 ou 3 est réductible si et seulement s'il a une racine dans K. En effet, une factorisation non triviale $P=UV$ vérifie $\deg U+\deg V=\deg P\in\{2\,;3\}$ avec $\deg U,\deg V\geqslant 1$: l'un des deux facteurs est donc de degré 1, de la forme $c(X-a)$, et a est racine de P. Réciproquement, si a est racine, $X-a$ divise P d'après la proposition 3.6, et le quotient est de degré au moins 1.

Piège. Dès le degré 4, l'argument tombe : un polynôme peut se factoriser en deux facteurs de degré 2 sans avoir aucune racine. Les polynômes (c) et (f) ci-dessous en donnent l'illustration.

Outil 2 : les racines rationnelles. Soit $P=a_nX^n+\cdots+a_1X+a_0\in\mathbb{Z}[X]$, et $\frac{r}{s}$ une racine rationnelle écrite sous forme irréductible. Alors $r\mid a_0$ et $s\mid a_n$. En effet, en multipliant l'égalité $P\left(\frac{r}{s}\right)=0$ par s^n, on obtient

$$a_nr^n+a_{n-1}r^{n-1}s+\cdots+a_1rs^{n-1}+a_0s^n=0$$

L'entier r divise tous les termes sauf le dernier, donc il divise a_0s^n ; comme r est premier avec s, il divise a_0. Le même raisonnement, en isolant le premier terme, montre que s divise a_nr^n, donc a_n. En particulier, les racines rationnelles d'un polynôme *unitaire* à coefficients entiers sont des entiers qui divisent a_0 : il n'y a qu'un nombre fini de candidats à tester.

Outil 3 : le critère d'Eisenstein. Soit $P=a_nX^n+\cdots+a_0\in\mathbb{Z}[X]$ et p un nombre premier. Si p divise $a_0,\ldots,a_{n-1}$, ne divise pas a_n, et si p^2 ne divise pas a_0, alors P est irréductible sur $\mathbb{Q}$. C'est le critère énoncé à la question 3, qui fait l'objet du théorème 3.6 ; il a l'avantage de s'appliquer en tout degré.

Outil 4 : la translation. Pour $a\in\mathbb{Q}$, le polynôme $P(X)$ est irréductible sur $\mathbb{Q}$ si et seulement si $P(X+a)$ l'est. En effet, l'application $\tau : U(X)\mapsto U(X+a)$ est un morphisme d'anneaux de $\mathbb{Q}[X]$ dans lui-même, bijectif de réciproque $U(X)\mapsto U(X-a)$, et qui conserve le degré puisque le coefficient dominant est inchangé. Une factorisation non triviale $P=UV$ donne donc la factorisation non triviale $\tau(P)=\tau(U)\,\tau(V)$, et inversement. Ce changement de variable sert à rendre le critère d'Eisenstein applicable quand il ne l'est pas directement.

Le choix du critère. On procède dans l'ordre suivant : en degré 2 ou 3, on cherche les racines rationnelles, ce qui règle la question ; en degré plus grand, on essaie Eisenstein directement, puis après une translation ; si rien ne fonctionne, on cherche une factorisation explicite.

(a) Le polynôme X^2-2 est de degré 2 : d'après l'outil 1, il suffit de vérifier qu'il n'a pas de racine rationnelle. Il est unitaire, donc l'outil 2 limite les candidats aux diviseurs de 2, à savoir ±1 et ±2. Or $(\pm1)^2-2=-1$ et $(\pm2)^2-2=2$: aucun ne convient.

$$\boxed{X^2-2 \text{ est irréductible sur } \mathbb{Q}.}$$

On vient simplement de redémontrer l'irrationalité de $\sqrt{2}$.

(b) Le polynôme $P=X^3-3X-1$ est de degré 3 et unitaire, de terme constant -1 : ses seules racines rationnelles possibles sont ±1. On calcule $P(1)=1-3-1=-3$ et $P(-1)=-1+3-1=1$, tous deux non nuls.

$$\boxed{X^3-3X-1 \text{ est irréductible sur } \mathbb{Q}.}$$

(c) Le polynôme X^4+1 est de degré 4 : l'outil 1 ne s'applique plus. Il n'a aucune racine réelle, puisque $x^4+1\geqslant 1$, mais cela ne prouve rien, comme le montrera (f). Le critère d'Eisenstein ne

s'applique pas directement : le terme constant 1 n'est divisible par aucun nombre premier. On effectue donc la translation $X \mapsto X+1$:

$$(X+1)^4+1 = X^4+4X^3+6X^2+4X+2$$

Avec $p=2$: les coefficients 4, 6, 4 et 2 sont pairs, le coefficient dominant 1 ne l'est pas, et le terme constant 2 n'est pas divisible par 4. Le critère d'Eisenstein s'applique, et l'outil 4 ramène la conclusion au polynôme de départ.

$$\boxed{X^4+1 \text{ est irréductible sur } \mathbb{Q}.}$$

(d) Le polynôme X^5-4X+2 relève directement d'Eisenstein avec $p=2$: ses coefficients sont, dans l'ordre des degrés décroissants, 1, 0, 0, 0, -4 et 2. Le nombre 2 divise tous les coefficients sauf le dominant, et 4 ne divise pas le terme constant 2.

$$\boxed{X^5-4X+2 \text{ est irréductible sur } \mathbb{Q}.}$$

En degré 5, aucune recherche de racines ne suffirait : c'est ici qu'Eisenstein montre toute son économie. Il possède trois racines réelles, et la proposition 7.5 montrera que son groupe de Galois est $\mathfrak{S}_5$: il n'est pas résoluble par radicaux.

(e) Le polynôme $X^4+X^3+X^2+X+1$ est le polynôme cyclotomique $\Phi_5 = \dfrac{X^5-1}{X-1}$. Son terme constant vaut 1, donc Eisenstein ne s'applique pas directement ; après la translation $X \mapsto X+1$:

$$\Phi_5(X+1) = \frac{(X+1)^5-1}{X} = X^4+5X^3+10X^2+10X+5$$

Avec $p=5$: les coefficients 5, 10, 10 et 5 sont multiples de 5, le coefficient dominant ne l'est pas, et 25 ne divise pas 5.

$$\boxed{\Phi_5 = X^4+X^3+X^2+X+1 \text{ est irréductible sur } \mathbb{Q}.}$$

C'est le cas $p=5$ de la question 3, conformément au théorème 3.6.

(f) Le polynôme X^4+4 n'a pas de racine réelle, puisque $x^4+4 \geqslant 4$, et Eisenstein ne s'applique pas : le seul candidat est $p=2$, mais $4=2^2$ est divisible par p^2. Cherchons alors une factorisation, en complétant le carré :

$$X^4+4 = (X^4+4X^2+4)-4X^2 = (X^2+2)^2-(2X)^2$$

C'est une différence de deux carrés, qui se factorise :

$$\boxed{X^4+4 = (X^2-2X+2)(X^2+2X+2)}$$

Le polynôme est donc **réductible**, alors qu'il n'a aucune racine rationnelle. Chacun des deux facteurs est irréductible sur $\mathbb{Q}$, étant de degré 2 et de discriminant $4-8=-4<0$. C'est l'identité de Sophie Germain, $a^4+4b^4 = (a^2-2ab+2b^2)(a^2+2ab+2b^2)$, prise en $b=1$.

Remarque. La même idée, appliquée à X^4+1, donne $X^4+1 = (X^2+1)^2-2X^2$. Mais $2X^2$ n'est pas le carré d'un polynôme à coefficients rationnels, puisque $\sqrt{2} \notin \mathbb{Q}$: la factorisation n'existe que sur $\mathbb{R}$, en $(X^2-\sqrt{2}X+1)(X^2+\sqrt{2}X+1)$. Toute la différence entre (c) et (f) tient à ce que 4 est un carré dans $\mathbb{Q}$ et 2 n'en est pas un.

Récapitulatif.

polynôme	outil décisif	irréductible ?
X^2-2	degré 2 et racines rationnelles	oui
X^3-3X-1	degré 3 et racines rationnelles	oui
X^4+1	Eisenstein en 2 après $X \mapsto X+1$	oui
X^5-4X+2	Eisenstein en 2	oui
$X^4+X^3+X^2+X+1$	Eisenstein en 5 après $X \mapsto X+1$	oui
X^4+4	factorisation explicite	**non**

À retenir. Au-delà du degré 3, l'absence de racine ne prouve rien : X^4+1 et X^4+4 n'ont ni l'un ni l'autre de racine rationnelle, et pourtant le premier est irréductible et le second non.

2. L'irréductibilité sur $\mathbb{Q}$ a été établie à la question 1 (c). Reste la réductibilité modulo tout nombre premier p.

Le cas $p=2$. Dans $\mathbb{F}_2[X]$, on a $2=0$, donc $(X+1)^2 = X^2+2X+1 = X^2+1$, puis

$$(X+1)^4 = \left(X^2+1\right)^2 = X^4+2X^2+1 = X^4+1$$

$$\boxed{\text{Dans } \mathbb{F}_2[X],\ X^4+1=(X+1)^4.}$$

Le cas p impair : un lemme sur les carrés. Montrons que l'un au moins des trois éléments $\overline{-1}$, $\overline{2}$, $\overline{-2}$ est un carré dans $\mathbb{F}_p$. L'application $\varphi : \mathbb{F}_p^* \to \mathbb{F}_p^*$, $x \mapsto x^2$, est un morphisme de groupes, puisque $\mathbb{F}_p^*$ est commutatif. Son noyau est l'ensemble des racines de X^2-1, qui en a au plus deux dans le corps $\mathbb{F}_p$ (proposition 3.6) : c'est $\{\overline{1}\,;\overline{-1}\}$, et ces deux éléments sont distincts car p est impair. Le premier théorème d'isomorphisme (théorème 2.2) montre alors que l'image C, formée des carrés non nuls, a $\frac{p-1}{2}$ éléments : c'est un sous-groupe d'indice 2. Le groupe quotient $\mathbb{F}_p^*/C$ est donc d'ordre 2, et son élément non trivial est la classe commune de tous les non-carrés ; comme cet élément est son propre inverse, *le produit de deux non-carrés est un carré.* Si $\overline{-1}$ et $\overline{2}$ ne sont pas des carrés, leur produit $\overline{-2}$ en est donc un.

Les trois factorisations. Chacun des trois cas fournit une factorisation explicite en deux facteurs de degré 2, obtenue comme en 1 (f) par une différence de deux carrés.

Si $\overline{-1}=a^2$, alors $X^4+1 = X^4-a^2 = (X^2-a)(X^2+a)$.

Si $\overline{2}=b^2$, alors $X^4+1 = \left(X^2+1\right)^2 - 2X^2 = (X^2-bX+1)(X^2+bX+1)$.

Si $\overline{-2}=c^2$, alors $X^4+1 = \left(X^2-1\right)^2 + 2X^2 = (X^2-cX-1)(X^2+cX-1)$.

Par exemple, modulo 3 on a $\overline{-2}=\overline{1}^2$, d'où $X^4+1=(X^2-X-1)(X^2+X-1)$; modulo 5 on a $\overline{-1}=\overline{2}^2$, d'où $(X^2-2)(X^2+2)$; modulo 7 on a $\overline{2}=\overline{3}^2$, d'où $(X^2-3X+1)(X^2+3X+1)$.

$$\boxed{X^4+1 \text{ est irréductible sur } \mathbb{Q} \text{ et réductible sur tout } \mathbb{F}_p.}$$

Remarque. Sur $\mathbb{Q}$, aucune de ces trois factorisations n'existe, parce qu'aucun des nombres -1, 2, -2 n'est un carré rationnel ; la remarque de la question 1 (f) l'avait constaté pour 2. Modulo p, l'un des trois l'est toujours : c'est tout le contraste entre $\mathbb{Q}$ et les $\mathbb{F}_p$.

Remarque. Le chapitre 5 donnera une explication plus structurelle. Pour p impair, $p^2-1=(p-1)(p+1)$ est le produit de deux entiers pairs consécutifs, dont l'un est multiple de 4 : il est donc divisible par 8. Le groupe $\mathbb{F}_{p^2}^*$, cyclique d'ordre p^2-1, contient alors un élément ζ d'ordre 8, dont les puissances impaires sont les quatre racines de X^4+1. Toutes ces racines vivant dans une extension de degré 2 de $\mathbb{F}_p$, les facteurs irréductibles de X^4+1 sur $\mathbb{F}_p$ sont de degré au plus 2.

3. *Le critère d'Eisenstein* s'énonce ainsi : soit $P=a_nX^n+\cdots+a_0 \in \mathbb{Z}[X]$ et p un nombre premier ; si p divise $a_0,\ldots,a_{n-1}$, ne divise pas a_n, et si p^2 ne divise pas a_0, alors P est irréductible sur $\mathbb{Q}$.

