

1. Pour chacune des extensions algébriques finies suivantes, déterminer si elle est séparable ou non, normale ou non, galoisienne ou non. Lorsque l'extension est galoisienne, donner son groupe de Galois. (1) $\mathbb{R} \subseteq \mathbb{C}$, (2) $\mathbb{Q} \subseteq \mathbb{Q}(\sqrt{2})$, (3) $\mathbb{Q} \subseteq \mathbb{Q}(\sqrt[3]{2})$, (4) $\mathbb{Q}(j) \subseteq \mathbb{Q}(\sqrt[3]{2}, j)$ (où j est une racine primitive cubique de l'unité), (5) $\mathbb{Q} \subseteq \mathbb{Q}(j)$, (6) $\mathbb{Q} \subseteq \mathbb{Q}(\sqrt[3]{2}, j)$, (7) $\mathbb{F}_p \subseteq \mathbb{F}_{p^d}$ (p étant un nombre premier, et d un naturel non nul), (8) $\mathbb{C}(t) \subseteq \mathbb{C}(t^{1/\ell})$ où ℓ est un nombre premier quelconque, (9) $\mathbb{F}_p(t) \subseteq \mathbb{F}_p(t^{1/p})$, (10) $\mathbb{F}_p(t) \subseteq \mathbb{F}_p(t^{1/\ell})$ où ℓ est un nombre premier strictement supérieur à p .

Corrigé. Tout d'abord, n'importe quelle extension algébrique finie $K \subseteq L$ en caractéristique zéro, ou bien dont le corps K est parfait, est séparable. Les extensions (1) à (8) sont donc séparables (et elles sont alors normales si et seulement si elles sont galoisiennes).

L'extension (1) peut s'écrire comme $\mathbb{C} = \mathbb{R}(i)$, corps de rupture de $t^2 + 1 \in \mathbb{R}[t]$, au-dessus de $\mathbb{R}$. Mais dès lors que $t^2 + 1$ a acquis une racine, i , il est totalement décomposé, c'est-à-dire que son autre racine $-i$, est également dans $\mathbb{C}$, donc l'extension est normale. (On peut aussi simplement dire que $\mathbb{C}$ est la clôture algébrique de $\mathbb{R}$, donc évidemment normale.) Le groupe de Galois est $\mathbb{Z}/2\mathbb{Z}$, l'unique élément non trivial, σ , envoyant $a + ib$ sur $a - ib$ (c'est la conjugaison complexe).

L'extension (2) est également normale : quand on rompt le polynôme $t^2 - 2$ en lui adjoignant une racine $\sqrt{2}$ sur $\mathbb{Q}$, on lui adjoint du même coup son autre racine, $-\sqrt{2}$. Le groupe de Galois $\text{Gal}(\mathbb{Q}(\sqrt{2})/\mathbb{Q})$ est $\mathbb{Z}/2\mathbb{Z}$, l'unique élément non trivial envoyant $a + b\sqrt{2}$ sur $a - b\sqrt{2}$.

L'extension (3), en revanche, n'est pas normale : le polynôme $t^3 - 2$ admet dans $\mathbb{Q}(\sqrt[3]{2})$ la racine $\sqrt[3]{2}$, mais il n'est pas pour autant complètement décomposé : sinon, le rapport entre deux racines serait une racine primitive cubique de l'unité, j , et j n'appartient pas à $\mathbb{Q}(\sqrt[3]{2})$ (par exemple parce que j , vérifiant $j^2 = -1 - j$, est de degré 2 sur $\mathbb{Q}$, donc ne peut pas appartenir à $\mathbb{Q}(\sqrt[3]{2})$ qui est de degré 3 sur $\mathbb{Q}$). L'extension (4), elle, est normale : on a adjoint du même coup les trois racines, $\sqrt[3]{2}$, $j\sqrt[3]{2}$ et $j^2\sqrt[3]{2}$, de $t^3 - 2$. Le groupe de Galois est $\mathbb{Z}/3\mathbb{Z}$, engendré par l'automorphisme envoyant $a + b\sqrt[3]{2} + c\sqrt[3]{4}$ (avec $a, b, c \in \mathbb{Q}(j)$) sur $a + jb\sqrt[3]{2} + j^2c\sqrt[3]{4}$. L'extension (5) est normale, de nouveau car toute extension quadratique est normale (quand un polynôme de degré 2 admet une racine, il est complètement décomposé) ; son groupe de Galois est $\mathbb{Z}/2\mathbb{Z}$, l'élément non trivial envoyant j sur j^2 .

