# Exercices de théorie de Galois

***Exercice 1***. — *Montrer que si $a$ et $b$ sont deux éléments non nuls d'un corps $K$ de caractéristique différente de 2, $K(\sqrt{a})$ est égal à $K(\sqrt{b})$ si et seulement si $b/a$ est un carré dans $K$.*

***Exercice 2***. — *Soit $K = \mathbb{Q}(i + \sqrt{2})$. Montrer que $K$ est galoisien sur $\mathbb{Q}$. Calculer le degré de $K$ sur $\mathbb{Q}$ et le groupe de Galois de $K/\mathbb{Q}$. Donner la liste des sous-corps de $K$.*

***Exercice 3***. — *Soit $L = \mathbb{Q}(\sqrt{5})$ et $M = \mathbb{Q}(\sqrt{2+\sqrt{5}})$. Déterminer les degrés des extensions $L/\mathbb{Q}$, $M/\mathbb{Q}$ et $M/L$. Indiquer lesquelles de ces extensions sont galoisiennes. Déterminer les polynômes minimaux de $\sqrt{2+\sqrt{5}}$ sur $\mathbb{Q}$ et sur $L$.*

***Exercice 4***. — *Soit $a$ et $b$ deux rationnels, donnez une condition suffisante pour que le polynôme $X^4 + aX^2 + b$ soit irréductible sur $\mathbb{Q}$. Donnez une CNS pour qu'alors son corps de rupture soit galoisien sur $\mathbb{Q}$. En particulier que se passe-t-il si on suppose que $a^2 - 4b$ est positif mais pas un carré rationnel, et $b$ négatif.*

***Exercice 5***. — *Soit $K = \mathbb{Q}(\sqrt[3]{2})$, $L$ la clôture galoisienne de $K$ sur $\mathbb{Q}$. Calculer le degré de $L$ sur $\mathbb{Q}$, le groupe de Galois de $L/K$. Donner la liste des sous-corps de $L$.*

***Exercice 6***. — *Soit $G$ le groupe de Galois de $X^5 - 2$. Quel est le cardinal de $G$ ? Est-il abélien, résoluble ?*

***Exercice 7***. — *Quel est le degré du corps de décomposition du polynôme $(X^3 - 5)(X^3 - 7)$ sur $\mathbb{Q}$ ?*

***Exercice 8***. — *Déterminez le groupe de Galois de $X^6 - 5$ sur $\mathbb{Q}$, $\mathbb{R}$.*

***Exercice 9***. — *Trouvez un élément primitif de $\mathbb{Q}[\sqrt{3}, \sqrt{7}]$.*

***Exercice 10***. — *Soit $G$ le groupe de Galois de $(X^3 - 5)(X^4 - 2)$ sur $\mathbb{Q}$.*
*1) Donner un ensemble de générateurs de $G$ ainsi que l'ensemble de relations entre eux.*
*2) $G$ est-il un groupe cyclique, diédral, symétrique ?*

***Exercice 11***. — *Trouvez un élément primitif du corps de décomposition de $(X^2 - 2)(X^2 - 5)(X^2 - 7)$.*

***Exercice 12***. — *Soit $\zeta$ un racine primitive 12-ième de l'unité. Combien y a-t-il d'extension comprises entre $\mathbb{Q}[\zeta^3]$ et $\mathbb{Q}[\zeta]$.*

***Exercice 13***. — *Soit $\zeta$ une racine primitive 5-ième de l'unité.*
*(1) Décrivez le groupe de Galois de $K = \mathbb{Q}[\zeta]/\mathbb{Q}$ et montrez que $K$ contient un unique sous-corps de degré 2 sur $\mathbb{Q}$ à savoir $\mathbb{Q}[\zeta + \zeta^4]$.*
*(2) Donnez le polynôme minimal de $\zeta + \zeta^4$ sur $\mathbb{Q}$.*
*(3) Donnez le groupe de Galois de $(X^2 - 5)(X^5 - 1)$.*
*(4) Donnez le groupe de Galois de $(X^2 + 3)(X^5 - 1)$.*

***Exercice 14***. — *Notons $K$ le corps $\mathbb{Q}(\sqrt{-15})$, $f$ son automorphisme non trivial, et $\alpha$ un élément de $K$ tel que le polynôme $X^3-\alpha$ soit irréductible sur $K$. Pourquoi existe-t-il de tels $\alpha$ ? On note $L$ le corps de décomposition de ce polynôme, et $\{\theta, j\theta, j^2\theta\}$ ses différentes racines dans $L$.*

*1) Pourquoi sont-elles de cette forme ?*

*2) Montrer que $L$ est une extension galoisienne de $K$ de degré 6, et que $L$ contient $\sqrt{5}$.*

*3) Montrer qu'il existe deux $K-$automorphismes $\sigma$ et $\tau$ de $L$ tels que*

$$\sigma(\sqrt{5})=\sqrt{5}, \quad \sigma(\theta)=j\theta, \quad \tau(\sqrt{5})=-\sqrt{5}, \quad \tau(\theta)=\theta.$$

*4) Déterminer l'ordre des éléments $\sigma$ et $\tau$ du groupe $Gal(L/K)$ et calculer $\tau\sigma\tau^{-1}$. Etablir la liste des extensions de $K$ contenues dans $L$.*

