EXTENSIONS DE CORPS ET THÉORIE DE GALOIS

Contents

Notations

Clôture algébrique des corps premiers. La clôture algébrique de $\mathbb{Q}$ contenue dans $\mathbb{C}$ est notée $\overline{\mathbb{Q}}$. La lettre p désigne toujours un nombre premier. Pour tout p on fixe une clôture algébrique $\overline{\mathbb{F}}_p$ de $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$.

Morphismes. Soient K un corps, $\overline{K}$ une clôture algébrique de K et L un corps tel que $K \subseteq L \subseteq \overline{K}$. L'ensemble des K-plongements de L dans $\overline{K}$, i.e. des morphismes de corps de L dans $\overline{K}$ fixant K, est noté $\mathrm{Hom}_K(L, \overline{K})$. Le groupe des automorphismes de corps de L fixant K est noté $\mathrm{Aut}_K(L)$. Si G est un sous-groupe de $\mathrm{Aut}_K(L)$ le sous-corps de L fixe par G est noté $L^G = \{x \in L \mid \forall\, \sigma \in G, \sigma(x) = x\}$. Si l'extension L/K est galoisienne son groupe de Galois est noté $\mathrm{Gal}(L/K) = \mathrm{Aut}_K(L)$.

Groupes. Si A est un groupe abélien A_{tors} est le sous-groupe de A formé des éléments de torsion. Si G est un groupe agissant sur un ensemble E et $x \in E$, l'orbite de x sous G est $\mathrm{Orb}_G(x) = \{gx,\, g \in G\} \subseteq E$ et $\mathrm{Stab}_G(x) = \{g \in G \mid gx = x\} \subseteq G$ est le stabilisateur de x sous G. Le groupe des permutations d'un ensemble à n éléments est noté $\mathcal{S}_n$.

1. Extensions algébriques

Exercice 1.1. Calculer le degré sur $\mathbb{Q}$ des corps suivants.

1. $\mathbb{Q}(\sqrt{2},\sqrt{3})$, $\mathbb{Q}(\sqrt{2},\sqrt{3}+\sqrt{2})$, $\mathbb{Q}(\sqrt{2},\sqrt{6})$, $\mathbb{Q}(\sqrt{3},\sqrt{6}+\sqrt{2})$.
2. $\mathbb{Q}(\sqrt{2},\sqrt{3},\sqrt{5})$, $\mathbb{Q}(\sqrt{2}+\sqrt{3},\sqrt{2}+\sqrt{5},\sqrt{3}+\sqrt{5})$, $\mathbb{Q}(\sqrt{6},\sqrt{15},\sqrt{10})$.
3. $\mathbb{Q}(e^{i2\pi/3},i)$, $\mathbb{Q}(i\sqrt{3},i)$, $\mathbb{Q}(\sqrt{3},i)$.
4. $\mathbb{Q}(\sqrt{2},\sqrt[3]{2})$, $\mathbb{Q}(\sqrt[3]{2},\sqrt[4]{2})$, $\mathbb{Q}(\sqrt{2},\sqrt[4]{2})$.

Exercice 1.2. Pour $\alpha=\frac{1+\sqrt{5}}{2}$, $i+\sqrt{3}$, $e^{i2\pi/5}$ et $K=\mathbb{Q}$, $\mathbb{Q}(i)$,

1. Calculer $[K(\alpha):K]$ et donner une base de $K(\alpha)$ sur K.
2. Déterminer les coordonnées de α^{-1} et de $\frac{\alpha+1}{\alpha-1}$ dans cette base.

Exercice 1.3. Soit L/K une extension finie de corps telle que $[L:K]$ est premier.

1. Déterminer toutes les extensions intermédiaires entre K et L.
2. Montrer qu'il existe $\alpha\in L$ tel que $L=K(\alpha)$.

Exercice 1.4. Soient K un corps et $\overline{K}$ une clôture algébrique de K. Soient $P(X)\in K[X]$ irréductible de degré n et L/K une extension de degré m dans $\overline{K}$ tels que n et m sont premiers entre eux. Soit $\alpha\in\overline{K}$ tel que $P(\alpha)=0$.

1. Montrer que $[L(\alpha):L]\leq n$.
2. Montrer que nm divise $[L(\alpha):K]$.
3. Montrer que n divise $[L(\alpha):L]$.
4. Montrer que $P(X)$ est irréductible dans $L[X]$.

Exercice 1.5. Soit $K=\mathbb{Q}(\sqrt{2},\sqrt{3})\subset\overline{\mathbb{Q}}$.

1. Montrer que $[K:\mathbb{Q}]=4$ et donner une base de K sur $\mathbb{Q}$.
2. Montrer que $\mathbb{Q}(\sqrt{2}+\sqrt{3})=K$.
3. Déterminer le polynôme minimal de $\sqrt{2}+\sqrt{3}$ sur $\mathbb{Q}$.