L'extension (6) est normale car elle est le corps de décomposition de $(t^2 + t + 1)(t^3 - 2)$ sur $\mathbb{Q}$. Son groupe de Galois est de cardinal 6 (puisque l'extension est de degré 6, admettant $1, j, \sqrt[3]{2}, j\sqrt[3]{2}, j^2, j^2\sqrt[3]{2}$ pour base sur $\mathbb{Q}$) ; or on y a déjà trouvé un élément τ d'ordre 3, qui fixe j et j^2 et envoie $\sqrt[3]{2}$ sur $j\sqrt[3]{2}$ et $\sqrt[3]{4}$ sur $j^2\sqrt[3]{4}$, et un élément σ d'ordre 2, qui fixe $\sqrt[3]{2}$ et $\sqrt[3]{4}$ et qui envoie j sur j^2 ; ces éléments vérifient $\tau\sigma = \sigma\tau^2$, donc le groupe de Galois est $\text{Gal}(\mathbb{Q}(\sqrt[3]{2}, j)/\mathbb{Q}) \cong \mathfrak{S}_3$ (les six éléments étant $1, \sigma, \tau, \sigma\tau, \tau^2, \sigma\tau^2$).

L'extension (7) est normale ($\mathbb{F}_{p^d}$ est le corps de décomposition de $t^{p^d} - t$ sur $\mathbb{F}_p$) et son groupe de Galois est engendré par le frobenius $\text{Fr}: x \mapsto x^p$, qui est d'ordre d , donc $\text{Gal}(\mathbb{F}_{p^d}/\mathbb{F}_p) \cong \mathbb{Z}/d\mathbb{Z}$.

L'extension (8) est normale, étant le corps de décomposition de $u^\ell - t \in \mathbb{C}(t)[u]$: en effet, dès que ce polynôme acquiert une racine, $t^{1/\ell}$, il acquiert toutes ses racines $t^{1/\ell}, \zeta t^{1/\ell}, \dots, \zeta^{\ell-1} t^{1/\ell}$, où $\zeta \in \mathbb{C}$ est une racine primitive ℓ -ième de l'unité. Le groupe de Galois de l'extension, $\text{Gal}(\mathbb{C}(t^{1/\ell})/\mathbb{C}(t))$, est d'ordre ℓ , donc c'est le groupe cyclique d'ordre ℓ engendré par l'élément $\sigma: t^{1/\ell} \mapsto \zeta t^{1/\ell}$.

L'extension (9) n'est pas séparable. En effet, l'élément $t^{1/p}$ a pour polynôme minimal $u^p - t \in \mathbb{F}_p(t)[u]$, qui n'est pas séparable. Elle est, en revanche, normale, puisque c'est le corps de décomposition du polynôme en question.

Enfin, l'extension (10) est séparable parce que $t^{1/\ell}$ a un polynôme minimal séparable sur

$\mathbb{F}_p(t)$, mais elle n'est pas normale car le polynôme en question, $u^\ell - t$, n'est pas complètement décomposé (sinon une racine ℓ -ième de l'unité serait dans $\mathbb{F}_p(t)$, donc dans $\mathbb{F}_p$, et ce n'est pas le cas lorsque $\ell > p$ est premier). ✓

Rappel (indépendance linéaire des caractères) : Soit Γ un groupe et E un corps. On suppose que $\chi_1, \dots, \chi_n$ sont des homomorphismes $\Gamma \rightarrow E^\times$ deux à deux distincts : alors $\chi_1, \dots, \chi_n$ sont linéairement indépendants, sur E , en tant qu'applications $\Gamma \rightarrow E$.

2. Soit L une extension galoisienne finie d'un corps K , de groupe de Galois $G = \text{Gal}(L/K)$. Montrer que

$$L \otimes_K L \cong \bigoplus_{\sigma \in G} L$$

en tant que K -algèbres — et même en tant que L -algèbres si on munit $L \otimes_K L$ de sa structure de L -espace vectoriel provenant de la multiplication sur le facteur de gauche — l'isomorphisme envoyant $x \otimes y$ sur la famille des $x \sigma(y)$ pour σ parcourant G . (Utiliser l'indépendance linéaire des caractères.)