*5) On suppose désormais que $N_{K/\mathbb{Q}}(\alpha)$ est le cube d'un nombre rationnel $b$ (on admettra que c'est possible). Déterminer les différents conjugués de $\theta$ sur $\mathbb{Q}$. Montrer que l'extension $L/\mathbb{Q}$ est galoisienne de degré 12. Prouver qu'il est possible de prolonger l'automorphisme $f$ de $K$ en un automorphisme $\phi$ de $L$ tel que $\phi(\sqrt{5})=\sqrt{5}$ et $\phi(\theta)=b/\theta$. Calculer $\phi^2$, $\phi\sigma\phi^{-1}$ et $\phi\tau\phi^{-1}$. Montrer que $\mathbb{Q}(\sqrt{5})$ admet une extension de degré 3 contenue dans $L$ et galoisienne sur $\mathbb{Q}$.*

***Exercice 15***. — *On note $L$ le corps de décomposition dans $\mathbb{C}$ du polynôme $P=T^4-3T-3$.*

*a) Montrer que le polynôme $P$ est irréductible sur $\mathbb{Q}$, et qu'il admet dans $\mathbb{C}$ deux racines réelles $x$ et $y$, et un couple $(z,\overline{z})$ de racines complexes conjuguées l'une de l'autre.*

*b) Notons $T^2+aT+b$ et $T^2-aT+b'$ les polynômes unitaires de degré 2 qui divisent $P$ dans $\mathbb{R}[X]$. Montrer que $a$ est une racine du polynôme $X^6+12X^2-9$, et calculer le degré de $a^2$ sur $\mathbb{Q}$.*

*c) Montrer que $[L:\mathbb{Q}]$ est un multiple de 12.*

*d) Montrer que le groupe alterné $\mathcal{A}_4$ est le seul sous-groupe d'indice 2 du groupe symétrique $\mathcal{S}_4$.*

*e) Montrer qu'il existe un automorphisme de $L$ qui échange $z$ et $\overline{z}$ et qui laisse $x$ fixe. Déterminer le groupe de Galois de $L/\mathbb{Q}$. Combien $L$ a-t'il de sous-corps ?*

***Exercice 16***. — *Montrez en réduisant modulo 2 et 3, que le groupe de Galois de $X^5-X-1$ est $\mathcal{S}_5$.*

**1** Il est clair que, si $b/a = x^2$ est un carré dans $K$, on a $\sqrt{b} = \pm x\sqrt{a}$ et $K(\sqrt{a}) = K(\sqrt{b})$. Réciproquement, si ces deux corps sont égaux et différents de $K$, on peut écrire par exemple $\sqrt{b} = x + y\sqrt{a}$ avec $x$ et $y$ dans $K$. On en déduit $(b - x^2 - ay^2)^2 = 4x^2y^2a$. Comme $a$ n'est pas un carré dans $K$, cela implique $2xy = 0$ et $b = x^2 + ay^2$. Comme $b$ n'est pas un carré et la caractéristique n'est pas 2, $2y \neq 0$. On en déduit que $x = 0$ et $b/a = y^2$ est un carré dans $K$. Reste le cas $K(\sqrt{a}) = K(\sqrt{b}) = K$ pour lequel $b$ et $a$ sont des carrés, et leur quotient aussi.

**2** Comme $-1/2$ n'est pas un carré dans $\mathbb{Q}$, l'exercice précédent montre que $\mathbb{Q}(i)$ et $\mathbb{Q}(\sqrt{2})$ sont deux extensions quadratiques distinctes de $\mathbb{Q}$. Le composé $L = \mathbb{Q}(i, \sqrt{2})$ est donc une extension galoisienne de degré 4 de $\mathbb{Q}$. On peut décrire l'action du groupe de Galois $\mathrm{Gal}(L/\mathbb{Q}) = \{Id, \tau_1, \tau_2, \tau_3\}$ sur $i$ et $\sqrt{2}$ :

$$\tau_1(i) = -i,\ \tau_1(\sqrt{2}) = \sqrt{2},\ \tau_2(i) = i,\ \tau_2(\sqrt{2}) = -\sqrt{2},\ \tau_3(i) = -i,\ \tau_3(\sqrt{2}) = -\sqrt{2}.$$

Seul $Id$ laisse fixe l'élément $\alpha = i + \sqrt{2}$ de $L$. On en déduit que le corps engendré par $\alpha$ est $L$ tout entier, c'est-à-dire $L = K$.

**3** Comme 5 n'est pas un carré dans $\mathbb{Q}$, $L/\mathbb{Q}$ est une extension quadratique. Montrons que $2 + \sqrt{5}$ n'est pas un carré dans $L$ : en effet, si $(x + y\sqrt{5})^2 = 2 + \sqrt{5}$, son conjugué vérifie $(x - y\sqrt{5})^2 = 2 - \sqrt{5}$ et en faisant le produit, on obtient

$$(x^2 - 5y^2)^2 = 4 - 5 = -1$$

mais $-1$ n'est pas un carré dans $\mathbb{Q}$, une contradiction. L'extension $M/L$ est donc quadratique, et $[M : \mathbb{Q}] = [M : L][L : \mathbb{Q}] = 4$.. Le générateur $\alpha = \sqrt{2 + \sqrt{5}}$ de $M$ sur $\mathbb{Q}$ vérifie $(\alpha^2 - 2)^2 = 5$, son polynôme minimal sur $\mathbb{Q}$ est donc $(X^2 - 2)^2 - 5 = X^4 - 4X^2 - 1$. Les deux racines imaginaires de ce polynôme ne peuvent appartenir à $M$ qui est inclus dans $\mathbb{R}$. On en déduit que l'extension $M/\mathbb{Q}$ n'est pas galoisienne. D'autre part, une extension quadratique est toujours galoisienne, c'est donc le cas de $M/L$ et $L/\mathbb{Q}$. Le polynôme minimal de $\alpha$ sur $L$ est simplement $X^2 - 2 - \sqrt{5}$.