Pour l'appliquer à Φ_p, on remarque d'abord que $(X-1)(X^{p-1}+\cdots+X+1)=X^p-1$, les termes intermédiaires s'annulant deux à deux, de sorte que $\Phi_p=\dfrac{X^p-1}{X-1}$. La formule du binôme donne alors :

$$\Phi_p(X+1)=\frac{(X+1)^p-1}{X}=\sum_{k=1}^{p}\binom{p}{k}X^{k-1}=X^{p-1}+\binom{p}{p-1}X^{p-2}+\cdots+\binom{p}{2}X+\binom{p}{1}$$

Pour $1\leqslant k\leqslant p-1$, le nombre premier p divise $\binom{p}{k}$. En effet, $k!\,(p-k)!\,\binom{p}{k}=p!$ est divisible par p, tandis que $k!\,(p-k)!$ est un produit d'entiers tous strictement inférieurs à p, donc premier avec p ; le lemme d'Euclide conclut. Ainsi tous les coefficients sauf le dominant sont divisibles par p, le coefficient dominant vaut 1, et le terme constant vaut $\binom{p}{1}=p$, qui n'est pas divisible par p^2. Le critère d'Eisenstein s'applique à $\Phi_p(X+1)$, et l'outil 4 de la question 1 le transporte à Φ_p.

$$\boxed{\Phi_p \text{ est irréductible sur } \mathbb{Q}.}$$

Pour $p=5$, on retrouve exactement le calcul de la question 1 (e).

4. On établit le critère suivant : *soit $P\in\mathbb{Z}[X]$ unitaire de degré $n\geqslant 1$ et p un nombre premier ; si la réduction $\overline{P}\in\mathbb{F}_p[X]$ est irréductible, alors P est irréductible sur $\mathbb{Q}$.*

Raisonnons par contraposée et supposons $P=UV$ dans $\mathbb{Q}[X]$, avec $\deg U,\deg V\geqslant 1$. Un polynôme unitaire est primitif, et le lemme de Gauss (théorème 3.6) montre qu'on peut alors écrire $P=U_0V_0$ avec $U_0,V_0\in\mathbb{Z}[X]$ de mêmes degrés que U et V. Leurs coefficients dominants sont deux entiers de produit 1, donc tous deux égaux à 1 ou tous deux à -1 ; quitte à remplacer U_0 et V_0 par leurs opposés, ils sont unitaires, et l'on renomme $U=U_0$ et $V=V_0$. En réduisant modulo p, on obtient $\overline{P}=\overline{U}\,\overline{V}$ dans $\mathbb{F}_p[X]$. Comme U et V sont unitaires, leur coefficient dominant 1 ne s'annule pas modulo p, de sorte que $\overline{U}$ et $\overline{V}$ gardent les degrés de U et de V, tous deux au moins égaux à 1. On obtient ainsi une factorisation non triviale de $\overline{P}$, qui n'est donc pas irréductible.

Piège. L'hypothèse « unitaire » — ou plus généralement « p ne divise pas le coefficient dominant » — est indispensable, car sans elle le degré peut chuter à la réduction. Ainsi $P=(2X+1)(X+1)=2X^2+3X+1$ est réductible sur $\mathbb{Q}$, alors que sa réduction modulo 2 vaut $X+1$, polynôme de degré 1 donc irréductible.

Piège. La réciproque est fausse : X^4+1 est irréductible sur $\mathbb{Q}$ mais réductible modulo tout nombre premier, d'après la question 2. Le critère ne fonctionne que dans un sens, et il peut ne jamais s'appliquer.

Application. Le polynôme X^3+X+1 est unitaire. Dans $\mathbb{F}_2$, il prend les valeurs $\overline{0}^3+\overline{0}+\overline{1}=\overline{1}$ et $\overline{1}^3+\overline{1}+\overline{1}=\overline{3}=\overline{1}$: il n'a pas de racine, et comme il est de degré 3, l'outil 1 de la question 1, valable sur tout corps, le rend irréductible sur $\mathbb{F}_2$. Le critère conclut.

$$\boxed{X^3+X+1 \text{ est irréductible sur } \mathbb{Q}.}$$

On pouvait aussi conclure directement par l'outil 2 : les seules racines rationnelles possibles sont ±1, et $P(1)=3$, $P(-1)=-1$. La réduction modulo p devient en revanche précieuse lorsque le degré dépasse 3 et qu'Eisenstein échoue : c'est ainsi que l'exercice 52 établira l'irréductibilité d'un polynôme de degré 5, en réduisant modulo 7.

Exercice 20 ⋆

Le polynôme $P=X^3-X^2+X+2$ est de degré 3, et ses seules racines rationnelles possibles sont ±1 et ±2 ; or $P(1)=3$, $P(-1)=-1$, $P(2)=8$ et $P(-2)=-12$. Il est donc irréductible sur $\mathbb{Q}$, et le quotient est un corps d'après la proposition 3.7 et le théorème 3.2.

Le produit. On réduit à l'aide de $\alpha^3=\alpha^2-\alpha-2$, d'où $\alpha^4=\alpha^3-\alpha^2-2\alpha=-3\alpha-2$:

$$(\alpha^2+\alpha+1)(\alpha^2-\alpha)=\alpha^4-\alpha \qquad \text{d'où} \qquad \boxed{(\alpha^2+\alpha+1)(\alpha^2-\alpha)=-4\alpha-2}$$

L'inverse. La division de P par $X-1$ donne $P=(X-1)(X^2+1)+3$, puisque $P(1)=3$. En évaluant en α, il vient $(\alpha-1)(\alpha^2+1)=-3$:

$$\boxed{(\alpha-1)^{-1}=-\frac{1}{3}\alpha^2-\frac{1}{3}}$$

Cette astuce n'est qu'un cas particulier de la relation de Bézout entre P et $X-1$, qui fournit l'inverse de tout élément non nul.

Exercice 21 ⋆⋆

1. Le polynôme X^2+X+1 n'a pas de racine dans $\mathbb{F}_2$, donc est irréductible. En notant α la classe de X, on a $\mathbb{F}_4 = \{0\,;1\,;\alpha\,;\alpha+1\}$ avec $\alpha^2 = \alpha+1$.

$+$	0	1	α	$\alpha+1$
0	0	1	α	$\alpha+1$
1	1	0	$\alpha+1$	α
α	α	$\alpha+1$	0	1
$\alpha+1$	$\alpha+1$	α	1	0

$\times$	1	α	$\alpha+1$
1	1	α	$\alpha+1$
α	α	$\alpha+1$	1
$\alpha+1$	$\alpha+1$	1	α

2. $\mathbb{F}_4^*$ est d'ordre 3, donc cyclique, et tout élément $\neq 1$ l'engendre :

$$\boxed{\alpha \text{ est un générateur, avec } \alpha^2 = \alpha+1 \text{ et } \alpha^3 = 1.}$$

3. X^3+X+1 est irréductible sur $\mathbb{F}_2$ (exercice 19), donc le quotient est un corps à $2^3 = 8$ éléments. La classe β de X vérifie $\beta^3 = \beta+1$, et $\mathbb{F}_8^*$ est d'ordre 7 premier :

$$\boxed{\left|\mathbb{F}_8\right| = 8, \text{ et } \beta \text{ est d'ordre } 7.}$$

4. Le polynôme X^2+1 n'a pas de racine dans $\mathbb{F}_3$, puisque $0^2+1=1$, $1^2+1=2$ et $2^2+1=2$:

$$\boxed{\mathbb{F}_9 = \mathbb{F}_3[X]/(X^2+1) = \left\{a+b\mathrm{i} \;\middle|\; a,b \in \mathbb{F}_3\right\}}$$

Exercice 22 ⋆⋆

1. Les quatre unitaires de degré 2 sont X^2, X^2+1, X^2+X, X^2+X+1. Les trois premiers ont une racine dans $\mathbb{F}_2$:

$$\boxed{\text{Un seul irréductible : } X^2+X+1.}$$

2. Parmi les huit unitaires de degré 3, ceux sans racine sont ceux dont le terme constant vaut 1 et qui ont un nombre impair de coefficients non nuls :

$$\boxed{X^3+X+1 \quad \text{et} \quad X^3+X^2+1}$$

3. Fixons un nombre premier p et un entier $n \geqslant 1$, et posons $F = X^{p^n} - X$. Tout repose sur la factorisation suivante : *F est le produit des polynômes unitaires irréductibles de $\mathbb{F}_p[X]$ dont le degré divise n, chacun n'apparaissant qu'une seule fois.* On l'établit en deux étapes, puis on compare les degrés.

Première étape : F n'a pas de facteur carré. Supposons $F = Q^2R$ avec Q non constant. Le polynôme dérivé, défini formellement par $\left(X^m\right)' = mX^{m-1}$ et prolongé par linéarité, vérifie la règle de dérivation d'un produit, ce que l'on contrôle sur les monômes. On en tire :

$$F' = 2QQ'R + Q^2R' = Q\left(2Q'R + QR'\right)$$

donc Q divise F'. Or $F' = p^n X^{p^n-1} - 1 = -1$, puisque l'entier p^n est nul dans $\mathbb{F}_p$. Un polynôme non constant ne pouvant pas diviser -1, c'est absurde.

Deuxième étape : un polynôme unitaire irréductible P de degré d divise F si et seulement si d divise n. On travaille dans $K = \mathbb{F}_p[X]/(P)$, qui est un corps puisque P est irréductible (théorème 3.2), exactement comme $\mathbb{F}_4$ à l'exercice 21. On note α la classe de X : pour tout polynôme Q, la classe de Q est $Q(\alpha)$, de sorte que $Q(\alpha) = 0$ si et seulement si P divise Q. Trois faits vont servir.

Premier fait : K a p^d éléments. Chaque classe contient en effet un unique reste de la division euclidienne par P, c'est-à-dire un polynôme de degré au plus $d-1$, dont les d coefficients se choisissent de p façons chacun.

Deuxième fait : tout $x \in K$ vérifie $x^{p^d} = x$. Si $x \neq 0$, le théorème de Lagrange, appliqué dans le groupe K^* d'ordre $p^d - 1$, donne $x^{p^d-1} = 1$, puis on multiplie par x ; si $x = 0$, c'est évident.

Troisième fait : l'application $x \mapsto x^p$ est un morphisme d'anneaux de K dans lui-même. Elle respecte évidemment le produit, et la formule du binôme donne $(x+y)^p = x^p + y^p$, puisque p divise $\binom{p}{k}$ pour $1 \leqslant k \leqslant p-1$ (exercice 19, question 3) et que $p \cdot 1 = 0$ dans K. En la composant n fois avec elle-même, on obtient que $x \mapsto x^{p^n}$ est aussi un morphisme d'anneaux.

Supposons d'abord que d divise n, et écrivons $n = qd$. En appliquant q fois le deuxième fait, on obtient $\alpha^{p^n} = \alpha$, c'est-à-dire $F(\alpha) = 0$: donc P divise F.

Réciproquement, supposons que P divise F, c'est-à-dire que $\alpha^{p^n} = \alpha$. L'ensemble des $x \in K$ tels que $x^{p^n} = x$ est stable par somme et par produit, d'après le troisième fait ; il contient les éléments de $\mathbb{F}_p$, qui vérifient $x^p = x$ d'après le petit théorème de Fermat, ainsi que α. Il contient donc toutes les expressions polynomiales en α, c'est-à-dire K tout entier. Écrivons alors $n = qd + r$ avec $0 \leqslant r < d$. Pour tout $x \in K$, le deuxième fait donne $x^{p^{qd}} = x$, d'où :

$$x = x^{p^n} = \left(x^{p^{qd}}\right)^{p^r} = x^{p^r}$$

Si l'on avait $r \geqslant 1$, le polynôme non nul $X^{p^r} - X$, de degré p^r, aurait les p^d éléments de K pour racines, avec $p^d > p^r$: c'est impossible dans un corps, d'après la proposition 3.6. Donc $r = 0$, et d divise n.

Conclusion. Le polynôme F est unitaire, et se décompose de façon unique en produit de polynômes unitaires irréductibles de $\mathbb{F}_p[X]$. D'après la première étape, chaque facteur n'y apparaît qu'une fois ; d'après la deuxième, ces facteurs sont exactement les unitaires irréductibles dont le degré divise n. En notant $\mathcal{I}_d$ l'ensemble des N_d unitaires irréductibles de degré d :

$$X^{p^n} - X = \prod_{d|n} \prod_{P \in \mathcal{I}_d} P$$

Le membre de droite est un produit de N_d polynômes de degré d pour chaque diviseur d de n : son degré vaut $\sum_{d|n} d\,N_d$, celui de gauche vaut p^n.

$$\boxed{\sum_{d|n} d\,N_d = p^n}$$

Par exemple, pour $p = 2$ et $n = 3$, on obtient $X^8 - X = X\,(X+1)(X^3+X+1)(X^3+X^2+1)$, de degré $1+1+3+3 = 8$: on y retrouve les deux irréductibles de degré 1 et les deux irréductibles de degré 3 de la question 2.

Remarque. Cette factorisation sera au cœur de l'étude des corps finis au chapitre 5. On voit ici qu'elle se démontre dès le chapitre 3, avec le théorème de Lagrange, la construction de $\mathbb{F}_p[X]/(P)$ et la majoration du nombre de racines d'un polynôme.