Exercice 1.6. Soit $\zeta\in\overline{\mathbb{Q}}$ une racine de X^6+X^3+1. Déterminer $\mathrm{Hom}_{\mathbb{Q}}\big(\mathbb{Q}(\zeta),\overline{\mathbb{Q}}\big)$.

Exercice 1.7. Soient K un corps, $\overline{K}$ une clôture algébrique de K, et $\alpha\in\overline{K}$. Soient $P_\alpha(X)$ et $P_{\alpha^2}(X)$ les polynômes minimaux sur K de α et α^2 respectivement. Montrer que $[K(\alpha):K(\alpha^2)]=2$ si et seulement si $P_\alpha(X)=P_{\alpha^2}(X^2)$.

Exercice 1.8. Soient K un corps, $\overline{K}$ une clôture algébrique de K, et $\alpha\in\overline{K}$ de polynôme minimal $P_\alpha(X)$ sur K. Soit $Q(X)\in K[X]$ non nul. On définit l'application

$$\begin{aligned}\phi_Q : K[X] &\longrightarrow K[X]\\ P(X) &\longmapsto (P\circ Q)(X)=P\big(Q(X)\big).\end{aligned}$$

1. Montrer que ϕ_Q est un morphisme d'anneaux K-linéaire et déterminer $\operatorname{Ker}\phi_Q$.
2. Soit $\psi_Q : K[X]\to K[X]/(P_\alpha(X))$ le morphisme obtenu en composant ϕ_Q avec le morphisme de réduction modulo $(P_\alpha(X))$. Montrer que $\operatorname{Ker}\psi_Q=(P_{Q(\alpha)}(X))$ où $P_{Q(\alpha)}(X)$ est le polynôme minimal de $Q(\alpha)$ sur K.

Exercice 1.9. Soient K un corps et $\overline{K}$ une clôture algébrique de K. Soient $\alpha,\beta\in\overline{K}$ de polynômes minimaux respectifs $P_\alpha(X), P_\beta(X)$ sur K. Montrer que les assertions suivantes sont équivalentes.

(i) $K(\beta)$ contient un sous-corps K-isomorphe à $K(\alpha)$.

(ii) Il existe $\sigma \in \mathrm{Hom}_K\big(K(\alpha), \overline{K}\big)$ tel que $K(\sigma(\alpha)) \subseteq K(\beta)$.
(iii) Il existe $Q(X) \in K[X]$ tel que $P_\beta(X)$ divise $(P_\alpha \circ Q)(X)$ dans $K[X]$.

Exercice 1.10. Déterminer toutes les extensions de $\mathbb{Q}$ contenues dans $\mathbb{Q}(\sqrt[4]{2})$.

Exercice 1.11. Soit K l'ensemble des $x \in \mathbb{R}$ tels qu'il existe une suite de corps $\mathbb{Q} = K_0 \subseteq K_1 \subseteq \ldots \subseteq K_n \subseteq \mathbb{R}$ tels que $x \in K_n$ et $[K_i : K_{i-1}] \leq 3$ pour tout $1 \leq i \leq n$.

1. Montrer que K est un sous-corps de $\mathbb{R} \cap \overline{\mathbb{Q}}$.
2. Soit $\alpha \in K$. Montrer que $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 2^n 3^m$ avec $n, m \in \mathbb{N}$.
3. Soit $\alpha \in K$ tel que $\alpha \geq 0$. Montrer que $X^2 - \alpha$ est réductible dans $K[X]$.
4. Soit $P(X) \in K[X]$ tel que $\deg P = 3$. Montrer que $P(X)$ a une racine dans K.
5. Soit $\alpha \in K$ tel que $[\mathbb{Q}(\alpha) : \mathbb{Q}]$ divise 35. Montrer que $\alpha \in \mathbb{Q}$.

2. Extensions transcendantes

Exercice 2.1. Soient $\mathbb{K}/K$ une extension de corps, $x \in \mathbb{K}$ transcendant sur K, et $f(X) \in K(X)$ tel que $f(X) \notin K$. Soit $y \in \mathbb{K}$.

1. On suppose que $y = f(x)$. Montrer que y est transcendant sur K.
2. On suppose que $x = f(y)$. Montrer que y est transcendant sur K.

Exercice 2.2. Soient $\mathbb{K}/K$ une extension de corps, $x \in \mathbb{K}$ transcendant sur K, et $\alpha \in \mathbb{K}$ algébrique sur K tel que $\alpha \notin K$. Montrer que le corps $K(\alpha, x)$ n'est contenu dans aucune extension simple de K dans $\mathbb{K}$.