**4** (i) Le discriminant $\Delta = a^2 - 4b$ ne doit pas être un carré, sinon le polynôme serait réductible. Le corps quadratique $\mathbb{Q}(\sqrt{\Delta})$ contient alors $(-a + \sqrt{\Delta})/2$ et $(-a - \sqrt{\Delta})/2$, dont les racines carrées sont les racines de $X^4 + aX^2 + b$. Ces racines engendrent des extensions quadratiques de $\mathbb{Q}(\sqrt{\Delta})$ qui coïncident si et seulement si le quotient

$$\frac{-a - \sqrt{\Delta}}{-a + \sqrt{\Delta}} = \frac{a^2 - \Delta}{(-a + \sqrt{\Delta})^2} = b\left(\frac{2}{-a + \sqrt{\Delta}}\right)^2$$

est un carré dans $\mathbb{Q}(\sqrt{\Delta})$, ce qui équivaut à dire que $b$ lui-même est un carré dans $\mathbb{Q}(\sqrt{\Delta})$. L'équation $b = (x + y\sqrt{\Delta})^2$ implique que $x$ ou $y$ est nul, et $b$ est un carré ou $\Delta$ fois un carré dans $\mathbb{Q}$.

Ainsi $X^4 + aX^2 + b$ est réductible si et seulement si $(-a + \sqrt{\Delta})/2$ est un carré dans $\mathbb{Q}(\sqrt{\Delta})$. Dans le cas contraire le corps de rupture associé est galoisien si et seulement si $b$ eou $\Delta b$ est un carré dans $\mathbb{Q}$.

(ii) Ainsi si $\delta$ est positif sans être un carré dans $\mathbb{Q}$ et si $b$ est négatif alors ni $b$ ni $\Delta b$ ne sont des carrés dans $\mathbb{Q}$ de sorte que $X^4 + aX^2 + b$ est irréductible mais son corps de rupture n'est pas galoisien.

(iii) Par exemple, pour $b = 1$ et $a = -1$ : le polynôme $X^4 - X^2 + 1$ est irréductible et son corps de rupture est galoisien sur $\mathbb{Q}$.

**5** Le corps $L$ est le corps de décomposition de $X^3-2$. Comme $X^3-2$ est irréductible, $K$ est de degré 3. Les autres racines ne sont pas réelles : le polynôme $X^2+\sqrt[3]{2}X+\sqrt[3]{4}$ est donc irréductible sur $K$ et ses racines engendrent une extension quadratique $L=K(j)$ de $K$, et $[L:\mathbb{Q}]=6$. Le groupe de Galois est un sous-groupe du groupe des permutations des trois racines : c'est $\mathcal{S}_3$ tout entier. Ce groupe a 6 sous-groupes : les deux sous-groupes triviaux, correspondant aux corps $\mathbb{Q}$ et $L$, les trois sous-groupes d'ordre 2 correspondant aux trois corps cubiques $K=\mathbb{Q}(\sqrt[3]{2})$, $K'=\mathbb{Q}(\rho\sqrt[3]{2})$ et $K''=\mathbb{Q}(\rho^2\sqrt[3]{2})$, enfin le groupe alterné, d'ordre 3, correspond au corps quadratique $\mathbb{Q}(\rho)=\mathbb{Q}(\sqrt{-3})$.

**6** On note $\zeta=e^{\frac{2i\pi}{5}}$ et $\alpha=\sqrt[5]{2}$ dont les polynômes minimaux sont respectivement $\Phi_5(X)=X^4+X^3+X^2+X+1$ et $X^5-2$. Le corps de décomposition de $X^5-2$ est $L=\mathbb{Q}[\zeta,\alpha]$ qui contient entr'autre les corps $\mathbb{Q}[\zeta]$ et $\mathbb{Q}[\alpha]$ qui sont respectivement de degré 4 et 5 sur $\mathbb{Q}$. On en déduit alors que $[L:\mathbb{Q}]$ est divisible par 5 et 4 et donc par 20. Par ailleurs $\zeta$ est au plus de degré 4 sur $\mathbb{Q}[\alpha]$ de sorte que $[L:\mathbb{Q}]\leq 20$. Ainsi d'après le théorème de Galois, $G$ est de cardinal 20.

Pour tout $\sigma\in G$, on a $\sigma(\alpha)\in\{\alpha,\zeta\alpha,\zeta^2\alpha,\zeta^3\alpha,\zeta^4\alpha\}$ et $\sigma(\zeta)\in\{\zeta,\zeta^2,\zeta^3,\zeta^4\}$. Comme $G$ est de cardinal 20, alors pour tout $0\leq k\leq 4$ et $1\leq l\leq 4$, il existe $\sigma\in G$ tel que $\sigma(\alpha)=\alpha\zeta^k$, $\sigma(\zeta)=\zeta^l$.