4. On applique la question 3 avec $p = 2$, successivement pour $n = 1$, 2, 3 et 4. Les diviseurs de 2 sont 1 et 2, ceux de 3 sont 1 et 3, ceux de 4 sont 1, 2 et 4 :

$$N_1 = 2 \qquad N_1 + 2N_2 = 4 \qquad N_1 + 3N_3 = 8 \qquad N_1 + 2N_2 + 4N_4 = 16$$

On en tire successivement $N_2 = 1$, $N_3 = 2$, puis $N_4 = \dfrac{16-2-2}{4} = 3$.

$$\boxed{N_1 = 2, \quad N_2 = 1, \quad N_3 = 2, \quad N_4 = 3}$$

Les valeurs de N_2 et N_3 confirment les questions 1 et 2. Les trois irréductibles de degré 4 sont X^4+X+1, X^4+X^3+1 et $X^4+X^3+X^2+X+1$.

Chapitre 4 - Extensions de corps

Questions de cours

Q1. Voir le théorème 4.1 : si (e_i) est une base de M/K et (f_j) une base de L/M, la famille $(e_i f_j)$ est une base de L/K.

Q2. Voir le théorème 4.2 : le noyau de $P \mapsto P(\alpha)$ est un idéal premier non nul de $K[X]$, donc engendré par un irréductible μ_α ; la division euclidienne par μ_α fournit la base.

Q3. Voir la proposition 4.3 : si $[L : K] = n$, les $n+1$ éléments $1, \alpha, \ldots, \alpha^n$ sont liés. Si α et β sont algébriques, $K(\alpha\,;\beta)$ est de degré fini, et contient $\alpha+\beta$, $\alpha\beta$ et α^{-1}.

Q4. Voir la proposition 4.4 et le théorème 4.4 : on prolonge l'isomorphisme racine par racine, en envoyant une racine d'un facteur irréductible sur une racine du facteur correspondant.

Q5. Voir le théorème 4.5 et la proposition 4.6 : $\sqrt[3]{2}$ est de degré 3, et $\cos\dfrac{\pi}{9}$ est racine de $8X^3-6X-1$, irréductible, donc de degré 3 ; or un nombre constructible a pour degré une puissance de 2.

Q6. Si $K \subseteq M \subseteq L$ avec $[L : K] = p$ premier, alors $[M : K]$ divise p : il vaut 1 ou p, et $M = K$ ou $M = L$.

Exercice 23 ⋆

1. On identifie le polynôme minimal puis on justifie son irréductibilité :

α	μ_α	irréductibilité
$\sqrt[3]{5}$	X^3-5	Eisenstein en 5
$\mathrm{i}\sqrt{3}$	X^2+3	pas de racine réelle
ζ_5	$X^4+X^3+X^2+X+1$	c'est Φ_5 (Eisenstein après $X \mapsto X+1$)
$1+\sqrt{2}$	X^2-2X-1	discriminant 8, non carré dans $\mathbb{Q}$

2. Sur $\mathbb{Q}(\sqrt{3})$, le polynôme X^2-2 reste sans racine, car $\sqrt{2} \notin \mathbb{Q}(\sqrt{3})$: l'égalité $\sqrt{2} = a + b\sqrt{3}$ donnerait $2 = a^2+3b^2+2ab\sqrt{3}$, donc $ab=0$, puis $2=a^2$ ou $2=3b^2$, ce qui est impossible dans $\mathbb{Q}$:

$$\boxed{\mu_{\sqrt{2}/\mathbb{Q}(\sqrt{3})} = X^2-2 \qquad \mu_{\sqrt{2}/\mathbb{Q}(\sqrt{2})} = X-\sqrt{2}}$$

Exercice 24 ⋆⋆⋆

Soit E une extension de F de degré 2 et $\beta \in E \setminus F$, de polynôme minimal X^2+bX+c. Comme la caractéristique est différente de 2, on peut compléter le carré : $\delta = 2\beta+b$ vérifie $\delta^2 = b^2-4c =: d \in F$, et $E = F(\delta)$. Le nombre d n'est pas un carré dans F, sinon $\delta \in F$.

1. Soit $x = u+v\delta \in E$, avec $u, v \in F$. Alors $x^2 = u^2+dv^2+2uv\delta$ appartient à F si et seulement si $uv=0$, et vaut alors u^2 ou dv^2. Ainsi :

$$\boxed{S(E) = F^{*2} \cup d\,F^{*2}}$$

C'est la réunion de deux classes de F^* modulo le sous-groupe F^{*2} ; comme $d^2 \in F^{*2}$, c'est le sous-groupe engendré par F^{*2} et d.

2. Un F-isomorphisme $E \to E'$ envoie un carré sur un carré et fixe F^*, donc $S(E) \subseteq S(E')$; par symétrie, $S(E) = S(E')$. Réciproquement, si $S(E) = S(E')$ avec $E = F(\delta)$, $\delta^2 = d$, alors $d \in S(E')$: il existe $\delta' \in E'$ tel que $\delta'^2 = d$. Comme d n'est pas un carré dans F, on a $F(\delta') = E'$ par égalité des degrés, et les deux corps sont isomorphes à $F[X]/(X^2-d)$.

$$\boxed{E \simeq_F E' \iff S(E) = S(E')}$$

3. Pour chaque nombre premier q, posons $E_q = \mathbb{Q}(\sqrt{q})$, de sorte que $S(E_q) = \mathbb{Q}^{*2} \cup q\,\mathbb{Q}^{*2}$. Si $q \neq q'$, le rationnel q' n'appartient pas à $S(E_q)$, car ni q' ni q'/q n'est un carré dans $\mathbb{Q}$.

$$\boxed{\text{Les corps } \mathbb{Q}(\sqrt{q}),\ q \text{ premier, sont deux à deux non isomorphes.}}$$

Exercice 25 ⋆⋆⋆

Soit g un facteur irréductible de f de degré d minimal, et $L = K[X]/(g)$ un corps de rupture de g, de degré d sur K. Le polynôme f y possède une racine, donc il y est scindé par hypothèse. Chaque facteur irréductible h de f possède alors une racine $\beta \in L$, et $K(\beta) \subseteq L$: par multiplicativité des degrés, $\deg h = [K(\beta) : K]$ divise $[L : K] = d$. Par minimalité de d, on obtient $\deg h = d$.

Tous les facteurs irréductibles de f ont donc le même degré d, et d divise $\deg f = p$. Ainsi $d = 1$, auquel cas f a une racine dans K, ou $d = p$, auquel cas f est irréductible.

$$\boxed{f \text{ est irréductible sur } K \text{ ou possède une racine dans } K.}$$

Sans l'hypothèse de primalité, la conclusion tombe : sur $\mathbb{Q}$, le polynôme $(X^2-2)^2$, de degré 4, vérifie l'hypothèse, puisque toute extension contenant l'une des racines $\pm\sqrt{2}$ contient l'autre ; il n'est pourtant ni irréductible, ni pourvu d'une racine rationnelle.

Exercice 26 ⋆⋆

Le polynôme $X^5 - 2$ est irréductible sur $\mathbb{Q}$ par le critère d'Eisenstein en 2. En notant $\alpha = \sqrt[5]{2}$ et $\zeta = \mathrm{e}^{2\mathrm{i}\pi/5}$, ses racines sont les $\alpha\zeta^k$ pour $0 \leqslant k \leqslant 4$. Le corps $L = \mathbb{Q}(\alpha\,;\zeta)$ les contient toutes, et il est engendré par elles puisque $\zeta = \dfrac{\alpha\zeta}{\alpha}$:

$$\boxed{L = \mathbb{Q}(\sqrt[5]{2}\,;\zeta)}$$

On a $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 5$ et $[\mathbb{Q}(\zeta) : \mathbb{Q}] = 4$, puisque ζ est racine de Φ_5, irréductible. Ces deux degrés divisent $[L : \mathbb{Q}]$ et sont premiers entre eux, donc 20 divise $[L : \mathbb{Q}]$. Par ailleurs ζ est racine de Φ_5 sur $\mathbb{Q}(\alpha)$, donc $[L : \mathbb{Q}(\alpha)] \leqslant 4$ et $[L : \mathbb{Q}] \leqslant 20$.

$$\boxed{[L : \mathbb{Q}] = 20}$$

Exercice 27 ⋆⋆

L'heptagone. Posons $\zeta = \mathrm{e}^{2\mathrm{i}\pi/7}$ et $c = \zeta + \zeta^{-1} = 2\cos\dfrac{2\pi}{7}$. En divisant la relation $1+\zeta+\cdots+\zeta^6 = 0$ par ζ^3, et en utilisant $\zeta^2 + \zeta^{-2} = c^2 - 2$ et $\zeta^3 + \zeta^{-3} = c^3 - 3c$, on obtient :

$$c^3 + c^2 - 2c - 1 = 0$$

Ce polynôme de degré 3 n'a pas de racine rationnelle, ses seules candidates ± 1 donnant -1 et 1 : il est irréductible, et $\cos\dfrac{2\pi}{7}$ est de degré 3 sur $\mathbb{Q}$. Or construire l'heptagone régulier revient à construire $\cos\dfrac{2\pi}{7}$; le critère de Wantzel l'interdit, 3 n'étant pas une puissance de 2.

L'ennéagone. La formule $\cos(3\theta) = 4\cos^3\theta - 3\cos\theta$, appliquée à $\theta = \dfrac{2\pi}{9}$, montre que $x = \cos\dfrac{2\pi}{9}$ est racine de $8X^3 - 6X + 1$. Aucun des candidats ± 1, $\pm\frac{1}{2}$, $\pm\frac{1}{4}$, $\pm\frac{1}{8}$ n'est racine : ce polynôme est irréductible, et la même conclusion s'impose.

$$\boxed{\text{Ni l'heptagone ni l'ennéagone réguliers ne sont constructibles.}}$$

La quadrature. Le critère de Wantzel ne porte que sur des nombres *algébriques* : il exige que le nombre à construire soit racine d'un polynôme, pour en mesurer le degré. Or la quadrature du cercle demande de construire $\sqrt{\pi}$, et l'on doit admettre un résultat d'une autre nature, la transcendance de π démontrée par Lindemann en 1882.

Chapitre 5 - Séparabilité, normalité, corps finis

Questions de cours

Q1. Voir les propositions 5.1 et 5.2 : une racine multiple de P est racine de $\text{pgcd}(P\,;P')$. Si P est irréductible, ce pgcd vaut 1 ou P, et il vaut P si et seulement si $P'=0$, ce qui est impossible en caractéristique nulle pour P non constant.

Q2. Le polynôme X^3-2 est irréductible, possède la racine réelle $\sqrt[3]{2}$, mais ses deux autres racines ne sont pas réelles. La clôture normale est $\mathbb{Q}(\sqrt[3]{2}\,;\mathrm{j})$, de degré $3\times 2=6$.

Q3. Un corps fini contient un sous-corps premier $\mathbb{F}_p$, et c'en est un espace vectoriel de dimension finie n : il a p^n éléments. Pour le théorème 5.3, voir le cours.

Q4. Voir la proposition 5.5 : si $\mathbb{F}_{p^d}\subseteq\mathbb{F}_{p^n}$, la multiplicativité des degrés donne $d\mid n$; réciproquement, $X^{p^d}-X$ divise alors $X^{p^n}-X$.

Q5. Voir le théorème 5.4 : pour chaque d divisant $q-1$, les éléments d'ordre d sont racines de X^d-1, qui en a au plus d ; un décompte à l'aide de l'indicatrice d'Euler montre qu'il existe un élément d'ordre $q-1$.

Q6. Voir le théorème 5.5 : toute extension finie séparable est monogène. L'élément $\sqrt{2}+\sqrt{3}$ convient pour $\mathbb{Q}(\sqrt{2}\,;\sqrt{3})$, de polynôme minimal X^4-10X^2+1.

Exercice 28 ⋆⋆

1. Soit $[L:K]=2$ et P irréductible sur K ayant une racine $\alpha\in L$. Alors $\deg P\mid 2$; si $\deg P=1$ c'est fini, si $\deg P=2$ alors $L=K(\alpha)$ et $P=(X-\alpha)(X-\beta)$ avec $\beta=-\alpha-\dfrac{a_1}{a_2}\in L$.

$$\boxed{\text{Toute extension de degré 2 est normale.}}$$

2. Avec $K=\mathbb{Q}$, $M=\mathbb{Q}(\sqrt{2})$, $L=\mathbb{Q}(\sqrt[4]{2})$: les deux étages sont de degré 2, donc normaux. Mais X^4-2 est irréductible sur $\mathbb{Q}$, possède la racine $\sqrt[4]{2}\in L$, et ses racines $\pm\mathrm{i}\sqrt[4]{2}$ ne sont pas réelles.

$$\boxed{L/\mathbb{Q}\text{ n'est pas normale : la normalité n'est pas transitive.}}$$

Exercice 29 ⋆

1. $64=2^6$ et les diviseurs de 6 sont 1, 2, 3, 6 :

$$\boxed{\mathbb{F}_2\subset\mathbb{F}_4\subset\mathbb{F}_{64}\quad\text{et}\quad\mathbb{F}_2\subset\mathbb{F}_8\subset\mathbb{F}_{64},\ \text{avec}\ \mathbb{F}_4\not\subseteq\mathbb{F}_8.}$$

Le treillis reproduit celui des diviseurs de 6.