Exercice 2.3. Soient $\mathbb{K}/K$ une extension de corps et $x \in \mathbb{K}$ transcendant sur K. Soit L une extension de K telle que $L \subseteq K(x)$ et $L \neq K$. Montrer que x est algébrique sur L.

Exercice 2.4. Soient $\mathbb{K}/K$ une extension de corps et $x \in \mathbb{K}$ transcendant sur K. Montrer que $\mathrm{Aut}_K\big(K(x)\big) \neq \mathrm{Hom}_K\big(K(x), K(x)\big)$.

Exercice 2.5. Soient L/K une extension de corps et R un anneau tel que $K \subseteq R \subseteq L$.

1. On suppose que L/K est algébrique. Montrer que R est un corps.
2. On suppose que L/K n'est pas algébrique. Donner des exemples d'anneaux R qui ne sont pas des corps.

Exercice 2.6. Soient $\mathbb{K}/K$ une extension de corps et $x \in \mathbb{K}$ transcendant sur K.

1. Soit $P(X) \in K[X]$ non constant. Montrer que $[K(x) : K(P(x))] = \deg P$.
2. Soit $f(x) = \frac{(x^2-x+1)^3}{x^2(x-1)^2} \in K(x)$. Montrer que $[K(x) : K(f(x))] = 6$.

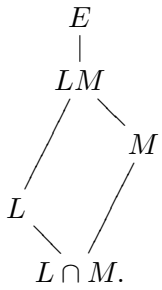
Exercice 2.7. Soient $\mathbb{K}/K$ une extension de corps et $x \in \mathbb{K}$ transcendant sur K.

1. Soit $f(X) \in K(X)$ avec $f(X) \notin K$. Soient $P(X), Q(X) \in K[X]$ premiers entre eux tels que $f(X) = P(X)/Q(X)$. Montrer que $[K(x) : K(f(x))] = \mathrm{Max}(\deg P, \deg Q)$.
2. Montrer que
$$\mathrm{Aut}_K\big(K(x)\big) = \Big\{ f(x) \mapsto f\Big(\frac{ax+b}{cx+d}\Big),\ a, b, c, d \in K \text{ tels que } ad - bc \neq 0 \Big\}.$$
3. Soient $\sigma, \rho_a, \tau_b \in \mathrm{Aut}_K(K(x))$ donnés par $\sigma(x) = x^{-1}$, $\rho_a(x) = ax$, $\tau_b(x) = x + b$ pour tous $a, b \in K$ avec $a \neq 0$. Montrer que ces éléments engendrent $\mathrm{Aut}_K(K(x))$.

3. Disjonction linéaire

Définition 1. Soient E un corps et $L, M \subseteq E$ deux sous-corps. On note LM le plus petit sous-corps de E contenant L et M.

Noter que LM est l'intersection de tous les sous-corps de E contenant L et M, ou bien encore le sous-corps de E engendré par $L \cup M$. Dualement $L \cap M$ est le plus grand sous-corps de E contenu dans L et dans M. On a donc le diagramme d'extensions suivant



Exercice 3.1. Soient E un corps et $L, M \subseteq E$ deux sous-corps.

1. Montrer que $LM = \{\sum_{\text{finie}} \alpha_k \beta_m,\ \alpha_k \in L,\ \beta_m \in M\}$ = le plus petit sous-anneau de E contenant $L \cup M$. (Comparer avec l'exercice 2.5.)
2. Montrer que $[LM : L \cap M] \leq [L : L \cap M]\,[M : L \cap M]$.
3. On suppose que $[L : L \cap M]$ et $[M : L \cap M]$ sont finis et premiers entre eux. Montrer que $[LM : L \cap M] = [L : L \cap M]\,[M : L \cap M]$.
4. Soit $\mathcal{E}$ l'ensemble des entiers $a \in \mathbb{Z}$ pour lesquels il existe un p premier tel que p divise a et p^2 ne divise pas a. Soient $a, b \in \mathcal{E}$ et $n, m > 1$ deux entiers premiers entre eux. Calculer $[\mathbb{Q}(\sqrt[n]{a}, \sqrt[m]{b}) : \mathbb{Q}]$.

Exercice 3.2. Soient L/K et M/K des extensions de corps. Montrer que les assertions suivantes sont equivalentes.

(i) Tout ensemble fini d'éléments de L linéairement indépendant sur K l'est sur M.
(ii) Tout ensemble fini d'éléments de M linéairement indépendant sur K l'est sur L.

Définition 2. Soient L/K et M/K des extensions de corps. Les extensions L et M sont *linéairement disjointes sur* K si l'une des conditions équivalentes de l'exercice 3.2 est vérifiée.

Exercice 3.3. Soient L et M deux extensions linéairement disjointes sur K.