Soit alors $\sigma$ (resp. $\tau$) tel que $\sigma(\alpha)=\alpha\zeta$ (resp. $\tau(\alpha)=\alpha$) et $\sigma(\zeta)=\zeta$ (resp. $\tau(\zeta)=\zeta^2$) de sorte que $\sigma$ est d'ordre 5 (resp. d'ordre 4) et que tout élément de $G$ s'écrit de manière unique sous la forme $\sigma^k\tau^l$ avec $0\leq k\leq 4$ et $0\leq l\leq 3$.

Clairement $G$ n'est pas abélien car $\mathbb{Q}[\alpha]/\mathbb{Q}$ n'est pas galoisien. Par contre il est résoluble car tout groupe de cardinal 20 l'est (le plus petit groupe non résoluble est $\mathcal{A}_5$).
*Remarque :* En fait $G\simeq\mathbb{Z}/5\mathbb{Z}\ltimes_\psi\mathbb{Z}/4\mathbb{Z}$ où $\psi:\mathbb{Z}/4\mathbb{Z}\to(\mathbb{Z}/5\mathbb{Z})^\times$ avec $\psi(1)$ est la multiplication par 2. On peut déterminer tous les sous-groupes de $G$ et donc toutes les sous-extensions de $L$, on obtient alors

| sous-groupe | corps intermédiaires | degré sur $\mathbb{Q}$ |
|---|---|---|
| $\{1\}$ | $\mathbb{Q}[\zeta,\alpha]$ | 20 |
| $\{1,\tau^2\}$ | $\mathbb{Q}[\alpha,\zeta^2+\zeta^3]$ | 10 |
| $\{1,\sigma\tau^2\sigma^{-1}\}$ | $\mathbb{Q}[\zeta\alpha,\zeta^2+\zeta^3]$ | 10 |
| $\{1,\sigma^2\tau^2\sigma^{-2}\}$ | $\mathbb{Q}[\zeta^2\alpha,\zeta^2+\zeta^3]$ | 10 |
| $\{1,\sigma^3\tau^2\sigma^{-3}\}$ | $\mathbb{Q}[\zeta^3\alpha,\zeta^2+\zeta^3]$ | 10 |
| $\{1,\sigma^4\tau^2\sigma^{-4}\}$ | $\mathbb{Q}[\zeta^4\alpha,\zeta^2+\zeta^3]$ | 10 |
| $<\tau>$ | $\mathbb{Q}[\alpha]$ | 5 |
| $<\sigma\tau\sigma^{-1}>$ | $\mathbb{Q}[\zeta\alpha]$ | 5 |
| $<\sigma^2\tau\sigma^{-2}>$ | $\mathbb{Q}[\zeta^2\alpha]$ | 5 |
| $<\sigma^3\tau\sigma^{-3}>$ | $\mathbb{Q}[\zeta^3\alpha]$ | 5 |
| $<\sigma^4\tau\sigma^{-4}>$ | $\mathbb{Q}[\zeta^4\alpha]$ | 5 |
| $<\sigma>$ | $\mathbb{Q}[\zeta]$ | 4 |
| $<\sigma,\tau^2>$ | $\mathbb{Q}[\zeta^2+\zeta^3]$ | 2 |
| $G$ | $\mathbb{Q}$ | 1 |

**7** Si $E_1$ et $E_2$ sont deux extensions galoisiennes de $F$ alors $E_1E_2$ et $E_1\cap E_2$ sont galoisiennes sur $F$ et on a la suite exacte suivante

$$\mathrm{Gal}(E_1E_2/F)\hookrightarrow\mathrm{Gal}(E_1/F)\times\mathrm{Gal}(E_2/F)\twoheadrightarrow\mathrm{Gal}(E_1\cap E_2/F)$$

où la dernière flèche n'est un morphisme que si $\mathrm{Gal}(E_1 \cap E_2/F)$ est abélien et où l'image de la première est exactement les éléments du groupe produit qui s'envoie sur l'élément neutre de $\mathrm{Gal}(E_1 \cap E_2/F)$. Ici on a $E_1 \cap E_2 = \mathbb{Q}[j]$ où $j$ est une racine cubique primitive de l'unité de sorte que le degré cherché est 18. On vérifie alors que $\mathrm{Gal}(E_1E_2/F)$ s'identifie aux éléments $\mathrm{d}(\sigma_1, \sigma_2) \in \mathfrak{S}_3 \times \mathfrak{S}_3$ tels que $\epsilon(\sigma_1) = \epsilon(\sigma_2)$ où $\epsilon$ désigne la signature.

**8** Soit $L$ le corps de décomposition de $X^6 - 5$ : $L = \mathbb{Q}[\zeta, \alpha]$ avec $\alpha^6 = 5$, $\alpha \in \mathbb{R}$ et $\zeta$ est une racine primitive 3-ième de l'unité de sorte que $-\zeta$ est une racine primitive 6-ième de l'unité. Le degré $[L : \mathbb{Q}]$ est donc égal à 12 et $G \simeq D_6$ engendré par (26)(35) et (123456). Sur $\mathbb{R}$ le groupe de galois est $\mathbb{Z}/2\mathbb{Z}$.