2. Les diviseurs de 12 sont au nombre de six :

$$\boxed{\mathbb{F}_3,\ \mathbb{F}_{3^2},\ \mathbb{F}_{3^3},\ \mathbb{F}_{3^4},\ \mathbb{F}_{3^6},\ \mathbb{F}_{3^{12}}}$$

Exercice 30 ⋆⋆

1. On teste les puissances successives :

$$\boxed{\text{Générateurs de }\mathbb{F}_7^*:\{3\,;5\}\qquad\text{de }\mathbb{F}_{11}^*:\{2\,;6\,;7\,;8\}}$$

On en compte $\varphi(6)=2$ et $\varphi(10)=4$, conformément à la question suivante.

2. Un groupe cyclique d'ordre m possède $\varphi(m)$ générateurs :

$$\boxed{\mathbb{F}_q^*\text{ possède }\varphi(q-1)\text{ générateurs.}}$$

3. Dans le produit $(p-1)!$, chaque élément de $\mathbb{F}_p^*$ apparaît une fois. On apparie x avec x^{-1} : les paires se simplifient, et il ne reste que les éléments égaux à leur inverse, c'est-à-dire les racines de X^2-1, à savoir 1 et -1.

$$\boxed{(p-1)! \equiv 1 \times (-1) = -1\ [p]}$$

4. $6! = 720 = 102 \times 7 + 6$, et $6 \equiv -1\ [7]$:

$$\boxed{6! \equiv -1\ [7] \quad \checkmark}$$

Exercice 31 ⋆⋆⋆

Le cas de -1. Le nombre -1 est un carré dans $\mathbb{F}_p$ si et seulement si $\mathbb{F}_p^*$ contient un élément d'ordre 4. Ce groupe étant cyclique d'ordre $p-1$ (théorème 5.4), cela équivaut à $4 \mid p-1$.

$$\boxed{-1 \text{ est un carré dans } \mathbb{F}_p \iff p \equiv 1\ [4]}$$

Le cas de 2. Comme p est impair, 8 divise p^2-1, et le groupe cyclique $\mathbb{F}_{p^2}^*$ contient un élément x d'ordre 8 ; on a $x^4 = -1$, seul élément d'ordre 2 d'un corps. Posons $y = x + x^{-1}$. Alors :

$$y^2 = x^2 + 2 + x^{-2} = 2 + x^{-2}(x^4+1) = 2$$

Les racines carrées de 2 dans $\mathbb{F}_{p^2}$ sont donc $\pm y$, et 2 est un carré dans $\mathbb{F}_p$ si et seulement si $y \in \mathbb{F}_p$, c'est-à-dire $y^p = y$. Le Frobenius étant un morphisme, $y^p = x^p + x^{-p}$, qui ne dépend que de p modulo 8.

Si $p \equiv \pm 1\ [8]$, alors $x^p = x^{\pm 1}$ et $y^p = y$. Si $p \equiv \pm 3\ [8]$, alors $y^p = x^3 + x^{-3} = x^3 + x^5$; comme $x^4 = -1$, on a $x^5 = -x$ et $x^3 = -x^{-1}$, d'où $y^p = -y \neq y$, puisque $y \neq 0$.

$$\boxed{2 \text{ est un carré dans } \mathbb{F}_p \iff p \equiv \pm 1\ [8]}$$

On retrouve ainsi, par la seule théorie des corps finis, les deux « lois complémentaires » de la réciprocité quadratique.

Exercice 32 ⋆⋆

Comme p ne divise pas n, le polynôme $X^n - 1$ est premier avec sa dérivée nX^{n-1} : il est séparable, et ses racines forment dans son corps de décomposition L un sous-groupe μ_n de L^* d'ordre n, cyclique d'après le théorème 5.4. Le corps L est fini, égal à $\mathbb{F}_p(\mu_n)$.

Un corps $\mathbb{F}_{p^k}$ contient n racines n-ièmes de l'unité si et seulement si son groupe multiplicatif, cyclique d'ordre $p^k - 1$, possède un sous-groupe d'ordre n, c'est-à-dire si $n \mid p^k - 1$, soit $p^k \equiv 1\ [n]$. Cela équivaut à dire que l'ordre d de $\overline{p}$ dans $(\mathbb{Z}/n\mathbb{Z})^*$ divise k. Le plus petit corps convenable est donc $\mathbb{F}_{p^d}$.

$$\boxed{\text{Le corps de décomposition de } X^n - 1 \text{ sur } \mathbb{F}_p \text{ est } \mathbb{F}_{p^d},\ d = \text{ordre de } \overline{p} \text{ dans } (\mathbb{Z}/n\mathbb{Z})^*.}$$

Pour $p = 3$ et $n = 7$, les puissances de 3 modulo 7 sont 3, 2, 6, 4, 5, 1 : l'ordre vaut 6. Une racine primitive septième ζ engendre μ_7, donc $\mathbb{F}_3(\zeta) = \mathbb{F}_3(\mu_7)$.

$$\boxed{\mathbb{F}_3(\zeta) = \mathbb{F}_{3^6} = \mathbb{F}_{729}}$$

Enfin, d'après le rêve du débutant, $X^{p^m} - 1 = (X-1)^{p^m}$: ce polynôme est déjà scindé sur $\mathbb{F}_p$, avec l'unique racine 1 de multiplicité p^m.

$$\boxed{\text{Le corps de décomposition de } X^{p^m} - 1 \text{ sur } \mathbb{F}_p \text{ est } \mathbb{F}_p \text{ lui-même.}}$$

Exercice 33 ⋆⋆⋆

1. Posons $\theta = \sqrt[3]{2}+\mathrm{j}$. L'extension $\mathbb{Q}(\sqrt[3]{2}\,;\mathrm{j})/\mathbb{Q}$ est de degré 6, séparable, donc monogène ; on vérifie que θ engendre, son degré devant diviser 6 sans valoir 1, 2 ni 3 — car $\mathbb{Q}(\theta)$ n'est contenu ni dans $\mathbb{R}$, ni dans $\mathbb{Q}(\mathrm{j})$.

$$\boxed{\theta = \sqrt[3]{2}+\mathrm{j} \text{ est un élément primitif, de degré 6.}}$$

2. Posons $K = \mathbb{F}_p(T^p\,;S^p)$ et $L = \mathbb{F}_p(T\,;S)$. On a $[L:K] = p^2$, mais tout $\alpha \in L$ vérifie $\alpha^p \in K$, donc $[K(\alpha):K] \leqslant p$: aucun élément n'engendre. Les corps $K(T+\lambda S)$, pour $\lambda \in \mathbb{F}_p(T^p;S^p)$, sont deux à deux distincts et en nombre infini.

$$\boxed{L/K \text{ est finie sans élément primitif, et possède une infinité de corps intermédiaires.}}$$

3. L'hypothèse manquante se lit sur le polynôme minimal :

$$\boxed{\text{La séparabilité : ici } \mu_\alpha \text{ divise } X^p - \alpha^p = (X-\alpha)^p.}$$

Chapitre 6 - La correspondance de Galois

Questions de cours

Q1. Voir la proposition 6.2 : un K-automorphisme est déterminé par les images des générateurs, qui sont des racines de leurs polynômes minimaux, en nombre fini.

Q2. Voir les théorèmes 6.1 et 6.2 : une relation de dépendance linéaire minimale entre caractères distincts conduit à une relation plus courte ; appliqué à G, cela donne $[L:L^G] \leqslant |G|$, puis l'égalité.

Q3. Voir les théorèmes 6.3 et 6.4.

Q4. Voir les exemples complets du paragraphe 6.5 : $\mathrm{Gal}(\mathbb{Q}(\sqrt[3]{2}\,;\mathrm{j})/\mathbb{Q}) \simeq \mathfrak{S}_3$, avec six sous-corps, et $\mathrm{Gal}(\mathbb{Q}(\sqrt[4]{2}\,;\mathrm{i})/\mathbb{Q}) \simeq D_4$, avec dix sous-corps.

Exercice 34 ⋆⋆

Posons $F = \mathbb{Q}(\sqrt{2}\,;\sqrt{3})$. Si l'on avait $\sqrt{3} = a+b\sqrt{2}$ avec $a,b \in \mathbb{Q}$, alors $3 = a^2+2b^2+2ab\sqrt{2}$ imposerait $ab = 0$, puis $3 = a^2$ ou $3 = 2b^2$, ce qui est impossible. Ainsi $[F:\mathbb{Q}] = 4$, et $F/\mathbb{Q}$ est galoisienne de groupe $(\mathbb{Z}/2\mathbb{Z})^2$, formé des quatre changements de signes de $\sqrt{2}$ et $\sqrt{3}$. Ce groupe a trois sous-groupes d'ordre 2, donc F a exactement trois sous-corps quadratiques : $\mathbb{Q}(\sqrt{2})$, $\mathbb{Q}(\sqrt{3})$ et $\mathbb{Q}(\sqrt{6})$.

Si $\sqrt{5}$ appartenait à F, le corps $\mathbb{Q}(\sqrt{5})$ serait l'un d'eux. Mais $\mathbb{Q}(\sqrt{5}) = \mathbb{Q}(\sqrt{m})$ entraîne, par le même calcul que ci-dessus, que $5m$ est un carré dans $\mathbb{Q}$, ce qui est faux pour $m = 2$, 3 et 6. Donc $L = \mathbb{Q}(\sqrt{2}\,;\sqrt{3}\,;\sqrt{5})$ est de degré 8 : c'est le corps de décomposition de $(X^2-2)(X^2-3)(X^2-5)$, galoisien, et ses huit automorphismes changent indépendamment les signes de $\sqrt{2}$, $\sqrt{3}$ et $\sqrt{5}$.

Les images de $\gamma = \sqrt{2}+\sqrt{3}+\sqrt{5}$ sont les huit nombres $\pm\sqrt{2}\pm\sqrt{3}\pm\sqrt{5}$. Ils sont deux à deux distincts : une égalité entre deux d'entre eux fournirait une relation $a\sqrt{2}+b\sqrt{3}+c\sqrt{5} = 0$ à coefficients dans $\{0\,;\pm 2\}$ non tous nuls, impossible puisque 1, $\sqrt{2}$, $\sqrt{3}$ et $\sqrt{5}$ font partie d'une base de L sur $\mathbb{Q}$. L'élément γ a donc huit conjugués, il est de degré 8, et son polynôme minimal est le produit des $X-(\pm\sqrt{2}\pm\sqrt{3}\pm\sqrt{5})$:

$$\boxed{\mu_\gamma = X^8 - 40X^6 + 352X^4 - 960X^2 + 576}$$

Au passage, γ est un élément primitif de L.

Exercice 35 ⋆⋆

Sur un corps fini $\mathbb{F}_q$, le corps de décomposition d'un polynôme séparable est un $\mathbb{F}_{q^m}$, et son groupe de Galois est cyclique d'ordre m, engendré par $x \mapsto x^q$; il suffit donc de trouver m. Posons $P = X^4 + X^3 + 1$.

Sur $\mathbb{F}_2$. On a $P(0) = P(1) = 1$: pas de racine. Le seul polynôme irréductible de degré 2 sur $\mathbb{F}_2$ est $X^2 + X + 1$, et son carré $X^4 + X^2 + 1$ diffère de P. Donc P est irréductible ; son corps de rupture $\mathbb{F}_{16}$ contient toutes ses racines, puisque c'est un corps de décomposition de $X^{16} - X$.

$$\boxed{\mathrm{Gal}_{\mathbb{F}_2}(P) \simeq \mathbb{Z}/4\mathbb{Z}}$$

Sur $\mathbb{F}_3$. On a $P(1) = 3 = 0$, et la division donne $P = (X-1)(X^3 - X^2 - X - 1)$. Ce facteur cubique prend les valeurs 2, 1 et 1 en 0, 1 et 2 : il est irréductible, et son corps de décomposition est $\mathbb{F}_{27}$.

$$\boxed{\mathrm{Gal}_{\mathbb{F}_3}(P) \simeq \mathbb{Z}/3\mathbb{Z}}$$

Sur $\mathbb{F}_4$. Les racines de P engendrent $\mathbb{F}_{16}$ sur $\mathbb{F}_2$, donc n'appartiennent pas à $\mathbb{F}_4$, et $\mathbb{F}_4(\text{racines}) = \mathbb{F}_{16}$, de degré 2 sur $\mathbb{F}_4$. Le polynôme P se factorise sur $\mathbb{F}_4$ en deux facteurs irréductibles de degré 2.

$$\boxed{\mathrm{Gal}_{\mathbb{F}_4}(P) \simeq \mathbb{Z}/2\mathbb{Z}}$$

Le même polynôme a donc trois groupes de Galois différents selon le corps de base.