Corrigé. Manifestement l'application $\varphi: L \otimes_K L \rightarrow \bigoplus_{\sigma \in G} L$ qui envoie $x \otimes y$ sur $(x \sigma(y))$ est bien définie et constitue un morphisme de K -algèbres. Comme les dimensions de part et d'autre sont les mêmes, il ne reste qu'à prouver l'injectivité. Or l'indépendance linéaire des caractères (appliqué au groupe $\Gamma = L^\times$ et sur le corps $E = L$) prouve que les différents $\sigma: L \rightarrow L$ de $G = \text{Gal}(L/K)$, vus comme applications K -linéaires de L dans L , sont L -linéairement indépendants. Soit $x_1, \dots, x_d$ une K -base de L , de sorte que $1 \otimes x_1, \dots, 1 \otimes x_d$ forme aussi une L -base de $L \otimes_K L$ muni de sa structure de L -espace vectoriel (de dimension $d = [L : K]$) par multiplication sur le facteur de gauche¹ : en prenant cette base au départ et la base canonique à l'arrivée, la matrice de φ (qui est L -linéaire) s'écrit comme $(\sigma_j(x_i))_{i,j}$ (où $\sigma_1, \dots, \sigma_d$ sont les éléments de G), et l'indépendance linéaire des σ_j prouve que cette matrice est inversible. ✓

3 (la trace). Soit $K \subseteq L$ une extension algébrique finie de corps. On appelle *trace* de L sur K , et on note $\text{tr}_{L/K}$, l'application qui à un $x \in L$ associe la trace (au sens des applications K -linéaires) de la multiplication par x , soit $y \mapsto xy$, de L dans L .

(0) Montrer que $\text{tr}_{L/K}: L \rightarrow K$ est K -linéaire.

(1) Quelle est la trace sur $\mathbb{R}$ de $a + ib \in \mathbb{C}$?

(2) Si $x \in K$ et que $d = [L : K]$, que vaut $\text{tr}_{L/K}(x)$?

(3) Si $L \subseteq E$ est une autre extension algébrique finie, montrer que $\text{tr}_{E/K} = \text{tr}_{L/K} \text{tr}_{E/L}$. (On pourra chercher à trouver une base de E sur K en fonction d'une base de E sur L et d'une base de L sur K .)

(4) Si $x \in L$, comment exprimer $\text{tr}_{L/K}(x)$ en fonction de son polynôme minimal μ_x ? (On pourra faire intervenir $d = [L : K]$ et $\delta = \deg_K x = \deg \mu_x$.)

(5) Si $K \subseteq L$ est finie galoisienne de groupe $G = \text{Gal}(L/K)$, montrer que $\text{tr}_{L/K}(x) = \sum_{\sigma \in G} \sigma(x)$. (On pourra éventuellement utiliser l'exercice 2, ou bien faire appel à la question précédente.)

(6a) Si $K \subseteq L$ n'est pas séparable, montrer que $\text{tr}_{L/K} = 0$ identiquement (on pourra se ramener à une extension de la forme $K(z^{1/p})$ avec $z \in K$ et p la caractéristique). (6b) Si L/K est séparable, montrer que $\text{tr}_{L/K}$ n'est pas identiquement nulle (en se ramenant à $K \subseteq L$

⁽¹⁾ Insistons bien : $L \otimes_K L$, qui est un K -espace vectoriel de dimension d^2 , a deux structures *différentes* de L -espace vectoriel de dimension d , l'une donnée par la multiplication $z \cdot (x \otimes y) = zx \otimes y$, qu'on considère ici, et l'autre donnée par $z \bullet (x \otimes y) = x \otimes zy$. L'application φ est L -linéaire pour la structure « gauche » mais non pour la structure « droite ».

galoisienne et en utilisant l'indépendance linéaire des caractères ou l'exercice 2 qui en résulte).
 (6c) Toujours lorsque $K \subseteq L$ est séparable, montrer que $B(x, y) = \text{tr}_{L/K}(xy)$ définit une forme K -bilinéaire symétrique non dégénérée sur L .