**9** Comme 3/7 n'est pas un carré dans $\mathbb{Q}$, on en déduit $\mathbb{Q}[\sqrt{3}] \cap \mathbb{Q}[\sqrt{7}] = \mathbb{Q}$ et donc que $[\mathbb{Q}[\sqrt{3}, \sqrt{7}] : \mathbb{Q}] = 4$ avec pour base $1, \sqrt{3}, \sqrt{7}, \sqrt{21}$. Le groupe de Galois est isomorphe à $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ avec $(i, j)(\sqrt{3}) = (-1)^i\sqrt{3}$ et $(i, j)(\sqrt{7}) = (-1)^j\sqrt{7}$. En particulier on remarque que $x = \sqrt{3} + \sqrt{7}$ possède 4 conjugués distincts deux à deux (utilisez que la famille $\sqrt{3}$ et $\sqrt{7}$ est libre sur $\mathbb{Q}$). On peut par ailleurs trouver son polynôme minimal en procédant selon le principe général suivant : soit $A$ et $B$ deux polynômes irréductibles unitaires sur $\mathbb{Q}$. Le système en d'équations $A(X) = B(Y - X) = 0$ possède comme solutions les couples $(x_a, x_b + x_a)$ où $x_a$ (resp. $x_b$) décrit les solutions de $A(X) = 0$ (resp. $B(X) = 0$). On considère alors les polynômes $A(X)$ et $B(Y - X)$ comme des polynômes à valeurs dans $K[Y]$ et on introduit leur résultant qui est un polynôme en $Y$ dont les zéros sont d'après ce qui précède, exactement les sommes des zéros de $A$ avec ceux de $B$.

Dans notre cas on a $A(X) = X^2 - 3$ et $B(X) = X^2 - 7$. Le résultant en question est donné par le déterminant

$$\begin{vmatrix} 1 & 0 & -3 & 0 \\ 0 & 1 & 0 & -3 \\ 1 & -2Y & Y^2 - 7 & 0 \\ 0 & 1 & -2Y & Y^2 - 7 \end{vmatrix}$$

soit après calcul $Y^4 - 20y^2 + 16$

**10** Le corps de décomposition de $X^4 - 2$ est $E_1 = \mathbb{Q}[i, \alpha]$ avec $\alpha^4 = 2$ qui est de degré 8 sur $\mathbb{Q}$ et de groupe de Galois $D_4$. Le corps de décomposition de $X^3 - 5$ est $E_2 = \mathbb{Q}[j, \beta]$ qui est de degré 6 et de groupe de Galois $\mathfrak{S}_3$ sur $\mathbb{Q}$. Comme les extensions $E_i/\mathbb{Q}$ sont galoisiennes le degré de $[E_1E_2 : \mathbb{Q}] = [E_1 : \mathbb{Q}].[E_2 : \mathbb{Q}]/[E_1 \cap E_2 : \mathbb{Q}]$ et on est donc ramené à étudier $E_1 \cap E_2$ qui est donc de degré sur $\mathbb{Q}$ un diviseur de 6 et 8 et donc égal à 1 ou 2. Il faut donc étudier les extensions de degré 2 contenues dans $E_1$ et $E_2$ ce qui revient à étudier les sous-groupes d'indice 2 dans les groupes de Galois respectifs. En ce qui concerne $E_2$, le seul sous-groupe d'indice 2 de $\mathfrak{S}_3$ est $\mathcal{A}_3$ (utilisez que la signature est le seul morphisme non trivial de $\mathfrak{S}_3 \twoheadrightarrow \mathbb{Z}/2\mathbb{Z}$) et donc $\mathbb{Q}[j]$ est la seule extension quadratique contenue dans $E_2$. En ce qui concerne $E_1$, les sous-groupes $H$ d'indice 2 de $D_4$ sont soit $D_4^+ \simeq \mathbb{Z}/4\mathbb{Z}$ correspondant aux rotations ; sinon $H \cap D_4^+$ ne peut pas être réduit à l'identité c'est donc le sous-groupe d'indice 2 de $D_4^+$ égal à $\pm\mathrm{Id}$ et $H$ est alors égal à $\{\pm\mathrm{Id}, \sigma_D, \sigma_{D^\perp}\} \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ où $\sigma_D$ est la réflexion par rapport à la droite $D$ (diagonale ou médiatrice du carré). Les corps correspondant sont alors $\mathbb{Q}[i]$, $\mathbb{Q}[\sqrt{2}]$ et $\mathbb{Q}[i\sqrt{2}]$. Comme $2/-3$, $2/3$ et $-1/-3$ ne sont pas dans $(\mathbb{Q}^\times)^2$, les extensions précédentes sont distinctes deux à deux et $E_1 \cap E_2 = \mathbb{Q}$. Ainsi le groupe de Galois est le groupe produit $D_4 \times D_3$.

**11** Comme 2/5 n'est pas un carré de $\mathbb{Q}$, $\mathbb{Q}[\sqrt{2}, \sqrt{5}]/\mathbb{Q}$ est de degré 4 de groupe de Galois $\mathbb{Z}/2\mathbb{Z}/2$ : les extensions quadratiques contenue dans $\mathbb{Q}[\sqrt{2}, \sqrt{5}]$ sont $\mathbb{Q}[\sqrt{2}]$, $\mathbb{Q}[\sqrt{5}]$ et $\mathbb{Q}[\sqrt{10}]$

correspondant aux trois sous-groupes d'indices 2 de $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. Celles-ci sont toutes distinctes de $\mathbb{Q}[\sqrt{7}]$ de sorte que le groupe de Galois est $(\mathbb{Z}/2\mathbb{Z})^3$ donné par $\sigma_{\epsilon_1,\epsilon_2,\epsilon_3}(\alpha_i) = \epsilon_i \alpha_i$ où $\epsilon_i = \pm 1$ et $\alpha_1 = \sqrt{2}$, $\alpha_2 = \sqrt{5}$ et $\alpha_3 = \sqrt{7}$. On remarque ainsi que les images de $x = \sqrt{2}+\sqrt{5}+\sqrt{7}$ par les éléments du groupe de Galois sont toutes distinctes, ce qui prouve que $x$ est générateur.