Exercice 36 ⋆⋆⋆

Le corps de décomposition. Le polynôme $X^6 + 3$ est irréductible par le critère d'Eisenstein en 3. Soit $\beta = \sqrt[6]{3}\,\mathrm{e}^{\mathrm{i}\pi/6}$, qui vérifie $\beta^3 = \sqrt{3}\,\mathrm{e}^{\mathrm{i}\pi/2} = \mathrm{i}\sqrt{3}$, donc $\beta^6 = -3$. Le corps $\mathbb{Q}(\beta)$ contient $\mathrm{i}\sqrt{3} = \beta^3$, donc $\omega = \mathrm{e}^{\mathrm{i}\pi/3} = \dfrac{1+\mathrm{i}\sqrt{3}}{2}$, racine primitive sixième de l'unité. Les six racines $\beta\omega^k$ sont donc dans $\mathbb{Q}(\beta)$, qui est le corps de décomposition L.

$$[L : \mathbb{Q}] = 6 \qquad \text{donc} \qquad |G| = 6$$

Les éléments. Pour chaque $k \in \{0\,;\ldots;5\}$, il existe un unique $\sigma_k \in G$ tel que $\sigma_k(\beta) = \beta\omega^k$. Comme $\omega = \dfrac{1+\beta^3}{2}$, on a $\sigma_k(\omega) = \dfrac{1+(-1)^k\beta^3}{2}$, qui vaut ω si k est pair et ω^{-1} si k est impair. Par conséquent $\sigma_k^2(\beta) = \beta\,\omega^k\,\sigma_k(\omega)^k$ vaut $\beta\omega^{2k}$ pour k pair et β pour k impair : les σ_k d'indice impair sont d'ordre 2, et σ_2, σ_4 sont d'ordre 3. Aucun élément n'est d'ordre 6. Or un groupe abélien d'ordre 6 est cyclique, le produit d'un élément d'ordre 2 et d'un élément d'ordre 3 qui commutent étant d'ordre 6 : le groupe n'est donc pas abélien, et l'exercice 4 conclut.

$$\boxed{\mathrm{Gal}(X^6+3) \simeq \mathfrak{S}_3}$$

Réductibilité modulo p. Pour $p = 2$, on a $X^6 + 1 = (X^3+1)^2$; pour $p = 3$, le polynôme vaut X^6. Soit $p \geqslant 5$.

- Si $p \equiv 2\ [3]$, l'application $x \mapsto x^3$ est injective sur $\mathbb{F}_p^*$, puisque 3 ne divise pas $p-1$; elle est donc bijective, et il existe c tel que $c^3 = -3$. Alors $X^6 + 3 = X^6 - c^3 = (X^2 - c)(X^4 + cX^2 + c^2)$.
- Si $p \equiv 1\ [3]$, le groupe cyclique $\mathbb{F}_p^*$ contient un élément j d'ordre 3, qui vérifie $j^2 + j + 1 = 0$, d'où $(2j+1)^2 = -3$. Avec $s = 2j+1$, il vient $X^6 + 3 = X^6 - s^2 = (X^3 - s)(X^3 + s)$.

$$\boxed{X^6 + 3 \text{ est réductible sur } \mathbb{F}_p \text{ pour tout nombre premier } p.}$$

C'est le même phénomène que pour $X^4 + 1$ à l'exercice 19. Son explication générale, hors programme, est que le groupe de Galois ne contient aucun 6-cycle.

Exercice 37 ⋆⋆⋆

D'après l'exercice 26, le corps de décomposition est $L = \mathbb{Q}(\alpha\,;\zeta)$ avec $\alpha = \sqrt[5]{2}$ et $\zeta = \mathrm{e}^{2\mathrm{i}\pi/5}$, de degré 20 ; comme $L/\mathbb{Q}$ est galoisienne, $|G| = 20$. Un élément $\sigma \in G$ envoie ζ sur une racine primitive cinquième de l'unité et α sur une racine de $X^5 - 2$:

$$\sigma(\zeta) = \zeta^a \quad (a \in \mathbb{F}_5^*) \qquad \text{et} \qquad \sigma(\alpha) = \alpha\zeta^b \quad (b \in \mathbb{F}_5)$$

L'élément σ est déterminé par le couple $(a\,;b)$, et il y a $4 \times 5 = 20$ couples : tous sont réalisés. Si τ correspond à $(c\,;d)$, alors $\sigma\tau(\zeta) = \zeta^{ac}$ et $\sigma\tau(\alpha) = \sigma\big(\alpha\zeta^d\big) = \alpha\zeta^{b+ad}$. Or dans le groupe affine, $\varphi_{a,b} \circ \varphi_{c,d} = \varphi_{ac,\,ad+b}$: l'application $\sigma \mapsto \varphi_{a,b}$ est un isomorphisme.

$$\boxed{\mathrm{Gal}(X^5 - 2) \simeq \mathrm{Aff}(\mathbb{F}_5),\ \text{d'ordre } 20}$$

Ce groupe est résoluble, conformément à l'exercice 15 et au fait évident que les racines de $X^5 - 2$ s'expriment par radicaux. Le sous-groupe $\mathrm{Gal}(L/\mathbb{Q}(\zeta))$ correspond aux translations, et $\mathrm{Gal}(L/\mathbb{Q}(\alpha))$ au stabilisateur de 0.

Exercice 38 ⋆⋆⋆

Soit x une racine de f dans un corps de décomposition L. Pour $b \in \mathbb{F}_p \subseteq K$, le rêve du débutant donne $f(x + b) = x^p + b^p - x - b - a = f(x) = 0$, puisque $b^p = b$. Les racines de f sont donc les p éléments distincts $x + b$, $b \in \mathbb{F}_p$: f est séparable, et $L = K(x)$ pour n'importe quelle racine x.

Tout $\sigma \in G = \mathrm{Gal}(L/K)$ vérifie $\sigma(x) = x + b_\sigma$ pour un unique $b_\sigma \in \mathbb{F}_p$, et $\sigma\tau(x) = x + b_\tau + b_\sigma$: l'application $\sigma \mapsto b_\sigma$ est un morphisme injectif de G dans $(\mathbb{F}_p\,;+)$. Comme $x \notin K$, le groupe G n'est pas trivial ; p étant premier, $G \simeq \mathbb{Z}/p\mathbb{Z}$. Ainsi $[K(x) : K] = |G| = p = \deg f$, et f, qui annule x, est son polynôme minimal.

$$\boxed{f \text{ est irréductible, } L = K(x),\ \text{et } \mathrm{Gal}(L/K) \simeq \mathbb{Z}/p\mathbb{Z}.}$$

Application. Le polynôme $X^p - X - 1$ n'a pas de racine dans $\mathbb{F}_p$, puisque $x^p - x = 0$ pour tout $x \in \mathbb{F}_p$. Il est donc irréductible sur $\mathbb{F}_p$; étant unitaire, il est irréductible sur $\mathbb{Q}$ d'après le critère de réduction de l'exercice 19, question 4.

$$\boxed{X^p - X - 1 \text{ est irréductible sur } \mathbb{Q} \text{ pour tout nombre premier } p.}$$

Exercice 39 ⋆⋆⋆

Notons $L = \mathbb{C}(t\,;u)$, $K = \mathbb{C}\big(t^n\,;u^n\big)$ et $\zeta = \mathrm{e}^{2\mathrm{i}\pi/n}$. Pour $(a\,;b) \in \big(\mathbb{Z}/n\mathbb{Z}\big)^2$, la substitution $F(t\,;u) \mapsto F\big(\zeta^a t\,;\zeta^b u\big)$ définit un automorphisme $\sigma_{a,b}$ de L, de réciproque $\sigma_{-a,-b}$, qui fixe K. Ces automorphismes forment un groupe $G \simeq \big(\mathbb{Z}/n\mathbb{Z}\big)^2$, d'ordre n^2, et $K \subseteq L^G$.

D'après le théorème d'Artin, L/L^G est galoisienne de groupe G, et $\big[L : L^G\big] = n^2$. D'autre part $L = K(t\,;u)$, où t est racine de $X^n - t^n \in K[X]$ et u racine de $X^n - u^n$; par multiplicativité des degrés, $[L : K] \leqslant n \times n = n^2$. Ainsi $n^2 = \big[L : L^G\big] \leqslant [L : K] \leqslant n^2$, et $L^G = K$.

$$\boxed{\mathbb{C}(t\,;u)/\mathbb{C}\big(t^n\,;u^n\big) \text{ est galoisienne, de groupe } \big(\mathbb{Z}/n\mathbb{Z}\big)^2.}$$

Le corps $\mathbb{C}$ ne sert qu'à fournir une racine primitive n-ième de l'unité : le résultat vaut sur tout corps qui en contient une.

Exercice 40 ⋆⋆⋆

Posons $\beta = \sqrt{a - \sqrt{b}}$, racine carrée complexe de $a - \sqrt{b}$. Les nombres $\pm\alpha$ et $\pm\beta$ sont les racines de $f = X^4 - 2aX^2 + (a^2 - b) \in \mathbb{Q}[X]$, et l'on a :

$$(\alpha\beta)^2 = (a + \sqrt{b})(a - \sqrt{b}) = a^2 - b$$

Condition suffisante. Si $a^2-b=c^2$ avec $c\in\mathbb{Q}_+$, alors $b\leqslant a^2$; comme $a+\sqrt{b}>0$, on a nécessairement $a>0$. Posons $x=\dfrac{a+c}{2}$ et $y=\dfrac{a-c}{2}$: leur somme vaut $a>0$ et leur produit $\dfrac{b}{4}>0$, donc ils sont positifs, et $\left(\sqrt{x}+\sqrt{y}\right)^2=a+2\sqrt{xy}=a+\sqrt{b}$. Ainsi $\alpha=\sqrt{x}+\sqrt{y}$ se désimbrique.

Condition nécessaire. Supposons $\alpha\in M=\mathbb{Q}\left(\sqrt{c_1}\,;\ldots\,;\sqrt{c_k}\right)$. Le corps M est le corps de décomposition de $\prod\left(X^2-c_i\right)$; tout élément de son groupe de Galois change les signes des $\sqrt{c_i}$, si bien que ce groupe est abélien, d'exposant 2. Tout sous-groupe étant distingué, $\mathbb{Q}(\alpha)/\mathbb{Q}$ est galoisienne, et son groupe, quotient du précédent, est abélien d'exposant 2. Comme $\alpha^2=a+\sqrt{b}\notin\mathbb{Q}$, on a $[\mathbb{Q}(\alpha):\mathbb{Q}]\in\{2\,;4\}$.

- Si $[\mathbb{Q}(\alpha):\mathbb{Q}]=2$, alors $\mathbb{Q}(\alpha)=\mathbb{Q}(\sqrt{b})$, et $\alpha=u+v\sqrt{b}$ avec $u,v\in\mathbb{Q}$. En identifiant, $u^2+bv^2=a$ et $2uv=1$, d'où $a^2-b=\left(u^2+bv^2\right)^2-4u^2v^2b=\left(u^2-bv^2\right)^2$.
- Si $[\mathbb{Q}(\alpha):\mathbb{Q}]=4$, alors f est le polynôme minimal de α, et $\beta\in\mathbb{Q}(\alpha)$. Soit σ l'automorphisme tel que $\sigma(\alpha)=\beta$: comme $\sigma^2=\mathrm{id}$, on a $\sigma(\beta)=\alpha$, donc $\sigma(\alpha\beta)=\alpha\beta$. Soit τ tel que $\tau(\alpha)=-\alpha$: il fixe $\sqrt{b}=\alpha^2-a$, donc $\tau(\beta)=\pm\beta$. Si l'on avait $\tau(\beta)=\beta$, alors $\sigma\tau(\alpha)=-\beta$ et $\tau\sigma(\alpha)=\beta$, contredisant la commutativité ; donc $\tau(\beta)=-\beta$ et $\tau(\alpha\beta)=\alpha\beta$. Le produit $\alpha\beta$ est fixé par σ et τ, qui engendrent le groupe d'ordre 4 : il est rationnel, et $a^2-b=(\alpha\beta)^2$ est le carré d'un rationnel.

$$\boxed{\sqrt{a+\sqrt{b}}\text{ se désimbrique }\iff a^2-b\text{ est le carré d'un rationnel.}}$$

Application. Pour $\sqrt{2+\sqrt{11}}$, on a $a^2-b=-7$; pour $\sqrt{11+\sqrt{6}}$, on a $a^2-b=115$: ces deux nombres ne se désimbriquent pas. Pour $\sqrt{6+\sqrt{11}}$, on a $a^2-b=25$, d'où $x=\frac{11}{2}$ et $y=\frac{1}{2}$; pour $\sqrt{11+6\sqrt{2}}=\sqrt{11+\sqrt{72}}$, on a $a^2-b=49$, d'où $x=9$ et $y=2$:

$$\boxed{\sqrt{6+\sqrt{11}}=\frac{\sqrt{22}+\sqrt{2}}{2}\qquad\sqrt{11+6\sqrt{2}}=3+\sqrt{2}}$$

Exercice 41 ⋆⋆⋆⋆

D'après l'exemple du cours consacré aux fonctions symétriques, L/M est galoisienne de groupe $\mathfrak{S}_4$, agissant par permutation des indéterminées. Une permutation envoie le découpage $\{\{1\,;3\}\,;\{2\,;4\}\}$ de $\{1\,;2\,;3\,;4\}$ sur l'un des trois découpages en deux paires ; l'orbite de θ est donc formée des trois éléments distincts

$$\theta_1=X_1X_3+X_2X_4\qquad\theta_2=X_1X_2+X_3X_4\qquad\theta_3=X_1X_4+X_2X_3$$

Le polynôme minimal de θ sur M est le produit des $T-\theta_i$, de coefficients symétriques donc dans M. Son développement donne :

$$\boxed{\mu_\theta=T^3-s_2T^2+(s_1s_3-4s_4)T-(s_1^2s_4-4s_2s_4+s_3^2)}$$

Le stabilisateur H de θ est formé des permutations qui préservent le découpage $\{\{1\,;3\}\,;\{2\,;4\}\}$; il est d'ordre $\dfrac{24}{3}=8$. Les permutations (1 2 3 4) et (1 3) préservent ce découpage et engendrent un groupe D d'ordre 8, isomorphe à D_4 : donc $D=H$. D'après la correspondance de Galois, L^D contient $M(\theta)$, et $\left[L^D:M\right]=\left[\mathfrak{S}_4:D\right]=3=[M(\theta):M]$.

$$\boxed{L^D=M(\theta)}$$

Pour un polynôme X^4+pX+q, on a $s_1=s_2=0$, $s_3=-p$ et $s_4=q$, et μ_θ devient $T^3-4qT-p^2$: c'est la résolvante cubique utilisée à l'exercice 50, qui prend ici tout son sens.