Corrigé. (0) L'application $L \rightarrow \text{Hom}_K(L, L)$ envoyant x sur l'application $y \mapsto xy$ de multiplication par x est K -linéaire, et la trace $\text{Hom}_K(L, L) \rightarrow K$ est K -linéaire.

(1) Sur la base $1, i$ de $\mathbb{C}$ sur $\mathbb{R}$, la multiplication par i a une matrice de diagonale nulle, donc $\text{tr}_{\mathbb{C}/\mathbb{R}}(i) = 0$, tandis que la multiplication par 1 est l'identité, donc de trace $\text{tr}_{\mathbb{C}/\mathbb{R}}(1) = 2$ (voir aussi la question suivante). Par $\mathbb{R}$ -linéarité (question précédente), on a $\text{tr}_{\mathbb{C}/\mathbb{R}}(a + ib) = 2a$.

(2) L'identité sur L , c'est-à-dire la multiplication par 1 , a pour trace $\text{tr}_{L/K}(1) = d = \dim_K L = [L : K]$. Il s'ensuit par K -linéarité que $\text{tr}_{L/K}(x) = dx$ pour tout $x \in K$.

(3) Si $x_1, \dots, x_d$ est une K -base de L et $y_1, \dots, y_e$ une L -base de E , alors $x_1 y_1, \dots, x_d y_1, x_1 y_2, \dots, x_d y_e$ est une K -base de E (en effet, tout élément t de E s'écrit de façon unique comme $\sum_{i=1}^n t_i y_i$ avec $t_i \in L$, et chacun des t_i s'écrit de façon unique comme $\sum_{j=1}^d t_{ij} x_j$ avec $t_{ij} \in K$, d'où l'écriture unique $t = \sum_{i,j} t_{ij} x_j y_i$). Si $t \in L$, la matrice de multiplication par t dans cette base s'écrit par blocs en remplaçant, dans la matrice de multiplication par t dans la L -base $y_1, \dots, y_e$ de E , chaque entrée a par la matrice de multiplication par a dans la K -base $x_1, \dots, x_d$ de L . On voit donc que la trace de t sur K , somme des coefficients diagonaux de cette matrice, est la somme des traces sur K des coefficients diagonaux de la matrice de multiplication par t sur L , c'est-à-dire $\text{tr}_{E/K}(t) = \text{tr}_{L/K}(\text{tr}_{E/L}(t))$.

(4) Le polynôme minimal μ_x de x sur K (c'est-à-dire l'unique polynôme unitaire irréductible qui annule x) est manifestement égal au polynôme minimal de la multiplication par x (en tant qu'endomorphisme du K -espace vectoriel L). Si $\delta = \deg_K x = \deg \mu_x$ est égal à $d = [L : K] = \dim_K L$ alors ce polynôme minimal est le polynôme caractéristique (de la multiplication par x) donc la trace se lit comme l'opposé du coefficient de degré $d - 1$ (on a choisi le polynôme unitaire). Sinon, en introduisant $F = K(x)$ le corps engendré par x sur K , on a $d = c\delta$ où $c = [L : F]$ et $\delta = [F : K]$, et d'après les questions précédentes, $\text{tr}_{L/K}(x) = c \text{tr}_{F/K}(x)$ et on est ramené au cas qu'on vient de traiter.

(5) Soit μ_x le polynôme minimal de x sur K . Sur L , on peut factoriser $\mu_x(t) = \prod_{\sigma(x)} (t - \sigma(x))$ où $\sigma(x)$ parcourt tous les conjugués (*distincts*) de x . Si $\delta = \deg_K x = \text{card}\{\sigma(x)\}$ et $d = [L : K]$, alors chaque $\sigma(x)$ est atteint pour $c = d/\delta$ valeurs σ différentes dans $G = \text{Gal}(L/K)$ (on a un groupe G d'ordre d qui agit transitivement sur l'ensemble de cardinal δ des conjugués de x). Comme $\text{tr}_{L/K}(x) = c \sum_{\sigma(x)} \sigma(x)$ (somme sur des conjugués distincts) d'après la question précédente, on a bien $\text{tr}_{L/K}(x) = \sum_{\sigma \in G} \sigma(x)$.