**12** On a $\mathbb{Q}[\zeta] = \mathbb{Q}[\zeta', i]$ où $\zeta'$ est une racine primitive 3-ième de l'unité et $\pm i = \zeta^3$ ...

**13** (1) Le groupe de galois est $(\mathbb{Z}/5\mathbb{Z})^\times$, cyclique de cardinal 4 engendré par $\sigma_0 := 2$ ; il possède donc un unique sous-groupe $H$ d'indice 2 à savoir le groupe engendré par $2^2$. Le sous-corps correspondant est donc engendré par $\sum_{\sigma \in H} \sigma(\zeta) = \zeta + \zeta^4$.

(2) On a $\sigma_0(\zeta + \zeta^4) = \zeta^2 + \zeta^3$ et

$$(\zeta + \zeta^4)(\zeta^2 + \zeta^3) = -1 \qquad (\zeta + \zeta^4) + (\zeta^2 + \zeta^3) = -1$$

de sorte que le polynôme minimal de $\zeta + \zeta^4$ est $X^2 + X - 1$. Par ailleurs les racines de ce polynôme sont $\frac{-1 \pm \sqrt{5}}{2}$ de sorte que $\mathbb{Q}[\zeta + \zeta^4] = \mathbb{Q}[\sqrt{5}]$.

(3) On a d'après (2), $\mathbb{Q}[\sqrt{5}, \zeta] = \mathbb{Q}[\zeta]$.

(4) On a $\mathbb{Q}[\sqrt{5}] \cap \mathbb{Q}[i\sqrt{3}] = \mathbb{Q}$ de sorte que d'après (1), on a $\mathbb{Q}[\zeta] \cap \mathbb{Q}[i\sqrt{3}] = \mathbb{Q}$ de sorte que le groupe de Galois est le produit direct de ceux de $X^2 + 3$ et $X^5 - 1$, soit $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$.

**14** (1) Un polynôme de degré 3 est irréductible si et seulement s'il n'a pas de racine. Il s'agit donc de montrer que tous les éléments de $\mathbb{Q}(\sqrt{-15})$ ne sont pas des cubes. Mais si $\alpha = x + y\sqrt{-15} = \theta^3$ avec $\theta \in \mathbb{Q}(\sqrt{-15}$, alors $f(\alpha) = f(\theta)^3$ et la quantité

$$x^2 + 15y^2 = N(\alpha) = \alpha f(\alpha) = N(\theta)^3$$

est le cube d'un rationnel. Il suffit de prendre par exemple $y = 0$ et $x$ non cube pour trouver un $\alpha$ qui convient. Si $\theta'$ est une autre racine, on a $(\theta'/\theta)^3 = 1$. Alors $\theta$ et $\theta'$ différent par une racine cubique de l'unité, $j$ ou $j^2$.

(2) Comme $L$ est défini comme corps de décomposition en caractéristique nulle, $L/K$ est forcément galoisienne, et son degré est un multiple de $3 = [K(\theta)/K]$ et de $[K(j) : K] = 2$ car $j \notin K$ : en effet si $K = \mathbb{Q}(\sqrt{-15})$ et $\mathbb{Q}(j) = \mathbb{Q}(\sqrt{-3})$ sont deux extensions quadratiques distinctes de $\mathbb{Q}$ car $\frac{-15}{-3} = 5$ n'est pas un carré dans $\mathbb{Q}$. Donc $j$ est quadratique sur $K$, donc pas dans $K(\theta)$, donc quadratique sur $K(\theta)$, et $L = K(\theta)(\rho)$ est de degré 6 sur $K$. Au passage, on a vu que $L$ contenait $\frac{\sqrt{-15}}{\sqrt{-3}} = \sqrt{5}$.

(3) Le groupe de Galois du corps de décomposition est un sous-groupe du groupe des permutations des racines du polynôme. Ici le groupe est d'ordre 6, et il y a trois racines : $\mathrm{Gal}(L/K)$ s'identifie au groupe des permutations de $\{\theta, j\theta, j^2\theta\}$. Il existe en particulier $\sigma$ qui envoie $\theta$ sur $j\theta$ et $j\theta$ sur $j^2\theta$. On en déduit $\sigma(j) = \sigma(\frac{j\theta}{\theta}) = \frac{j^2\theta}{j\theta} = j$, donc aussi $\sigma(\sqrt{-3}) = \sigma(1 + 2j) = 1 + 2\sigma(j) = \sqrt{-3}$. Comme on a par définition $\sigma(\sqrt{-15}) = \sqrt{-15}$, on en déduit $\sigma(\sqrt{5}) = \frac{\sigma(\sqrt{-15})}{\sigma(\sqrt{-3})} = \sqrt{5}$. De même, la permutation $\tau$ qui échange $j\theta$ et $j^2\theta$ en laissant fixe $\theta$ vérifie $\tau(j) = \frac{\tau(j\theta)}{\tau(\theta)} = j^{-1} = j^2$, donc $\tau(\sqrt{-3}) = -\sqrt{-3}$ et $\tau(\sqrt{5}) = \frac{\tau(\sqrt{-15})}{\tau(\sqrt{-3})} = -\sqrt{5}$.