Exercice 42 ⋆⋆⋆⋆

Posons $F=\mathbb{Q}(\sqrt{2}\,;\sqrt{3})$, de degré 4, et $a=(2+\sqrt{2})(3+\sqrt{3})$. Pour des signes ε,ε', notons $a_{\varepsilon,\varepsilon'}=(2+\varepsilon\sqrt{2})(3+\varepsilon'\sqrt{3})$: ce sont quatre éléments distincts de F.

Le nombre a n'est pas un carré dans F. Soit ρ l'automorphisme de F qui change le signe de $\sqrt{2}$ et fixe $\sqrt{3}$. Si $a = \gamma^2$ avec $\gamma \in F$, alors $\gamma\rho(\gamma)$ est fixé par ρ, donc appartient à $\mathbb{Q}(\sqrt{3})$, et $\big(\gamma\rho(\gamma)\big)^2 = a\,\rho(a) = 2(3+\sqrt{3})^2$. Le nombre 2 serait un carré dans $\mathbb{Q}(\sqrt{3})$, ce qui est faux. Ainsi $[F(\alpha) : F] = 2$ et $[F(\alpha) : \mathbb{Q}] = 8$.

Le corps $F(\alpha)$ est galoisien. Il contient les racines carrées de tous les $a_{\varepsilon,\varepsilon'}$, car les produits

$$\alpha^2 a_{-,+} = 2(3+\sqrt{3})^2 \qquad \alpha^2 a_{+,-} = 6(2+\sqrt{2})^2 \qquad \alpha^2 a_{-,-} = 12$$

sont des carrés dans F. C'est donc le corps de décomposition du polynôme $\prod (X^2 - a_{\varepsilon,\varepsilon'})$, à coefficients rationnels, et $F(\alpha)/\mathbb{Q}$ est galoisienne de degré 8.

On a $E = F(\alpha)$. Tout $g \in G = \mathrm{Gal}(F(\alpha)/\mathbb{Q})$ vérifie $g(\alpha)^2 = g(a) = a_{\varepsilon,\varepsilon'}$, les signes étant ceux de la restriction de g à F. Si $g(\alpha) = g'(\alpha)$, alors $g(a) = g'(a)$, les restrictions à F coïncident, et $g = g'$. L'élément α a donc huit conjugués distincts : $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 8$, et $E = F(\alpha)$ est galoisienne de degré 8.

Le groupe. Notons z l'automorphisme qui fixe F et change α en $-\alpha$; il change aussi le signe des racines $\dfrac{\gamma}{\alpha}$, $\gamma \in F$, donc il commute à tout $g \in G$. Soit σ un relèvement de ρ. D'après la première égalité ci-dessus, $\sigma(\alpha) = \dfrac{s\sqrt{2}(3+\sqrt{3})}{\alpha}$ avec $s = \pm 1$, d'où :

$$\sigma^2(\alpha) = \frac{s\,\sigma(\sqrt{2}(3+\sqrt{3}))}{\sigma(\alpha)} = \frac{-s\sqrt{2}(3+\sqrt{3})\,\alpha}{s\sqrt{2}(3+\sqrt{3})} = -\alpha$$

Donc $\sigma^2 = z$. Le même calcul, mené avec $\sqrt{6}(2+\sqrt{2})$ et $2\sqrt{3}$, montre que tout relèvement τ de l'automorphisme qui fixe $\sqrt{2}$ et change le signe de $\sqrt{3}$ vérifie $\tau^2 = z$, et que $(\sigma\tau)^2 = z$, puisque $\sigma\tau$ relève le troisième élément non trivial de $\mathrm{Gal}(F/\mathbb{Q})$.

Le commutateur $\sigma\tau\sigma^{-1}\tau^{-1}$ se restreint à l'identité sur F, le groupe $\mathrm{Gal}(F/\mathbb{Q})$ étant abélien : il vaut id ou z. S'il valait id, on aurait $(\sigma\tau)^2 = \sigma^2\tau^2 = z^2 = \mathrm{id}$, ce qui est faux. Donc $\sigma\tau = z\,\tau\sigma$. Posons alors $\mathrm{i} = \sigma$, $\mathrm{j} = \tau$, $\mathrm{k} = \sigma\tau$ et $-1 = z$: on a $\mathrm{i}^2 = \mathrm{j}^2 = \mathrm{k}^2 = -1$, l'élément -1 est central d'ordre 2, et

$$\mathrm{jk} = \tau\sigma\tau = z\,\sigma\tau^2 = \sigma = \mathrm{i} \qquad \mathrm{ki} = \sigma\tau\sigma = z\,\sigma^2\tau = \tau = \mathrm{j}$$

Ce sont exactement les relations qui définissent Q_8 à l'exercice 8. Les huit éléments ± 1, $\pm\mathrm{i}$, $\pm\mathrm{j}$, $\pm\mathrm{k}$ de G sont distincts, car leurs restrictions à F et leurs actions sur α les séparent, et leur table de multiplication est entièrement déterminée par ces relations.

$$\boxed{\mathrm{Gal}(E/\mathbb{Q}) \simeq Q_8}$$

Le groupe des quaternions, dont les sous-groupes sont tous distingués, n'a que des sous-corps galoisiens : les trois corps quadratiques de F, le corps F lui-même, $\mathbb{Q}$ et E.

Chapitre 7 - Résolubilité par radicaux

Questions de cours

Q1. Voir la proposition 7.1 : chaque racine n-ième de l'unité est racine primitive d-ième pour un unique $d \mid n$; l'intégralité s'obtient par récurrence, en divisant $X^n - 1$ par le produit des Φ_d, $d \mid n$, $d < n$, qui est unitaire à coefficients entiers.

Q2. Voir le théorème 7.2 : $\mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}) \simeq (\mathbb{Z}/n\mathbb{Z})^*$, d'ordre $\varphi(n)$.

Q3. Le groupe de Galois d'un polynôme de degré au plus 4 se plonge dans $\mathfrak{S}_4$, qui est résoluble ; le critère 7.4 conclut. Dans la méthode de Cardan, la racine carrée du discriminant fournit le premier étage, les racines cubiques le second.

Q4. Voir la proposition 7.5 et le théorème 7.5 : le groupe contient un 5-cycle, par le théorème de Cauchy, et une transposition, la conjugaison complexe ; ils engendrent $\mathfrak{S}_5$, qui n'est pas résoluble.

Q5. Voir le théorème 7.7 : le polygone régulier à n côtés est constructible si et seulement si n est le produit d'une puissance de 2 par des nombres premiers de Fermat distincts.

Q6. Voir le théorème 7.8 : on se ramène à une extension galoisienne L de $\mathbb{R}$ contenant $\mathbb{C}$; son 2-Sylow fixe un corps de degré impair, égal à $\mathbb{R}$, puis un sous-groupe d'indice 2 fournirait une extension quadratique de $\mathbb{C}$, qui n'existe pas.

Exercice 43 ⋆

1. On divise successivement $X^n - 1$ par les Φ_d déjà connus, pour $d \mid n$ et $d < n$:

n	Φ_n	$\varphi(n)$	n	Φ_n	$\varphi(n)$
1	$X-1$	1	7	$X^6+X^5+X^4+X^3+X^2+X+1$	6
2	$X+1$	1	8	X^4+1	4
3	X^2+X+1	2	9	X^6+X^3+1	6
4	X^2+1	2	10	$X^4-X^3+X^2-X+1$	4
5	$X^4+X^3+X^2+X+1$	4	11	$\sum_{k=0}^{10} X^k$	10
6	X^2-X+1	2	12	X^4-X^2+1	4

2. Le degré de Φ_n est le nombre de racines primitives n-ièmes, c'est-à-dire le nombre de $k \in [\![1\,;n]\!]$ premiers à n :

$$\boxed{\deg \Phi_n = \varphi(n), \text{ ce que confirme le tableau.}}$$

3. Si m est impair > 1, l'application $\zeta \mapsto -\zeta$ est une bijection entre les racines primitives m-ièmes et les racines primitives $2m$-ièmes. Comme $\deg \Phi_m = \varphi(m)$ est pair, le signe dominant est préservé :

$$\boxed{\Phi_{2m}(X) = \Phi_m(-X)}$$

Vérification : $\Phi_3(-X) = X^2 - X + 1 = \Phi_6$ et $\Phi_5(-X) = X^4 - X^3 + X^2 - X + 1 = \Phi_{10}$ ✓

Exercice 44 ⋆⋆⋆⋆

1. $\mathbb{Q}(\zeta_{15})$ est le corps de décomposition de $X^{15} - 1$, séparable puisque $\mathrm{pgcd}(X^{15} - 1\,; 15X^{14}) = 1$ en caractéristique nulle :

$$\boxed{\text{Extension galoisienne de degré } \varphi(15) = 8.}$$

2. Tout $\sigma \in G$ envoie ζ_{15} sur ζ_{15}^k avec $\mathrm{pgcd}(k\,;15) = 1$, et $\sigma \mapsto \overline{k}$ est un isomorphisme. Par le théorème chinois :

$$\boxed{G \simeq (\mathbb{Z}/15\mathbb{Z})^* \simeq (\mathbb{Z}/3\mathbb{Z})^* \times (\mathbb{Z}/5\mathbb{Z})^* \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}}$$

3. Le groupe $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$ possède huit sous-groupes, dont trois d'ordre 4 :

$$\boxed{\text{Huit corps intermédiaires, dont trois quadratiques : } \mathbb{Q}(\sqrt{5}),\ \mathbb{Q}(\sqrt{-3}),\ \mathbb{Q}(\sqrt{-15}).}$$

4. La somme de Gauss $g = \sum_{k=1}^{4} \left(\frac{k}{5}\right) \zeta_5^k = \zeta_5 + \zeta_5^4 - \zeta_5^2 - \zeta_5^3$ vérifie $g^2 = 5$:

$$\boxed{\sqrt{5} = \zeta_5 + \zeta_5^4 - \zeta_5^2 - \zeta_5^3 \in \mathbb{Q}(\zeta_5) \subset \mathbb{Q}(\zeta_{15})}$$

On peut aussi écrire $\zeta_5 + \zeta_5^4 = 2\cos\dfrac{2\pi}{5} = \dfrac{-1+\sqrt{5}}{2}$.

5. $\mathrm{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q}) \simeq (\mathbb{Z}/p\mathbb{Z})^*$ est cyclique d'ordre $p-1$ pair, donc possède un unique sous-groupe d'indice 2, donc $\mathbb{Q}(\zeta_p)$ possède un unique sous-corps quadratique. La somme de Gauss donne $g^2 = \left(\frac{-1}{p}\right) p$:

$$\boxed{\mathbb{Q}(\sqrt{p}) \text{ si } p \equiv 1\ [4] \qquad \mathbb{Q}(\sqrt{-p}) \text{ si } p \equiv 3\ [4]}$$

Exercice 45 ⋆⋆⋆

1. On a $X^{16} - 1 = \prod_{d|16} \Phi_d$, et $16 = 2^4$ n'a que des diviseurs de la forme 2^j. Comme $X^8 - 1 = \prod_{j \leqslant 3} \Phi_{2^j}$, il vient $\Phi_{16} = \dfrac{X^{16}-1}{X^8-1} = X^8 + 1$.

$$\boxed{\Phi_{16} = X^8 + 1 \qquad \text{et} \qquad [\mathbb{Q}(\zeta_{16}) : \mathbb{Q}] = \varphi(16) = 8}$$

2. Le groupe $(\mathbb{Z}/16\mathbb{Z})^* = \{1\,;3\,;5\,;7\,;9\,;11\,;13\,;15\}$ est d'ordre 8. On calcule les ordres :

a	1	3	5	7	9	11	13	15
ordre	1	4	4	2	2	4	4	2

$$\boxed{\text{Aucun élément d'ordre 8 : } (\mathbb{Z}/16\mathbb{Z})^* \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}}$$

Un isomorphisme est donné par $(-1)^i 5^j \mapsto (i\,;j)$.