Une autre solution pour cette même question (5) consiste à faire appel à l'exercice 2 : sur la L -algèbre $\bigoplus_{\sigma \in G} L$, l'application L -linéaire qui multiplie sur chaque facteur par $\sigma(x)$ a évidemment pour trace $\sum_{\sigma \in G} \sigma(x)$, et l'isomorphisme $L \otimes_K L \cong \bigoplus_{\sigma \in G} L$ montre que cette trace est celle de la multiplication par x sur le facteur de droite sur la L -algèbre $L \otimes_K L$ (pour la structure L -linéaire provenant du facteur de gauche); comme la trace ne dépend pas du corps de base, cette trace est également la trace de la multiplication par x sur L comme K -espace vectoriel.

(6a) Soit $K \subseteq L$ une extension qui n'est pas séparable : il existe alors $x \in L$ qui n'est pas séparable sur K , et comme on a vu que $\text{tr}_{L/K} = \text{tr}_{K(x)/K} \text{tr}_{L/K(x)}$, il suffit de prouver que $\text{tr}_{K(x)/K} = 0$ identiquement, c'est-à-dire qu'on peut supposer $L = K(x)$. Par ailleurs, en notant p la caractéristique, toujours comme $\text{tr}_{K(x)/K} = \text{tr}_{K(x^p)/K} \text{tr}_{K(x)/K(x^p)}$, et l'inséparabilité nous assure que $K(x)/K(x^p)$ est bien une extension de degré p (le polynôme minimal de x n'a des coefficients non nuls que dans les degrés multiples de p), bref, on est ramené au cas où $z = x^p \in K$ et l'extension L est $K(z^{1/p})$. Or dans ce cas, en écrivant explicitement la matrice

de la multiplication par $x^i = z^{i/p}$ dans la base $1, x, \dots, x^{p-1}$ de L sur K , on voit clairement que la trace est identiquement nulle, y compris pour $i = 0$ (car p est la caractéristique).

(6b) Si $K \subseteq L$ est séparable, on peut trouver² une extension galoisienne finie E de K contenant L . Puisque $\text{tr}_{E/K} = \text{tr}_{L/K} \text{tr}_{E/L}$, il suffit de montrer que $\text{tr}_{E/K}$ est non nulle, bref, on peut supposer L galoisienne sur K . Si on utilise l'isomorphisme $L \otimes_K L \cong \bigoplus_{\sigma \in G} L$ donné par l'exercice 2, le fait que la trace $L \otimes_K L \rightarrow L$ n'est pas identiquement nulle est clair (prendre l'élément $(1, 0, \dots, 0) \in \bigoplus_{\sigma \in G} L$, dont la trace est manifestement 1) et il s'ensuit que la trace $L \rightarrow K$ ne l'est pas non plus ; cela découle aussi directement de l'indépendance linéaire des caractères : si $\sum_{\sigma \in G} \sigma(x)$ était nul pour tout $x \in L$, cela représenterait une relation de dépendance linéaire entre tous les $\sigma \in G$ vus comme des applications $L^\times \rightarrow L$.

(6c) Manifestement, B est une forme K -linéaire symétrique $L \times L \rightarrow K$. Il s'agit de prouver que si $x \in L$ n'est pas nul alors $B(x, \cdot) : L \rightarrow K$ est une forme linéaire non nulle. Or si on avait $\text{tr}_{L/K}(xy) = 0$ pour tout y , on aurait $\text{tr}_{L/K}(z) = 0$ pour tout z (puisque $x \neq 0$ donc tout $z \in L$ s'écrit de la forme xy), et on vient de voir que ceci n'est pas le cas. ✓

Rappel n°1 : Si $p \in \mathbb{Z}[t]$ et si $q, r \in \mathbb{Q}[t]$ sont unitaires et vérifient $p = qr$ alors en fait $q, r \in \mathbb{Z}[t]$. (Démonstration : soient M et N les plus petits entiers possibles tels que $Mq \in \mathbb{Z}[t]$ et $Nr \in \mathbb{Z}[t]$, et on cherche à prouver que $MN = 1$; or s'il existe un facteur premier $\ell | MN$ alors la réduction de Mq dans $\mathbb{F}_\ell[t]$ n'est pas nulle puisque M est minimal, et de même la réduction de Nr n'est pas nulle, donc la réduction de $MNqr = MNp$ n'est pas nulle, ce qui contredit le fait que ℓ divise MN donc chaque coefficient de MNp . Cela peut aussi se voir d'après l'algorithme de division euclidienne de polynômes.)