1. Montrer que $L \cap M = K$.
2. Montrer que $[LM : M] = [L : K]$ et $[LM : L] = [M : K]$.

Exercice 3.4. Soient $\zeta_3 = e^{2i\pi/3}$ et $\zeta_4 = i$ dans $\overline{\mathbb{Q}}^{\times}_{\text{tors}}$.

1. Montrer que $\mathbb{Q}(\sqrt[4]{2})$ et $\mathbb{Q}(\zeta_4 \sqrt[4]{2})$ ne sont pas linéairement disjoints sur $\mathbb{Q}$.
2. (a) Montrer que $\mathbb{Q}(\sqrt[3]{2}) \cap \mathbb{Q}(\zeta_3 \sqrt[3]{2}) = \mathbb{Q}$.
   (b) Montrer que $\mathbb{Q}(\sqrt[3]{2})$ et $\mathbb{Q}(\zeta_3 \sqrt[3]{2})$ ne sont pas linéairement disjoints sur $\mathbb{Q}$ (considérer par exemple le produit scalaire de $(1, \sqrt[3]{2}, \sqrt[3]{4})$ par $(\zeta_3^2 \sqrt[3]{4}, \zeta_3 \sqrt[3]{2}, 1)$).

Exercice 3.5. Soient L/K et M/K des extensions finies de corps.

1. On suppose que $[LM : K] = [L : K]\,[M : K]$.
   (a) Soient $(x_i)_{1 \leq i \leq n}$ une base de L sur K et $(y_j)_{1 \leq j \leq m}$ une base de M sur K. Montrer que $(x_i y_j)_{1 \leq i \leq n, 1 \leq j \leq m}$ est une base de LM sur K.

(b) Montrer que L et M sont linéairement disjoints sur K.

2. On suppose que $[L : K]$ et $[M : K]$ sont premiers entre eux. Montrer que L et M sont linéairement disjoints sur K.

Définition 3. Soient $\mathbb{K}/K$ une extension de corps, $n \geq 1$ un entier, et $x_1, \ldots, x_n \in \mathbb{K}$. Les éléments $x_1, \ldots, x_n$ sont *algébriquement indépendants sur* K si

$$\mathrm{Ker}\begin{pmatrix} K[X_1, \ldots, X_n] \longrightarrow \mathbb{K} \\ P(X_1, \ldots, X_n) \longmapsto P(x_1, \ldots, x_n) \end{pmatrix} = 0.$$

Si $x_1, \ldots, x_n$ sont algébriquement indépendants sur K alors ils sont transcendants sur K.

Exercice 3.6. Soient $\mathbb{K}/K$ une extension de corps et $x, y \in \mathbb{K}$.

1. Montrer que si x est transcendant sur K et L est une extension algébrique de K alors $K(x)$ et L sont linéairement disjoints sur K.
2. Montrer que si x et y sont algébriquement indépendants sur K alors $K(x)$ et $K(y)$ sont linéairement disjoints sur K.

4. Norme et Trace (cas séparable)

Exercice 4.1. Soient K un corps, $\overline{K}$ une clôture algébrique de K, et L une extension de K contenue dans $\overline{K}$. On pose

$$L_K \underset{\text{def}}{=} \{\, x \in L \mid \forall\, \sigma \in \mathrm{Hom}_K(L, \overline{K}),\, \sigma x = x \,\}.$$

1. Montrer que L_K est un sous-corps de L contenant K.
2. On suppose que L/K est séparable. Montrer que $L_K = K$.
3. Soient $\mathbb{K}$ un corps de caractéristique p et $x \in \mathbb{K}$ transcendant sur $\mathbb{F}_p$. Soient $K = \mathbb{F}_p(x^p)$ et $L = \mathbb{F}_p(x)$. Montrer que $L_K = L$ (cf. exercice 5.3).

Exercice 4.2 (Indépendance linéaire des caractères)**.** Soient Γ un groupe, K un corps, $n \geq 1$ un entier, et $\chi_1, \ldots, \chi_n$ des morphismes distincts de Γ dans $K^\times$.

1. Montrer que l'ensemble des applications de Γ dans K est un K-espace vectoriel.
2. On suppose qu'il existe $a_1, \ldots, a_n \in K$ non tous nuls tels que $a_1\chi_1 + \ldots + a_n\chi_n = 0$ et que n est le plus petit entier pour lequel il existe une telle relation de dépendance.
   (a) Montrer que $n \geq 2$ et que $a_i \neq 0$ pour tout $1 \leq i \leq n$.
   (b) Montrer qu'il existe $h \in \Gamma$ tel que $\chi_1(h) \neq \chi_2(h)$.
   (c) Montrer que $a_1\chi_1(h)\chi_1 + \ldots + a_n\chi_n(h)\chi_n = 0$.
   (d) Montrer que $a_2(\chi_2(h)\chi_1(h)^{-1} - 1)\chi_2 + \ldots + a_n(\chi_n(h)\chi_1(h)^{-1} - 1)\chi_n = 0$.
3. Montrer que $\chi_1, \ldots, \chi_n$ sont linéairement indépendants sur K.