3.

$$\boxed{\mathrm{Gal}(\mathbb{Q}(\zeta_{16})/\mathbb{Q}) \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z} \text{ n'est pas cyclique.}}$$

Piège à retenir. On retient volontiers que $\mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}) \simeq (\mathbb{Z}/n\mathbb{Z})^*$ *et* que ce groupe est cyclique. La seconde affirmation n'est vraie que pour n premier, ou plus généralement pour $n \in \{1\,;2\,;4\,;p^k\,;2p^k\}$ avec p impair. Dès $n = 16$, elle tombe.

4. Les sous-corps quadratiques correspondent aux sous-groupes d'indice 2, c'est-à-dire d'ordre 4. Le groupe $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$ en possède trois.

$$\boxed{\mathbb{Q}(\mathrm{i})\ ,\ \mathbb{Q}(\sqrt{2})\ ,\ \mathbb{Q}(\sqrt{-2})}$$

En effet $\zeta_{16}^4 = \mathrm{i}$ et $\zeta_{16}^2 + \zeta_{16}^{-2} = 2\cos\dfrac{\pi}{4} = \sqrt{2}$.

5. Posons $k \geqslant 3$. On démontre par récurrence que $5^{2^{k-3}} = 1 + 2^{k-1} + \lambda 2^k$ pour un entier λ, ce qui donne $5^{2^{k-3}} \neq 1$ et $5^{2^{k-2}} = 1$ modulo 2^k : l'élément 5 est d'ordre 2^{k-2}. Par ailleurs $\langle 5 \rangle$ ne contient que des éléments congrus à 1 modulo 4, alors que $-1 \equiv 3\ [4]$.

$$\boxed{(\mathbb{Z}/2^k\mathbb{Z})^* = \{\pm 1\} \times \langle 5 \rangle \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2^{k-2}\mathbb{Z}}$$

6. Aucune : le critère de constructibilité porte sur $\varphi(n)$, qui doit être une puissance de 2, et non sur la cyclicité du groupe. Ici $\varphi(16) = 8 = 2^3$.

$$\boxed{\text{Le polygone régulier à 16 côtés est constructible, comme tout } 2^k\text{-gone.}}$$

La tour de radicaux carrés se lit d'ailleurs sur la chaîne de sous-groupes d'indices 2 successifs du groupe de Galois.

Exercice 46 ⋆⋆

1. $(\mathbb{Z}/7\mathbb{Z})^*$ est cyclique d'ordre 6, engendré par $\overline{3}$:

$$\boxed{\mathrm{Gal}(\mathbb{Q}(\zeta_7)/\mathbb{Q}) \simeq \mathbb{Z}/6\mathbb{Z}, \text{ engendré par } \sigma : \zeta \mapsto \zeta^3.}$$

2. Un groupe cyclique d'ordre 6 possède exactement quatre sous-groupes, d'ordres 1, 2, 3, 6 :

$$\boxed{\mathbb{Q} \subset \mathbb{Q}(\sqrt{-7}) \subset \mathbb{Q}(\zeta_7) \qquad \text{et} \qquad \mathbb{Q} \subset \mathbb{Q}(\cos\tfrac{2\pi}{7}) \subset \mathbb{Q}(\zeta_7)}$$

Le corps de degré 2 correspond au sous-groupe d'ordre 3, celui de degré 3 au sous-groupe d'ordre 2, engendré par la conjugaison complexe $\zeta \mapsto \zeta^{-1}$.

3. Le corps fixe de $\langle\sigma^3\rangle = \{\mathrm{id}\,; \zeta \mapsto \zeta^{-1}\}$ est engendré par les *périodes de Gauss* :

$$\boxed{\eta_1 = \zeta + \zeta^6, \quad \eta_2 = \zeta^3 + \zeta^4, \quad \eta_3 = \zeta^2 + \zeta^5}$$

Ce sont les $2\cos\dfrac{2k\pi}{7}$, racines de $X^3 + X^2 - 2X - 1$, et $\mathbb{Q}(\eta_1)$ est le sous-corps de degré 3.

4. Un groupe abélien est résoluble (proposition 2.6), et le théorème 7.4 conclut.

$$\boxed{\text{Toute extension abélienne de } \mathbb{Q} \text{ est résoluble par radicaux.}}$$

Exercice 47 ⋆⋆⋆

La formule $2\cos\dfrac{\theta}{2} = \sqrt{2 + 2\cos\theta}$, valable pour $\theta \in [0\,;\pi]$, appliquée trois fois à partir de $2\cos\dfrac{\pi}{4} = \sqrt{2}$, donne :

$$\alpha = \sqrt{2 + \sqrt{2 + \sqrt{2}}} = 2\cos\frac{\pi}{16} = \zeta + \zeta^{-1} \qquad \text{avec} \qquad \zeta = \mathrm{e}^{\mathrm{i}\pi/16}$$

et ζ est une racine primitive 32-ième de l'unité. L'extension $\mathbb{Q}(\zeta)/\mathbb{Q}$ est galoisienne de groupe $(\mathbb{Z}/32\mathbb{Z})^*$, abélien, d'après le théorème 7.2 : tous ses sous-groupes sont distingués, donc le sous-corps $\mathbb{Q}(\alpha)$ est galoisien sur $\mathbb{Q}$.

Le nombre ζ est racine de $X^2 - \alpha X + 1 \in \mathbb{Q}(\alpha)[X]$ et n'est pas réel, alors que $\mathbb{Q}(\alpha) \subset \mathbb{R}$: ainsi $[\mathbb{Q}(\zeta) : \mathbb{Q}(\alpha)] = 2$, et $\mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q}(\alpha))$ est le sous-groupe $\{\pm 1\}$, qui correspond à la conjugaison. Par conséquent :

$$\mathrm{Gal}(\mathbb{Q}(\alpha)/\mathbb{Q}) \simeq (\mathbb{Z}/32\mathbb{Z})^*/\{\pm 1\}, \text{ d'ordre } \frac{16}{2} = 8$$

Ce quotient est cyclique : $3^4 = 81 \equiv 17\ [32]$ n'est pas ± 1, donc la classe de 3 n'est pas d'ordre divisant 4 ; elle est d'ordre 8 et engendre le quotient.

$$\boxed{\mathbb{Q}\Big(\sqrt{2 + \sqrt{2 + \sqrt{2}}}\Big)/\mathbb{Q} \text{ est galoisienne de groupe } \mathbb{Z}/8\mathbb{Z}.}$$

Le polynôme minimal de α est $X^8 - 8X^6 + 20X^4 - 16X^2 + 2$, irréductible par Eisenstein en 2 : on retrouve le degré 8 sans passer par la cyclotomie.

Exercice 48 ⋆⋆⋆

Un sens est immédiat : une factorisation non triviale sur K en est une sur $K(\zeta)$. Réciproquement, supposons $X^p - a$ irréductible sur K, et soit α une racine, de sorte que $[K(\alpha) : K] = p$. Le nombre ζ est racine de $X^{p-1} + \cdots + X + 1$, donc $m = [K(\zeta) : K] \leqslant p - 1$ est premier avec p. Le degré $[K(\zeta\,;\alpha) : K]$ est divisible par p et par m, donc par mp, et il vaut au plus $m\,[K(\zeta\,;\alpha) : K(\zeta)] \leqslant mp$. Ainsi $[K(\zeta\,;\alpha) : K(\zeta)] = p$, et $X^p - a$, qui annule α, est irréductible sur $K(\zeta)$.

$$\boxed{X^p - a \text{ est irréductible sur } K \iff \text{il l'est sur } K(\zeta)}$$

Le résultat tombe pour un exposant composé : $X^4 + 1 = X^4 - (-1)$ est irréductible sur $\mathbb{Q}$ d'après l'exercice 19, mais se factorise sur $\mathbb{Q}(\mathrm{i}) = \mathbb{Q}(\zeta_4)$ en $(X^2 - \mathrm{i})(X^2 + \mathrm{i})$. L'argument échoue parce que $[\mathbb{Q}(\mathrm{i}) : \mathbb{Q}] = 2$ n'est pas premier avec 4.

Exercice 49 ⋆⋆⋆

1. Les racines rationnelles possibles sont ± 1, et $P(1) = -1$, $P(-1) = 3$: le polynôme, de degré 3, est donc irréductible sur $\mathbb{Q}$.

L'étude de $x \mapsto x^3 - 3x + 1$ donne $P'(x) = 3(x^2 - 1)$, d'où un maximum local $P(-1) = 3 > 0$ et un minimum local $P(1) = -1 < 0$.

$$\boxed{P \text{ est irréductible et possède trois racines réelles, } \approx -1{,}879\ ;\ 0{,}347\ ;\ 1{,}532.}$$

2. Avec $p = -3$ et $q = 1$:

$$\Delta = -4(-3)^3 - 27(1)^2 = 108 - 27 = 81$$

$$\boxed{\Delta = 81 = 9^2 \text{ est un carré parfait.}}$$

3. Le groupe G est un sous-groupe transitif de $\mathfrak{S}_3$, donc $\mathfrak{S}_3$ ou $\mathfrak{A}_3$. Le discriminant étant un carré, $G \subseteq \mathfrak{A}_3$.

$$\boxed{G = \mathfrak{A}_3 \simeq \mathbb{Z}/3\mathbb{Z}}$$

4. On a $|G| = 3$, donc $[L : \mathbb{Q}] = 3$. Comme $\mathbb{Q}(\alpha) \subseteq L$ et $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 3$, il vient $L = \mathbb{Q}(\alpha)$: le corps de décomposition est engendré par *une* racine.

Vérifions que $\alpha^2 - 2$ est encore racine. De $\alpha^3 = 3\alpha - 1$ on tire :

$$(\alpha^2 - 2)^3 - 3(\alpha^2 - 2) + 1 = \alpha^6 - 6\alpha^4 + 9\alpha^2 - 1$$

et $\alpha^6 = (3\alpha - 1)^2 = 9\alpha^2 - 6\alpha + 1$, $\alpha^4 = \alpha \cdot \alpha^3 = 3\alpha^2 - \alpha$, d'où :

$$9\alpha^2 - 6\alpha + 1 - 6(3\alpha^2 - \alpha) + 9\alpha^2 - 1 = 9\alpha^2 - 18\alpha^2 + 9\alpha^2 - 6\alpha + 6\alpha = 0$$

$$\boxed{\alpha \mapsto \alpha^2 - 2 \text{ permute les trois racines : c'est un générateur de } G.}$$

5. La formule $\cos(3\theta) = 4\cos^3\theta - 3\cos\theta$ avec $\theta = \dfrac{2\pi}{9}$ donne $\cos\dfrac{2\pi}{3} = -\dfrac{1}{2}$, soit :

$$4c^3 - 3c = -\frac{1}{2} \qquad \text{avec} \qquad c = \cos\frac{2\pi}{9}$$

En posant $\alpha = 2c$, il vient $\dfrac{\alpha^3}{2} - \dfrac{3\alpha}{2} = -\dfrac{1}{2}$, donc $\alpha^3 - 3\alpha + 1 = 0$.

$$\boxed{2\cos\frac{2\pi}{9} \text{ est racine de } P, \text{ et } L = \mathbb{Q}\big(2\cos\tfrac{2\pi}{9}\big) \subset \mathbb{Q}(\zeta_9).}$$

6. Le corps L est réel, de degré 3 sur $\mathbb{Q}$. Une formule de Cardan sans nombres complexes exigerait d'extraire une racine carrée de Δ puis une racine cubique à l'intérieur de $\mathbb{R}$. Or $\sqrt{\Delta} = 9 \in \mathbb{Q}$: l'étape

quadratique ne produit rien, et il faudrait que L contienne une racine cubique réelle non triviale, c'est-à-dire une sous-extension de degré 3 obtenue par radicaux réels — ce que le degré 3 de L sur $\mathbb{Q}$, premier, interdit sans passer par $\mathbb{Q}(\mathrm{j})$.

C'est le *casus irreducibilis* : une cubique à trois racines réelles n'est jamais résoluble par radicaux *réels* si elle est irréductible.

Le détour par $\mathbb{C}$ n'est donc pas une maladresse de Cardan : il est inévitable.

Exercice 50 ⋆⋆⋆⋆

1. Les racines rationnelles possibles divisent 12 : on vérifie que ±1, ±2, ±3, ±4, ±6, ±12 ne conviennent pas. Reste à écarter une factorisation en deux facteurs de degré 2 ; en écrivant

$$X^4 + 8X + 12 = (X^2 + aX + b)(X^2 - aX + c)$$

l'identification donne $b + c - a^2 = 0$, $a(c - b) = 8$ et $bc = 12$. De $c - b = \dfrac{8}{a}$ et $b + c = a^2$ on tire $4bc = a^4 - \dfrac{64}{a^2}$, soit $a^6 - 48a^2 - 64 = 0$: le réel a^2 serait racine de la résolvante de la question 4, qui est irréductible sur $\mathbb{Q}$.

P est irréductible sur $\mathbb{Q}$.