(4) La permutation $\sigma$ est circulaire, elle est d'ordre 3. De même, $\tau$ est une transposition, d'ordre 2. On voit que $\tau\sigma\tau^{-1}$ permute les trois racines circulairement, dans l'autre sens : $\tau\sigma\tau^{-1} = \sigma^{-1} = \sigma^2$. On peut écrire

$$\mathrm{Gal}(L/K) = \{Id, \sigma, \sigma^2, \tau, \sigma\tau, \sigma^2\tau\}.$$

Ce groupe a 4 sous-groupes non triviaux, $\{Id, \sigma, \sigma^2\}$ est d'ordre 3 et a pour corps fixe $K(\sqrt{5})$, et les trois groupes d'ordre 2 $\{Id, \tau\}$, $\{Id, \sigma\tau\}$ et $\{Id, \sigma^2\tau\}$ ont pour corps fixes respectifs $K(\theta)$, $K(\rho^2\theta)$ et $K(\rho\theta)$, ce qui complète, avec $K$ et $L$, la liste des corps intermédiaires entre $K$ et $L$.

(5) On a $t = \alpha + f(\alpha) \in \mathbb{Q}$ et $N_{K/\mathbb{Q}}(\alpha) = \alpha\overline{\alpha} = b^3 \in \mathbb{Q}$. On en déduit que $\theta$ est racine du polynôme à coefficients rationnels

$$P(X) = (X^3 - \alpha)(X^3 - f(\alpha)) = X^6 - tX^3 + b^3.$$

Sur $K$, ce polynôme se décompose en deux facteurs dont on sait qu'ils sont irréductibles ($b^3/\alpha$ n'est pas plus un cube que $\alpha$ dans $K$). Toute factorisation de $P$ sur $\mathbb{Q}$ serait encore valable sur $K$, or les facteurs ont des coefficients qui ne sont pas dans $\mathbb{Q}$ (en effet, si $\alpha$ appartenait à $\mathbb{Q}$, $\alpha^2$ serait un cube et donc $\alpha$ aussi (dans le groupe $\mathbb{Q}^\times/(\mathbb{Q}^\times)^3$) tous les éléments non triviaux sont d'ordre 3), ce qui contredit le fait que $X^3 - \alpha$ est irréductible sur $K$) ; on en déduit que $P$ est irréductible sur $\mathbb{Q}$.

Les racines du polynôme $P$ sont

$$\{\theta, j\theta, j^2\theta, b/\theta, jb/\theta, j^2b/\theta\}$$

et appartiennent toutes à $L$. D'autre part, le corps de décomposition de $P$ sur $\mathbb{Q}$ contient $\theta$, donc $\alpha$, donc $K$, donc $L = K(\theta, j\theta)$. On vient de prouver que c'est $L$, qui est donc une extension galoisienne de degré 12 de $\mathbb{Q}$. $\mathrm{Gal}(L/K)$ est un sous-groupe (distingué) d'indice 2 de $\mathrm{Gal}(L/\mathbb{Q})$.

Soit $\psi$ un élément quelconque de $\mathrm{Gal}(L/\mathbb{Q})$ qui n'est pas dans $\mathrm{Gal}(L/K)$. Par construction, la restriction de $\psi$ à $K$ n'est pas l'identité, c'est donc $f$. On en déduit que $\psi$ échange les deux facteurs de $P$ sur $K$, et donc l'image $\gamma = \psi(b/\theta)$ de $b/\theta$ par $\psi$ est $\theta$, $j\theta$ ou $j^2\theta$. Choisissons un élément $\kappa$ de $\mathrm{Gal}(L/K)$ tel que $\kappa(\theta) = \gamma$. Si l'image de $\sqrt{5}$ par $\psi^{-1}\kappa$ est $\sqrt{5}$, $\phi = \psi^{-1}\kappa$ présente les propriétés requises. Sinon, $\phi = \tau\psi^{-1}\kappa$ convient.

On a $\phi^2(\theta) = \phi(b/\theta) = b/\phi(\theta) = \theta$. Donc $\phi^2$ est un élément de $\mathrm{Gal}(L/K)$ qui laisse fixe $\sqrt{5}$ et $\theta$ : c'est l'identité. On a encore $\phi(\sqrt{-15}) = f(\sqrt{-15}) = -\sqrt{-15}$, donc $\phi(\sqrt{-3}) = \frac{\phi(\sqrt{-15})}{\phi(\sqrt{5})} = -\sqrt{-3}$, d'où $\phi(j) = j^2$. On en déduit que

$$\phi\sigma\phi^{-1}(\theta) = \phi\sigma(\frac{b}{\theta}) = \phi(\frac{b}{j\theta}) = \frac{\theta}{j^2} = j\theta,$$

donc $\phi\sigma\phi^{-1}$ est un élément de $\mathrm{Gal}(L/K)$ qui envoie $\sqrt{5}$ sur $\sqrt{5}$ et $\theta$ sur $j\theta$, donc $\phi\sigma\phi^{-1} = \sigma$. De même, on montre que $\phi\tau\phi^{-1} = \tau$, et $\phi$ commute à tous les éléments de $\mathrm{Gal}(L/K)$, et à lui-même, donc $\phi$ est dans le centre de $\mathrm{Gal}(L/\mathbb{Q})$ : le sous-groupe $\{Id, \phi\}$ est distingué, et le corps fixe de $\phi$ est un sous-corps $M$ de $L$ galoisien sur $\mathbb{Q}$. Comme $[L : M] = 2$, $M$ est de degré 6 sur $\mathbb{Q}$. Comme $\phi(\sqrt{5}) = \sqrt{5}$, $R = \mathbb{Q}(\sqrt{5})$ est inclus dans $M$ qui est donc une extension de degré 3 de $R$.