Exercice 4.3. Soient K un corps et $x_1, \ldots, x_n \in K^\times$ distincts. Soient $a_1, \ldots, a_n \in K$ tels que $a_1x_1^m + \ldots + a_nx_n^m = 0$ pour tout $m \in \mathbb{Z}$. Montrer que $a_1 = \ldots = a_n = 0$. (cf. exercice 4.2).

Définition 4. Soient K un corps, $\overline{K}$ une clôture algébrique de K, et L une extension finie de K contenue dans $\overline{K}$. Pour tout $x \in L$ on définit les éléments de $\overline{K}$

$$\mathrm{Tr}_{L/K}(x) \underset{\text{def}}{=} \sum_{\sigma \in \mathrm{Hom}_K(L, \overline{K})} \sigma(x) \qquad \text{et} \qquad N_{L/K}(x) \underset{\text{def}}{=} \prod_{\sigma \in \mathrm{Hom}_K(L, \overline{K})} \sigma(x).$$

Exercice 4.4. Soient K un corps, $\overline{K}$ une clôture algébrique de K, et L une extension finie et séparable de K contenue dans $\overline{K}$. Montrer que l'application $\mathrm{Tr}_{L/K} : L \to \overline{K}$ n'est pas nulle. (cf. exercice 4.2).

Exercice 4.5. Soient K un corps, $\overline{K}$ une clôture algébrique de K, et L une extension finie et séparable de K contenue dans $\overline{K}$.

1. Soit $x \in L$. Montrer que $\mathrm{Tr}_{L/K}(x) \in K$ et $N_{L/K}(x) \in K$ (considérer le corps de décomposition E du polynôme minimal de x sur K et montrer que $\mathrm{Tr}_{L/K}(x) \in E_K$ et $N_{L/K}(x) \in E_K$, cf. exercice 4.1).
2. Montrer que l'application $N_{L/K} : L^\times \to K^\times$ est un morphisme de groupes et que l'application $\mathrm{Tr}_{L/K} : L \to K$ est K-linéaire.
3. Soient $x \in L$ et $X^n + a_{n-1}X^{n-1} + \ldots + a_1X + a_0 \in K[X]$ son polynôme minimal sur K. Montrer que $\mathrm{Tr}_{K(x)/K}(x) = -a_{n-1}$ et $N_{K(x)/K}(x) = (-1)^n a_0$.
4. Soit M une extension finie et séparable de L contenue dans $\overline{K}$. Montrer que $\mathrm{Tr}_{M/K} = \mathrm{Tr}_{L/K} \circ \mathrm{Tr}_{M/L}$ et $N_{M/K} = N_{L/K} \circ N_{M/L}$.
5. Soient $x \in L$ et $\mu_x : L \to L$ l'application K-linéaire de multiplication par x. Montrer que $\mathrm{Tr}_{L/K}(x) = \mathrm{Tr}\,\mu_x$ et $N_{L/K}(x) = \det \mu_x$.

Exercice 4.6. Soient $K = \mathbb{Q}(\sqrt{2}) \subset \overline{\mathbb{Q}}$ et $\sigma \in \mathrm{Aut}_{\mathbb{Q}}(K)$ donné par $\sigma(\sqrt{2}) = -\sqrt{2}$.

1. Montrer que l'extension $K/\mathbb{Q}$ est séparable de degré 2.
2. Montrer que $\mathrm{Hom}_{\mathbb{Q}}(K, \overline{\mathbb{Q}}) = \mathrm{Aut}_{\mathbb{Q}}(K) = \langle\sigma\rangle$.
3. (a) Soient $x, y \in \mathbb{Q}$. Montrer que $N_{K/\mathbb{Q}}(x + y\sqrt{2}) = x^2 - 2y^2$.
   (b) Montrer que $N_{K/\mathbb{Q}}(2 \pm \sqrt{2}) = 2$ et $N_{K/\mathbb{Q}}(7 \pm 5\sqrt{2}) = -1$.
   (c) Montrer que $6 \in N_{K/\mathbb{Q}}(K^\times)$ si et seulement si $3 \in N_{K/\mathbb{Q}}(K^\times)$.
   (d) Montrer que $-6 \in N_{K/\mathbb{Q}}(K^\times)$ si et seulement si $3 \in N_{K/\mathbb{Q}}(K^\times)$.
4. Montrer que $3 \in N_{K/\mathbb{Q}}(K^\times)$ si et seulement si il existe $a, b \in \mathbb{Z}$ premiers entre eux tels que $2a^2 + 3b^2$ est un carré dans $\mathbb{Z}$.
5. Soient $a, b, c \in \mathbb{Z}$ tels que $2a^2 + 3b^2 = c^2$.
   (a) Montrer que $-a^2$ est un carré dans $\mathbb{Z}/3\mathbb{Z}$.
   (b) Montrer que 3 divise a.
   (c) On suppose que l'un des a, b, c est non nul. Montrer que $abc \neq 0$.
   (d) On suppose que $abc \neq 0$. Soit $\pm d = \mathrm{pgcd}(a, b)$. Montrer que $cd^{-1} \in 3\mathbb{Z}$.
   (e) Montrer que $a = b = c = 0$.
6. Montrer qu'aucun des éléments suivants ne sont dans $N_{K/\mathbb{Q}}(K^\times)$: $\pm 3, \pm 6, \pm 12$.