Rappel n°2 : Si $p(t) = t^3 + bt + c \in k[t]$ est un polynôme de degré 3 centré, avec k un corps quelconque, et si ξ_1, ξ_2, ξ_3 sont les racines de p , dans une clôture algébrique $\bar{k}$ de k , comptées avec multiplicités, alors le discriminant $\Delta = -4b^3 - 27c^2$ de p vaut δ^2 où $\delta = (\xi_2 - \xi_1)(\xi_3 - \xi_1)(\xi_3 - \xi_2)$. (Une façon fastidieuse — mais simple — de le voir est de développer complètement $\Delta = \delta^2$ et d'utiliser $\xi_1 + \xi_2 + \xi_3 = 0$, $\xi_1\xi_2 + \xi_1\xi_3 + \xi_2\xi_3 = b$ et $\xi_1\xi_2\xi_3 = -c$.)

4. Déterminer le groupe de Galois des équations suivantes (c'est-à-dire du corps de décomposition du polynôme qui les définit) sur $\mathbb{Q}$: (a) $t^3 - 2t + 1 = 0$, (b) $t^3 + t + 1 = 0$, (c) $t^3 - 6t + 1 = 0$, (d) $t^3 - 12t + 8 = 0$.

Corrigé. (a) Le polynôme $p(t) = t^3 - 2t + 1$ se factorise sur $\mathbb{Q}$ comme $p(t) = (t - 1)(t^2 + t - 1)$. Par conséquent, son corps de décomposition est celui de $t^2 + t - 1$, soit $\mathbb{Q}(\sqrt{5})$. Le groupe de Galois G_p est donc cyclique d'ordre 2 avec pour élément non trivial l'automorphisme envoyant $\sqrt{5}$ sur $-\sqrt{5}$.

(b) Le polynôme $p(t) = t^3 + t + 1 \in \mathbb{Z}[t]$ n'a pas de racine dans $\mathbb{F}_2$ donc est irréductible sur $\mathbb{F}_2$ (un polynôme réductible de degré 3 se décompose comme produit d'un polynôme de degré 2 et d'un polynôme de degré 1, donc il doit avoir une racine) donc sur $\mathbb{Z}$ donc sur $\mathbb{Q}$ (cf. le rappel n°1 ci-dessus). Le groupe de Galois G_p (du corps de décomposition) de ce polynôme opère donc transitivement sur les trois racines de $p(t)$ dans $\bar{\mathbb{Q}}$; or il n'y a que deux sous-groupes de $\mathfrak{S}_3$ qui opèrent transitivement, à savoir $\mathfrak{S}_3$ tout entier et $\mathbb{Z}/3\mathbb{Z}$. Comme $p(t)$ a une unique racine réelle, donc deux racines complexes conjuguées (c'est-à-dire que sur $\mathbb{R}$ il se factorise comme produit d'un polynôme de degré 2 et d'un polynôme de degré 1), il existe un élément d'ordre 2 dans le groupe de Galois (sur $\mathbb{R}$, la conjugaison complexe), et ceci montre que $G_p \cong \mathfrak{S}_3$.

(c) Le polynôme $p(t) = t^3 - 6t + 1 \in \mathbb{Z}[t]$ n'a pas de racine dans $\mathbb{Z}$ (soit parce qu'il n'en a pas dans $\mathbb{F}_7$, soit parce que tout facteur premier d'une telle racine devrait diviser le coefficient constant 1, donc la racine ne peut être que 1 ou -1 et il n'y en a pas) donc comme pour la question précédente il est irréductible sur $\mathbb{Q}$. De nouveau, on veut trouver un élément d'ordre 2 dans le groupe de Galois. Mais cette fois on ne peut pas simplement utiliser la conjugaison

⁽²⁾ Par exemple en prenant la composée de toutes les images d'un plongement de L dans une clôture algébrique de K au-dessus de K . Ou bien en prenant le corps de décomposition des polynômes minimaux de générateurs de L au-dessus de K .