2. Le groupe G permute les quatre racines et agit transitivement, puisque P est irréductible.

Sous-groupes transitifs de $\mathfrak{S}_4$: $\mathbb{Z}/4\mathbb{Z}$, V, D_4, $\mathfrak{A}_4$, $\mathfrak{S}_4$

Ce sont les seuls : un sous-groupe transitif a un ordre divisible par 4, donc d'ordre 4, 8 ou 24 ; les trois sous-groupes d'ordre 4 qui sont transitifs sont les trois $\mathbb{Z}/4\mathbb{Z}$ et V, les sous-groupes d'ordre 8 sont les trois conjugués de D_4, et l'on ajoute $\mathfrak{A}_4$ et $\mathfrak{S}_4$.

3. Le discriminant vaut 331 776, et $576^2 = 331\,776$.

Δ est un carré, donc $G \subseteq \mathfrak{A}_4$.

Il ne reste que deux possibilités, V et $\mathfrak{A}_4$, puisque $\mathbb{Z}/4\mathbb{Z}$ et D_4 contiennent des 4-cycles, qui sont impairs.

4. Avec $p = 8$ et $q = 12$:

$$R = X^3 - 4 \times 12\, X - 8^2 = X^3 - 48X - 64$$

Ses racines rationnelles diviseraient 64 ; on vérifie que ±1, ±2, ±4, ±8, ±16, ±32, ±64 ne conviennent pas — par exemple $R(8) = 512 - 384 - 64 = 64 \neq 0$. Étant de degré 3 sans racine rationnelle :

$R = X^3 - 48X - 64$ est irréductible sur $\mathbb{Q}$.

5. La résolvante n'étant pas scindée, $G \not\subseteq V$.

$$G \simeq \mathfrak{A}_4 \qquad \text{et} \qquad [L : \mathbb{Q}] = |G| = 12$$

6. Les exemples usuels de degré 4 épuisent les autres cas : $X^4 - 5X^2 + 6$ donne V, $X^4 + 1$ donne V également, $X^4 - 2$ donne D_4, et un polynôme « générique » donne $\mathfrak{S}_4$.

$\mathfrak{A}_4$ est le sous-groupe transitif de $\mathfrak{S}_4$ que l'on ne rencontre jamais dans les exemples classiques : il exige un discriminant carré *et* une résolvante cubique irréductible.

C'est aussi le seul des cinq pour lequel $[L : \mathbb{Q}] = 12$ n'est ni 4, ni 8, ni 24.

Exercice 51 ⋆⋆⋆

Sur $\mathbb{Q}$. Le polynôme $f = X^5 + 20X^2 - 2$ est irréductible par Eisenstein en 2. Sa dérivée $5x^4 + 40x = 5x(x^3 + 8)$ s'annule en -2 et 0, avec $f(-2) = 46 > 0$ et $f(0) = -2 < 0$; comme f tend vers $-\infty$ en $-\infty$ et vers $+\infty$ en $+\infty$, le théorème des valeurs intermédiaires fournit exactement trois racines réelles. La proposition 7.5 donne :

$$\boxed{\mathrm{Gal}_{\mathbb{Q}}(f) \simeq \mathfrak{S}_5}$$

Sur K. Soit $L \subset \mathbb{C}$ le corps de décomposition de f sur $\mathbb{Q}$, de degré 120, et LK le corps engendré par K et les racines de f, qui est le corps de décomposition de f sur K. En calculant $[LK : \mathbb{Q}]$ de deux façons :

$$[LK : K] \times q = [LK : \mathbb{Q}] = [LK : L] \times 120$$

Comme $q \geqslant 7$ est premier, il est premier avec 120, qui divise donc $[LK : K]$. Or $\mathrm{Gal}(LK/K)$ agit fidèlement sur les cinq racines, donc s'identifie à un sous-groupe de $\mathfrak{S}_5$, et $[LK : K] \leqslant 120$. Ainsi $[LK : K] = 120$.

$$\boxed{\mathrm{Gal}_K(f) \simeq \mathfrak{S}_5}$$

Pour $q \in \{2\,;3\,;5\}$, l'argument ne s'applique plus, et la conclusion peut tomber : sur l'extension de degré 2 engendrée par une racine carrée du discriminant de f, le groupe devient $\mathfrak{A}_5$.

Exercice 52 ⋆⋆⋆

1. Modulo 7, le polynôme devient $X^5 + 2X + 5$, qui n'a pas de racine dans $\mathbb{F}_7$ et ne se factorise pas en degrés $2 + 3$ — un calcul direct montre qu'il est irréductible sur $\mathbb{F}_7$. Le lemme de Gauss conclut.

$$\boxed{P \text{ est irréductible sur } \mathbb{Q}.}$$

Piège : le premier 2 ne convient pas, car $P \equiv X(X+1)^4$ [2] : le discriminant est divisible par 2, et la réduction perd la séparabilité.

2. On a $P'(x) = 5x^4 - 5 = 5(x^4 - 1)$, qui s'annule en ± 1. Or :

$$P(-1) = -1 + 5 + 12 = 16 > 0 \qquad \text{et} \qquad P(1) = 1 - 5 + 12 = 8 > 0$$

La fonction croît jusqu'à 16, redescend jusqu'à 8 en restant positive, puis croît. Comme $P(x) \to -\infty$ en $-\infty$, elle ne s'annule qu'une fois.

$$\boxed{P \text{ possède exactement une racine réelle, et quatre racines complexes non réelles.}}$$

3. Le discriminant vaut 64 000 000, et $8000^2 = 64\,000\,000$.

$$\boxed{\Delta \text{ est un carré, donc } G \subseteq \mathfrak{A}_5.}$$

4. Un sous-groupe transitif de $\mathfrak{S}_5$ a un ordre divisible par 5. Ceux contenus dans $\mathfrak{A}_5$ sont :

$$\boxed{\mathbb{Z}/5\mathbb{Z} \text{ (ordre 5)}, \qquad D_5 \text{ (ordre 10)}, \qquad \mathfrak{A}_5 \text{ (ordre 60)}}$$

Le groupe F_{20} d'ordre 20 n'est pas contenu dans $\mathfrak{A}_5$, car il contient des 4-cycles.

5. La conjugaison complexe fixe l'unique racine réelle et échange les racines complexes deux à deux conjuguées : c'est un produit de deux transpositions.

$$\boxed{G \text{ contient un élément d'ordre 2, donc } G \neq \mathbb{Z}/5\mathbb{Z}.}$$

6. Les motifs (5), $(1\,;2\,;2)$ et (1^5) correspondent respectivement à des éléments d'ordre 5, 2 et 1. L'absence du motif $(1\,;1\,;3)$ signale qu'aucun élément de G n'est d'ordre 3.

$$\boxed{G \text{ ne contient aucun élément d'ordre 3, donc } G \neq \mathfrak{A}_5.}$$

En effet $\mathfrak{A}_5$ possède vingt 3-cycles, d'après l'exercice 11. Or D_5 n'a que des éléments d'ordre 1, 2 et 5 — ce qui correspond exactement aux trois motifs observés.

7. Il ne reste qu'une possibilité, et D_5 est résoluble : la suite $\{\mathrm{id}\} \trianglelefteq \mathbb{Z}/5\mathbb{Z} \trianglelefteq D_5$ a pour quotients $\mathbb{Z}/5\mathbb{Z}$ et $\mathbb{Z}/2\mathbb{Z}$.

$$\boxed{G \simeq D_5, \text{ et } P = X^5 - 5X + 12 \textit{ est} \text{ résoluble par radicaux.}}$$

Morale. Le théorème d'Abel-Ruffini n'affirme pas que *toute* équation de degré 5 est irrésoluble, mais qu'il n'existe pas de formule *générale*. Comparée à $X^5 + 20X^2 - 2$ de l'exercice 51, qui a pour groupe $\mathfrak{S}_5$, cette quintique montre que le degré ne décide de rien : c'est la structure du groupe de Galois, et elle seule, qui tranche.

Exercice 53 ⋆⋆⋆

1. On applique le critère à chaque entier :

$$\boxed{n \in \{3\,;4\,;5\,;6\,;8\,;10\,;12\,;15\,;16\,;17\,;20\,;24\,;30\}}$$

2. On récapitule les exclusions :

n	$\varphi(n)$	raison
7, 14, 21, 28	6, 6, 12, 12	7 n'est pas un premier de Fermat
9, 18, 27	6, 6, 18	3^2 divise n
11, 22	10, 10	11 n'est pas un premier de Fermat
13, 26	12, 12	13 n'est pas un premier de Fermat
19	18	19 n'est pas un premier de Fermat
23	22	23 n'est pas un premier de Fermat
25	20	5^2 divise n
29	28	29 n'est pas un premier de Fermat

3. Si $k = ab$ avec a impair > 1, alors $2^b + 1$ divise $2^{ab} + 1$, puisque $Y + 1$ divise $Y^a + 1$ pour a impair, avec $Y = 2^b$. Le nombre $2^k + 1$ n'est donc pas premier.

$$\boxed{2^k + 1 \text{ premier} \Longrightarrow k \text{ est une puissance de 2.}}$$

4. $F_0 = 3$, $F_1 = 5$, $F_2 = 17$, $F_3 = 257$, $F_4 = 65537$ sont premiers ; mais Euler a montré en 1732 que $F_5 = 4294967297 = 641 \times 6700417$ ne l'est pas. Aucun F_m avec $m \geqslant 5$ n'est connu premier.

> On ne sait pas s'il existe une infinité de premiers de Fermat,
> donc la liste des polygones constructibles à nombre impair de côtés
> n'est pas connue en totalité.

Exercice 54 ⋆⋆⋆

Disposer d'un angle de mesure $\dfrac{2\pi}{n}$ revient à disposer du point $\zeta_n = \mathrm{e}^{2\mathrm{i}\pi/n}$, et le trisecter revient à construire ζ_{3n}.

Si 3 *ne divise pas* n. Il existe des entiers u et v tels que $3u + nv = 1$, d'où $\dfrac{2\pi}{3n} = u \cdot \dfrac{2\pi}{n} + v \cdot \dfrac{2\pi}{3}$. L'angle $\dfrac{2\pi}{3}$ est constructible, puisque le triangle équilatéral l'est, et l'on sait reporter et additionner des angles : la trisection est possible.

Si 3 *divise* n. Les points constructibles à partir de 0, 1 et ζ_n sont obtenus par une suite d'extensions de degré 2 au-dessus de $\mathbb{Q}(\zeta_n)$, stable par conjugaison puisque $\overline{\zeta_n} = \zeta_n^{-1}$: la démonstration du critère

de Wantzel s'applique mot pour mot avec ce corps de base, et tout point constructible a un degré sur $\mathbb{Q}(\zeta_n)$ qui est une puissance de 2. Or, d'après le théorème 7.2 :

$$[\mathbb{Q}(\zeta_{3n}) : \mathbb{Q}(\zeta_n)] = \frac{\varphi(3n)}{\varphi(n)} = 3 \qquad \text{lorsque } 3 \mid n$$

Donc ζ_{3n} n'est pas constructible à partir de ζ_n.

$$\boxed{\text{L'angle } \frac{2\pi}{n} \text{ est trisectable si et seulement si } 3 \nmid n.}$$

Pour $n = 6$, on retrouve l'impossibilité de trisecter l'angle $\dfrac{\pi}{3}$, établie au chapitre 4.

Exercice 55 ⋆⋆⋆

Irréductibilité. Soit $P = X^n + X + 3$, et supposons $P = GH$ avec $G, H \in \mathbb{Q}[X]$ unitaires non constants ; d'après le lemme de Gauss (théorème 3.6), on peut les prendre dans $\mathbb{Z}[X]$. Alors $G(0)H(0) = 3$, et l'un des deux, disons $G(0)$, vaut ± 1. D'après le théorème fondamental de l'algèbre, G est scindé sur $\mathbb{C}$, et $|G(0)|$ est le produit des modules de ses racines : l'une d'elles, z, vérifie $|z| \leqslant 1$. Mais z est racine de P, donc $3 = |z^n + z| \leqslant |z|^n + |z| \leqslant 2$: c'est absurde.

$$\boxed{X^n + X + 3 \text{ est irréductible sur } \mathbb{Q} \text{ pour tout } n \geqslant 2.}$$

Groupes de Galois. Pour $n = 2$, le groupe est $\mathbb{Z}/2\mathbb{Z}$. Pour $n = 3$, le discriminant $-4 \cdot 1^3 - 27 \cdot 3^2 = -247$ n'est pas un carré : le groupe, transitif et non contenu dans $\mathfrak{A}_3$, est $\mathfrak{S}_3$. Pour $n = 4$, avec les notations de l'exercice 50, la résolvante cubique $X^3 - 12X - 1$ n'a pas de racine rationnelle, donc est irréductible ; ses racines appartenant au corps de décomposition d'après l'exercice 41, le degré 3 divise $|G|$. Le discriminant $-27 + 256 \cdot 27 = 6\,885$ n'est pas un carré, donc $G \not\subseteq \mathfrak{A}_4$. Parmi les sous-groupes transitifs de $\mathfrak{S}_4$, seul $\mathfrak{S}_4$ a un ordre multiple de 3 sans être contenu dans $\mathfrak{A}_4$.

$$\boxed{\mathbb{Z}/2\mathbb{Z} \qquad \mathfrak{S}_3 \qquad \mathfrak{S}_4 \qquad (n = 2,\ 3,\ 4)}$$