Exercice 4.7. Soit L/K une extension séparable de degré n.

1. Montrer que l'application $L \times L \to K$, $(\alpha, \beta) \mapsto \mathrm{Tr}_{L/K}(\alpha\beta)$ est une forme K-bilinéaire symétrique non dégénérée.
2. Soit $(\alpha_1, \ldots, \alpha_n)$ une base de L sur K. Montrer qu'il existe une unique base $(\alpha_1^*, \ldots, \alpha_n^*)$ de L sur K telle que pour tous $1 \leq i, j \leq n$ on a $\mathrm{Tr}_{L/K}(\alpha_i\alpha_i^*) = 1$ et $\mathrm{Tr}_{L/K}(\alpha_i\alpha_j^*) = 0$ si $i \neq j$.
3. Soient $K = \mathbb{Q}$, $L = \mathbb{Q}(\sqrt{2})$ et $(\alpha_1, \alpha_2) = (1, \sqrt{2})$. Calculer (α_1^*, α_2^*) (cf. exercice 4.5).

5. Caractéristique p

Exercice 5.1. Soit F un corps de caractéristique p.

1. Montrer que le morphisme de groupes $F^\times \to F^\times$, $\alpha \mapsto \alpha^p$ est injectif.
2. Montrer que le morphisme de corps $\sigma : F \to F$, $\alpha \mapsto \alpha^p$ est injectif.
3. Donner un exemple de corps F avec σ non surjectif.

Exercice 5.2. Soit F un corps de caractéristique p. Soit $a \in F$. Montrer que $X^p - a$ est irréductible dans $F[X]$ si et seulement si $a \notin F^p = \{x^p,\, x \in F\}$.

Exercice 5.3. Soient $\mathbb{K}$ un corps de caractéristique p et $x \in \mathbb{K}$ transcendant sur $\mathbb{F}_p$. Soient $K = \mathbb{F}_p(x^p)$ et $\overline{K}$ une clôture algébrique de $K(x)$.

1. Montrer que $K(x) = \mathbb{F}_p(x)$ et que x est algébrique sur K.
2. Montrer que $X^p - x^p$ est le polynôme minimal de x sur K.
3. Montrer que $[K(x) : K] = p$ et que $K(x)/K$ n'est pas séparable.
4. Montrer que $\mathrm{Hom}_K(K(x), \overline{K})$ est réduit à l'inclusion de $K(x)$ dans $\overline{K}$.

Exercice 5.4. Soit $\mathbb{K}$ un corps de caractéristique p. Soient $x, y \in \mathbb{K}$ algébriquement indépendants sur $\mathbb{F}_p$ (cf. définition 3) et $K = \mathbb{F}_p(x^p, y^p)$, $L = \mathbb{F}_p(x, y)$.

1. Montrer que $[L : K] = p^2$.
2. Soit $f \in \mathbb{F}_p(X, Y)$. Montrer que $f(x, y) \in L$ est racine de $X^p - f(x^p, y^p) \in K[X]$.
3. Soient $f, g \in \mathbb{F}_p(X, Y)$ tels que $\mathbb{F}_p(f) = \mathbb{F}_p(g)$. Montrer que $f(x^p, y^p) = g(x^p, y^p)$.
4. Soit $L^p = \{z^p,\, z \in L\}$. Montrer que $L \setminus L^p$ est infini.
5. Montrer qu'il existe une infinité d'extensions entre K et L.
6. Montrer que l'extension L/K n'est pas simple.

Exercice 5.5. Soient F un corps de caractéristique p et K/F une extension finie de degré premier à p. Montrer que K/F est séparable.

Exercice 5.6. Soient F un corps de caractéristique p, $\overline{F}$ une clôture algébrique de F, et $\alpha \in \overline{F}$. Montrer que α est séparable si et seulement si $K(\alpha) = K(\alpha^{p^n})$ pour tout $n \in \mathbb{N}$.

Exercice 5.7. Soit F un corps de caractéristique p. Montrer que les assertions suivantes sont équivalentes.