complexe (elle agit trivialement puisque les trois racines de p sont réelles). On pourrait travailler en réduisant modulo 5 (i.e., faire jouer à « $\mathbb{Q}_5$ » le rôle de $\mathbb{R}$ dans la méthode précédente, puisque p a une unique racine, 3, dans $\mathbb{F}_5$), mais on va plutôt faire autrement. Appelons ξ_1, ξ_2, ξ_3 les trois racines réelles de p (dans un ordre quelconque), et soit $\delta = (\xi_2 - \xi_1)(\xi_3 - \xi_1)(\xi_3 - \xi_2)$. D'après le rappel n°2, on a $\Delta = \delta^2 = -4 \times (-6)^3 - 27 \times 1^2 = 27 \times 31$, qui n'est pas un carré dans $\mathbb{Q}$. Par conséquent, $\mathbb{Q}(\delta)$ est une extension de $\mathbb{Q}$ de degré exactement 2 contenue dans $\mathbb{Q}(\xi_1, \xi_2, \xi_3)$, donc $[\mathbb{Q}(\xi_1, \xi_2, \xi_3) : \mathbb{Q}] = 6$ et le groupe de Galois est de nouveau $\mathfrak{S}_3$.

(d) Le polynôme $p(t) = t^3 - 12t + 8 \in \mathbb{Z}[t]$ n'a pas de racine dans $\mathbb{F}_5$ donc, comme précédemment, est irréductible sur $\mathbb{Q}$. Appelons ξ_1, ξ_2, ξ_3 les trois racines réelles de p avec $\xi_1 < \xi_2 < \xi_3$, et soit $\delta = (\xi_2 - \xi_1)(\xi_3 - \xi_1)(\xi_3 - \xi_2)$. D'après le rappel n°2, on a $\delta^2 = -4 \times (-12)^3 - 27 \times 8^2 = 5184 = 72^2$ et comme $\delta > 0$ (vu l'ordre choisi sur les racines) c'est que $\delta = 72 \in \mathbb{Q}$. Il n'y a donc pas d'élément du groupe de Galois G_p de p qui échange ξ_1 et ξ_2 en laissant ξ_3 fixe, car un tel automorphisme transformerait δ en $-\delta$, ce qui n'est pas possible ($\mathbb{Q}$ doit rester fixe). ✓

5 (groupes de Galois cyclotomique). (1) Soit n un naturel non nul et ζ une racine primitive n -ième de l'unité. Soit f le polynôme minimal de ζ sur $\mathbb{Q}$ et h tel que $t^n - 1 = f(t)h(t)$: montrer que si p est un nombre premier ne divisant pas n alors ζ^p est aussi racine de f (si non, $f(t)$ diviserait $h(t^p)$, puis réduire modulo p). En déduire la valeur du groupe de Galois $\text{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q})$ et l'irréductibilité du polynôme cyclotomique Φ_n .

(2) Montrer que tout groupe cyclique (fini) est le groupe de Galois d'une certaine extension galoisienne L de $\mathbb{Q}$.

(3) Si ζ est une racine primitive n -ième de l'unité et p un nombre premier qui ne divise pas n , que vaut $\text{Gal}(\mathbb{F}_p(\zeta)/\mathbb{F}_p)$ (lorsque ζ est une racine primitive n -ième de l'unité dans $\bar{\mathbb{F}}_p$) ? Quels sont les n tels que Φ_n soit irréductible sur $\mathbb{F}_p$?

Corrigé. (1) Manifestement, ζ^p est racine de $t^n - 1$, donc, si on suppose par l'absurde qu'il n'est pas racine de f , c'est qu'il est racine de h , soit $h(\zeta^p) = 0$. Par action du groupe de Galois $\text{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q})$ de $t^n - 1$ (qui agit transitivement sur les racines de f) on voit que toute racine de $f(t)$ est racine de $h(t^p)$, c'est-à-dire que $f(t)$ divise $h(t^p)$. Or en réduisant modulo p ceci signifierait que $\bar{f}(t)$ (la réduction à $\mathbb{F}_p$ de f) diviserait $\bar{h}^p$ (car $\bar{h}(t^p) = \bar{h}^p(t)$). Notamment, $\bar{f}$ et $\bar{h}$ auraient une racine commune, c'est-à-dire que $\bar{f}\bar{h} = t^n - 1$ aurait une racine multiple dans $\mathbb{F}_p$, ce qui n'est possible que si p divise n .

