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.

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

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

3 (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.

4 (la trace). Soit $K \subseteq L$ 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 $L \subseteq E$ 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 $K \subseteq L$ est finie galoisienne de groupe $G = \mathrm{Gal}(L/K)$, montrer que $\mathrm{tr}_{L/K}(x) = \sum_{\sigma \in G} \sigma(x)$.

(6a) Si $K \subseteq L$ 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 $K \subseteq L$ galoisienne et en utilisant l'exercice 3). (6c) Toujours lorsque $K \subseteq L$ est séparable, montrer que $B(x, y) = \mathrm{tr}_{L/K}(xy)$ définit une forme K-bilinéaire symétrique non dégénérée sur L.

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

(0) Montrer que $\mathrm{N}_{L/K}\colon L \to K$ est multiplicative, i.e., $\mathrm{N}_{L/K}(xy) = \mathrm{N}_{L/K}(x)\ \mathrm{N}_{L/K}(y)$ si $x, y \in L$. À quelle condition a-t-on $\mathrm{N}_{L/K}(x) = 0$?

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

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

(3) Si $L \subseteq E$ est une autre extension algébrique finie, montrer que $\mathrm{N}_{E/K} = \mathrm{N}_{L/K}\,\mathrm{N}_{E/L}$.

(4) Si $x \in L$, comment exprimer $\mathrm{N}_{L/K}(x)$ 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 $G = \mathrm{Gal}(L/K)$, montrer que $\mathrm{N}_{L/K}(x) = \prod_{\sigma\in G} \sigma(x)$.

(6) Montrer que si K est un corps admettant une extension algébrique de degré d, où d est un certain entier naturel, alors il existe un polynôme $N(u_1, \ldots, u_d)$ homogène de degré d en d variables dont le seul zéro est le zéro trivial (l'origine). Donner un exemple de forme cubique (=polynôme homogène de degré 3) en trois variables sur $\mathbb{F}_7$ qui ne s'annule qu'en $(0, 0, 0)$.