(i) Toute extension algébrique de F est séparable.
(ii) Le morphisme de corps $F \to F$, $x \mapsto x^p$ est surjectif.

6. Corps finis

Exercice 6.1. Soit F un corps fini de caractéristique p. Montrer que le morphisme de corps $F \to F$, $x \mapsto x^p$ est bijectif.

Exercice 6.2. Soit E/F une extension de corps finis. Montrer qu'il existe $\alpha \in E$ tel que $E = F(\alpha)$.

Exercice 6.3. Soient F un corps fini à q éléments et $\mathcal{A}(F)$ l'anneau commutatif des applications de F dans F. Soit l'application $\phi : F[X] \to \mathcal{A}(F)$, $P(X) \mapsto f_P : F \to F$, $x \mapsto P(x)$.

1. Montrer que ϕ est un morphisme d'anneau.
2. Montrer que $\mathrm{Ker}\,\phi = (X^q - X)$.

Exercice 6.4. Soit F un corps fini à q éléments. Soient $C = \{x^2,\, x \in F\}$ l'ensemble des carrés de F et $N = \{x \in F \mid x \notin C\}$ l'ensemble des non-carrés de F.

1. On suppose que q est pair. Montrer que $C = F$.
2. On suppose que q est impair.
   (a) Montrer que $C^\times = \{x^2,\, x \in F^\times\}$ est un sous-groupe d'indice 2 de $F^\times$.
   (b) Montrer que $\#N = \frac{q-1}{2}$ et $\#C = \frac{q+1}{2}$.
   (c) Soit $\delta \in F^\times$ tel que $\delta \notin C^\times$. Montrer qu'il existe $c \in C$ tel que $\delta - c \in C$ (considérer l'application $C \to F, c \mapsto \delta - c$).
3. Montrer que tout élément de F est la somme de deux carrés de F.

Exercice 6.5 (Un cas particulier du théorème de la progression arithmétique de Dirichlet)**.**

1. Soit F un corps fini à q éléments avec q impair.
   (a) Soit $x \in F^\times$. Montrer que x est un carré dans F si et seulement si $x^{\frac{q-1}{2}} = 1$.
   (b) Montrer que -1 est un carré dans F si et seulement si $q \equiv 1 \bmod 4\mathbb{Z}$.
2. Soient $n \geq 2$ un entier et p un nombre premier divisant $(n!)^2 + 1$.
   (a) Montrer que $p > n$.
   (b) Montrer que $p \equiv 1 \bmod 4\mathbb{Z}$.
3. Montrer qu'il existe une infinité de nombres premiers de la forme $1 + 4m$, $m \in \mathbb{N}$.

Exercice 6.6 (Résidus quadratiques)**.** Soit $p \neq 2$ et $(\mathbb{F}_p^\times)^2 = \{x^2,\, x \in \mathbb{F}_p^\times\}$. Pour $x \in \mathbb{F}_p^\times$ on définit le symbole quadratique de x par

$$\left(\frac{x}{p}\right) \underset{\text{def}}{=} \begin{cases} +1 & \text{si } x \in (\mathbb{F}_p^\times)^2 \\ -1 & \text{si } x \notin (\mathbb{F}_p^\times)^2. \end{cases}$$

1. Montrer que $(\mathbb{F}_p^\times)^2$ est un sous-groupe d'indice 2 de $\mathbb{F}_p^\times$.
2. Montrer que l'application $\rho : \mathbb{F}_p^\times \to \mathbb{F}_p^\times$, $x \mapsto \left(\frac{x}{p}\right)$ est un morphisme de groupe et que $\operatorname{Im}\rho = \{\pm 1\}$, $\operatorname{Ker}\rho = (\mathbb{F}_p^\times)^2$.
3. Soit $x \in \mathbb{F}_p^\times$. Montrer que $\left(\frac{x}{p}\right) = x^{\frac{p-1}{2}}$.
4. Montrer que $\sum_{x \in \mathbb{F}_p^\times} \left(\frac{x}{p}\right) = 0$.

Exercice 6.7 (Clôture algébrique de $\mathbb{F}_p$)**.** Soient $m \leq n \in \mathbb{N}$ et $q \neq 1$ une puissance de p.

1. Montrer que $\left(\overline{\mathbb{F}}_p^\times\right)_{\text{tors}} = \overline{\mathbb{F}}_p^\times$.
2. Montrer que $\mathbb{F}_{p^{m!}} \subseteq \mathbb{F}_{p^{n!}}$.
3. Montrer qu'il existe $n \in \mathbb{N}$ tel que $\mathbb{F}_q \subseteq \mathbb{F}_{p^{n!}}$.
4. Montrer que $\overline{\mathbb{F}}_p = \bigcup_{n \in \mathbb{N}} \mathbb{F}_{p^{n!}}$.

