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) $\mathbb{C}/\mathbb{R}$, (2) $\mathbb{Q}(\sqrt{2})/\mathbb{Q}$, (3) $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$, (4) $\mathbb{Q}(\sqrt[3]{2}, j)/\mathbb{Q}(j)$ (où j est une racine primitive cubique de l'unité), (5) $\mathbb{Q}(j)/\mathbb{Q}$, (6) $\mathbb{Q}(\sqrt[3]{2}, j)/\mathbb{Q}$, (7) $\mathbb{F}_{p^d}/\mathbb{F}_p$ (p étant un nombre premier, et d un naturel non nul), (8) $\mathbb{C}(t^{1/\ell})/\mathbb{C}(t)$ où ℓ est un nombre premier quelconque, (9) $\mathbb{F}_p(t^{1/p})/\mathbb{F}_p(t)$, (10) $\mathbb{F}_p(t^{1/\ell})/\mathbb{F}_p(t)$ où ℓ est un nombre premier strictement supérieur à p.

2 (indépendance linéaire des caractères). Soit Γ un groupe et E un corps. On suppose que $\chi_1, \ldots, \chi_n$ sont des homomorphismes $\Gamma \to E^\times$ deux à deux distincts. Montrer que $\chi_1, \ldots, \chi_n$ sont linéairement indépendants, sur E, en tant qu'applications $\Gamma \to E$. Pour cela, on pourra partir d'une relation de dépendance linéaire sur un nombre n aussi petit que possible, et montrer (en utilisant le fait que $\chi_1(z) \neq \chi_2(z)$ pour un certain $z \in \Gamma$) qu'on peut la réduire encore d'un.

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

4 (la trace). Soit L/K une extension algébrique finie de corps. On appelle *trace* de L sur K, et on note $\mathrm{tr}_{L/K}$, 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 $\mathrm{tr}_{L/K}\colon L \to K$ 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 $\mathrm{tr}_{L/K}(x)$?

(3) Si E/L est une autre extension algébrique finie, montrer que $\mathrm{tr}_{E/K} = \mathrm{tr}_{L/K}\,\mathrm{tr}_{E/L}$. (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 $\mathrm{tr}_{L/K}(x)$ 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 L/K est finie galoisienne de groupe $G = \mathrm{Gal}(L/K)$, montrer que $\mathrm{tr}_{L/K}(x) = \sum_{\sigma \in G} \sigma(x)$. (On pourra éventuellement utiliser l'exercice 3, ou bien faire appel à la question précédente.)

(6a) Si L/K n'est pas séparable, montrer que $\mathrm{tr}_{L/K} = 0$ 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 $\mathrm{tr}_{L/K}$ n'est pas identiquement nulle (en se ramenant à L/K galoisienne et en utilisant un des exercices 2 ou 3). (6c) Toujours lorsque L/K est séparable, montrer que $B(x, y) = \mathrm{tr}_{L/K}(xy)$ définit une forme K-bilinéaire symétrique non dégénérée sur L.

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 $\xi_1\xi_2\xi_3 = -c$.)

5. 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) $t^3 - 12t + 8 = 0$.

6 (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 (sinon, $f(t)$ diviserait $h(t^p)$, puis réduire modulo p). En déduire la valeur du groupe de Galois $\mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q})$ 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 $\mathrm{Gal}(\mathbb{F}_p(\zeta)/\mathbb{F}_p)$ (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 $\mathbb{F}_p$?

Motivations : L'exercice 1 est un échauffement péliminaire. L'exercice 2 est un théorème de Dirichlet. L'exercice 3 est la formulation bourbachique-grothendieckienne de la théorie de Galois : elle signifie qu'une extension galoisienne L/K de corps se « déploie » elle-même, et son intérêt est de permettre de lire la structure de l'extension L/K après extension des scalaires à L, comme quelque chose de simple (d copies de L sur lesquelles le groupe de Galois opère simplement par permutation). L'exercice 4 introduit une forme linéaire très importante dans l'étude d'une extension galoisienne. L'exercice 5 ouvre la voie à des calculs de groupes de Galois sur $\mathbb{Q}$ en commençant par le cas le plus simple non trivial : celui des équations cubiques. L'exercice 6 est fondamental à plusieurs titres — on mentionnera le théorème difficile (dû à Kronecker et Weber) selon lequel toute extension galoisienne de $\mathbb{Q}$ dont le groupe de Galois est abélien est contenu dans une extension cyclotomique $\mathbb{Q}(\zeta)$.