Le groupe de Galois de $\mathbb{Q}(\zeta)$ sur $\mathbb{Q}$ est *a priori* un sous-groupe de $(\mathbb{Z}/n\mathbb{Z})^\times$ (les classes des entiers inversibles dans $\mathbb{Z}/n\mathbb{Z}$) puisque tout automorphisme de $\mathbb{Q}(\zeta)$ est déterminé par sa valeur ζ^k sur ζ , qui constitue un élément $k \in (\mathbb{Z}/n\mathbb{Z})^\times$. Mais par ailleurs, le groupe de Galois doit agir transitivement sur les racines de f : or on vient de voir que si ζ est une racine de f et que p ne divise pas n , alors ζ^p est encore une racine de f . C'est donc que $\text{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q}) \subseteq (\mathbb{Z}/n\mathbb{Z})^\times$ contient les classes de tous les p premiers ne divisant pas n , donc on a $\text{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q}) = (\mathbb{Z}/n\mathbb{Z})^\times$. Enfin, toutes les racines primitives n -ièmes de l'unité sont des racines de f , c'est-à-dire que Φ_n (le n -ième polynôme cyclotomique) divise f , et comme f est irréductible, en fait $\Phi_n = f$. On voit au passage que $[\mathbb{Q}(\zeta) : \mathbb{Q}] = \varphi(n)$ (fonction indicatrice d'Euler).

(2) Soit $m = p_1^{r_1} \cdots p_s^{r_s}$ (avec p_i premiers distincts et $r_i \geq 1$) un entier naturel non nul, et soit $m^* = p_1^{r_1^*} \cdots p_s^{r_s^*}$ où $r_i^* = r_i + 2$ (en fait, si $p_i \neq 2$ on peut se contenter de $r_i^* = r_i + 1$) : alors, pour tout i , $(\mathbb{Z}/p_i^{r_i^*}\mathbb{Z})^\times$ admet³ $\mathbb{Z}/p_i^{r_i}\mathbb{Z}$ pour quotient, donc (grâce au théorème chinois)

⁽³⁾ On rappelle que $(\mathbb{Z}/p^{r^*}\mathbb{Z})^\times$ est cyclique d'ordre $\varphi(p^{r^*}) = p^{r^*-1}(p-1)$ si $p \neq 2$, ou, si $p = 2$ et $r^* \geq 2$, est le produit de $\mathbb{Z}/2\mathbb{Z}$ par $\mathbb{Z}/2^{r^*-2}\mathbb{Z}$.

$(\mathbb{Z}/m^*\mathbb{Z})^\times$ admet $\mathbb{Z}/m\mathbb{Z}$ pour quotient. L'extension $\mathbb{Q}(\zeta)$ de $\mathbb{Q}$, où ζ est une racine m^* -ième de l'unité, a donc un groupe de Galois qui a un quotient isomorphe à $\mathbb{Z}/m\mathbb{Z}$: mais ceci signifie qu'il existe un sous-corps L de $\mathbb{Q}(\zeta)$, galoisien sur $\mathbb{Q}$, qui a $\mathbb{Z}/m\mathbb{Z}$ pour groupe de Galois sur ce dernier.

(3) Si r est le plus petit entier tel que $p^r - 1$ soit multiple de n , autrement dit l'ordre de p modulo n , alors $\mathbb{F}_p(\zeta) = \mathbb{F}_{p^r}$ (en effet, le groupe multiplicatif de $\mathbb{F}_{p^r}$ est précisément le groupe des racines $(p^r - 1)$ -ièmes de l'unité, et seules existent les extensions $\mathbb{F}_{p^r}$ de $\mathbb{F}_p$). Le groupe de Galois de $\mathbb{F}_p(\zeta)$ sur $\mathbb{F}_p$ est donc $\text{Gal}(\mathbb{F}_{p^r}/\mathbb{F}_p) = \mathbb{Z}/r\mathbb{Z}$. En particulier, Φ_n est irréductible sur $\mathbb{F}_p$ si et seulement si l'ordre de p modulo n est $\varphi(n)$, c'est-à-dire si et seulement si p engendre $(\mathbb{Z}/n\mathbb{Z})^\times$ (ce qui exige au moins que n soit un nombre premier ou le double d'un nombre premier, sinon $(\mathbb{Z}/n\mathbb{Z})^\times$ n'est pas cyclique). ✓