**15** (a) Le critère d'Eisenstein s'applique à $P$ pour le nombre premier $p = 3$, donc $P$ est irréductible sur $\mathbb{Q}$. La dérivée $P'(t) = 4t^3 - 3$ s'annule exactement une fois sur $\mathbb{R}$, au point $\vartheta = \sqrt[3]{\frac{3}{4}}$. Comme $P(\vartheta) = -9\vartheta/4 - 3 < 0$, et $\lim_{t\to\pm\infty} P(t) = +\infty$, la fonction $P(t)$ s'annule exactement deux fois sur $\mathbb{R}$. Les deux autres racines de $P$ dans $\mathbb{C}$ sont conjuguées (au sens habituel...) l'une de l'autre.

(b) La décomposition de $P$ en éléments irréductibles de $\mathbb{R}[T]$, s'écrit

$$(T - x)(T - y)(T^2 + aT + b).$$

Le coefficient de $T^2$ est nul, donc $(T-x)(T-y) = T^2 - aT + b'$. L'identification donne

$$a^2 = b + b' \qquad a(b-b') = 3 \qquad bb' = -3$$

on tire $a^6 = a^2(b^2 + 2bb' + b'^2)$ de la première équation et $9 = a^2(b^2 - 2bb' + b'^2)$ de la seconde. On a donc $a^6 - 9 = a^2(4bb') = -12a^2$, d'où le résultat. Comme $a^2$ est racine d'un polynôme de degré 3, il est de degré au plus 3. Pour montrer que $a^2$ est de degré 3, on peut montrer que le polynôme $X^3 + 12X^2 - 9$ est irréductible sur $\mathbb{Q}$, ce qui résulte du fait qu'aucun des entiers $\pm 1$, $\pm 3$ ou $\pm 9$ qui divisent son coefficient constant n'en est une racine.

(c) Le degré de $L$ est un multiple de celui de chacun de ses éléments. Or $x$ est de degré 4 et $a^2$ est de degré 3, d'où le résultat.

(d) Les classes de conjugaison de $\mathcal{S}_n$ sont en bijection avec les partitions de l'entier $n$. Pour $n = 4$, la permutation identique forme la seule classe de conjugaison de cardinal 1, les permutations (12), (123), (1234) et (12)(34) sont des représentants des autres classes, de cardinal respectif 6, 8, 6 et 3. Un sous-groupe d'indice 2 est forcément distingué, et formé de certaines de ces classes. La seule somme qui donne 12 est 1 + 8 + 3, qui donne le groupe alterné $\mathcal{A}_4$.

(e) Comme $L$ est une extension normale de $\mathbb{Q}$, il est laissé stable par tout automorphisme de $\mathbb{C}$, en particulier la conjugaison complexe, qui laisse $x$ et $y$ et échange $z$ et $\overline{z}$. Cette permutation est une transposition, c'est-à-dire que considéré comme sous-groupe du groupe des permutations des racines de $P$, le groupe de Galois de $L/\mathbb{Q}$ n'est pas inclus dans $\mathcal{A}_4$ ; Or, on a vu au c), que son cardinal $[L : \mathbb{Q}]$ vaut 12 ou 24. la question précédente permet donc de conclure $\mathrm{Gal}(L/\mathbb{Q}) = \mathcal{S}_4$. Reste à compter le nombre de sous-groupes de $\mathcal{S}_4$. Il y en a 1 d'ordre 24, un d'ordre 12, 3 d'ordre 8 (les 2-Sylow sont conjugués entre eux). Il y a 4 sous-groupes d'ordre 6, conjugués à $\mathcal{S}_3$. Les groupes d'ordre ' sont de 3 sortes : les cycliques, au nombre de 3, les conjugués de $\{Id, (12), (34), (12)(34)\}$, au nombre de 3, et le groupe de Klein $\{Id, (12)(34), (13)(24), (14)(23)$. Enfin, il y a 4 groupes d'ordre 3, 9 groupes d'ordre 2 et 1 groupe d'ordre 1, soit un total de 1 + 1 + 3 + 4 + (3 + 3 + 1) + 4 + 9 + 1 = 30 sous-corps.

**16** $X^5 - X - 1$ n'a pas de racines dans $\mathbb{F}_2$ mais il en a dans $\mathbb{F}_4$ comme on peut par exemple le voir calculant le pgcd de $X^5 - X - 1$ avec $X^4 - X$. Ainsi $X^5 - X - 1$ se factorise en un produit de deux facteurs irréductibles de degré 2 et 3. On en déduit alors que $G$ contient une permutation de type (12)(345) et donc en passant au cube, une transposition.

Modulo 3, $X^5 - X - 1$ reste irréductible, de sorte que $G$ contient un 5-cycle.

Par ailleurs comme 5 est premier quitte à prendre une puissance du 5-cycle trouvé, on peut supposer le 5-cycle et la transposition respectivement égale à (12) et (12345). On conclut en remarquant que $\mathcal{S}_n$ est engendré par (12) et $(12\cdots n)$.