Exercice 6.8. Soit $\alpha \in \overline{\mathbb{F}}_2$. Montrer que $[\mathbb{F}_2(\alpha) : \mathbb{F}_2] = 2$ si et seulement si $\alpha^2 + \alpha + 1 = 0$.

Exercice 6.9. Soient $\alpha, \beta \in \overline{\mathbb{F}}_3$ tels que $\alpha^2 + 1 = \beta^2 - \beta - 1 = 0$. Montrer que $\mathbb{F}_3(\alpha) = \mathbb{F}_3(\beta)$.

Exercice 6.10. Soit $\alpha \in \overline{\mathbb{F}}_p$ une racine de $X^4 + 51X^3 + 11X^2 + 21X + 1 \in \mathbb{F}_p[X]$. Calculer $[\mathbb{F}_p(\alpha) : \mathbb{F}_p]$ pour $p = 2, 3, 5$.

Exercice 6.11. Soit $\zeta \in \overline{\mathbb{F}}_p$ une racine de $X^4 + 1$. Calculer $[\mathbb{F}_p(\zeta) : \mathbb{F}_p]$ pour $p = 2, 3, 5$.

Exercice 6.12. Soit $P(X) = X^p - X + 1 \in \mathbb{F}_p[X]$.

1. Montrer que $P(X)$ est séparable.

2. Soit $\alpha \in \overline{\mathbb{F}}_p$ tel que $P(\alpha) = 0$. Soit $a \in \mathbb{F}_p$. Montrer que $P(\alpha + a) = 0$.
3. Montrer que $P(X)$ est irréductible dans $\mathbb{F}_p[X]$.
4. Montrer que $P(X)$ divise $X^{p^p} - X$ dans $\mathbb{F}_p[X]$.

Exercice 6.13. Soient F un corps fini à q éléments et $n \geq 1$ un entier.

1. Soit $P(X) \in F[X]$ irréductible. Montrer que $P(X)$ divise $X^{q^n} - X$ dans $F[X]$ si et seulement si $\deg P$ divise n.
2. Pour tout $d \geq 1$ entier soit $\mathcal{I}_d$ l'ensemble des polynômes unitaires irréductibles de degré d à coefficients dans F. Montrer que

$$X^{q^n} - X = \prod_{d|n} \prod_{P_d \in \mathcal{I}_d} P_d(X).$$

Exercice 6.14. Soient $\mathbb{F}_q$ et $\mathbb{F}_{q^n}$ les sous-corps de $\overline{\mathbb{F}}_p$ à q et q^n éléments respectivement. Soient $\sigma \in \mathrm{Aut}_{\mathbb{F}_q}(\mathbb{F}_{q^n})$ le Frobenius donné par $x \mapsto x^q$ et $N : \mathbb{F}_{q^n}^\times \to \mathbb{F}_q^\times$ la norme de $\mathbb{F}_{q^n}$ à $\mathbb{F}_q$ (cf. définition 4 et exercice 4.5).

1. Montrer que $\mathrm{Hom}_{\mathbb{F}_q}(\mathbb{F}_{q^n}, \overline{\mathbb{F}}_p) = \mathrm{Aut}_{\mathbb{F}_q}(\mathbb{F}_{q^n}) = \langle \sigma \rangle$.
2. Soit $x \in \mathbb{F}_{q^n}^\times$. Montrer que $N(x) = x^{(q^n-1)/(q-1)}$.
3. Soit x un générateur de $\mathbb{F}_{q^n}^\times$. Montrer que $\mathrm{ord}\big(x^{(q^n-1)/(q-1)}\big) = q - 1$.
4. Montrer que la norme de $\mathbb{F}_{q^n}$ à $\mathbb{F}_q$ est surjective.
5. Soit $(\mathbb{F}_{q^n}^\times)^{q-1} = \{y^{q-1},\, y \in \mathbb{F}_{q^n}^\times\}$. Montrer que $|(\mathbb{F}_{q^n}^\times)^{q-1}| = \frac{q^n-1}{q-1}$.
6. Montrer que $\mathrm{Ker}\, N = (\mathbb{F}_{q^n}^\times)^{q-1}$.

Exercice 6.15. Soient $\mathbb{F}_q$ et $\mathbb{F}_{q^n}$ les sous-corps de $\overline{\mathbb{F}}_p$ à q et q^n éléments respectivement. Soient $\sigma \in \mathrm{Aut}_{\mathbb{F}_q}(\mathbb{F}_{q^n})$ le Frobenius donné par $x \mapsto x^q$ et $\mathrm{Tr} : \mathbb{F}_{q^n} \to \mathbb{F}_q$ la trace de $\mathbb{F}_{q^n}$ à $\mathbb{F}_q$ (cf. définition 4 et exercice 4.5).

1. Montrer que $\mathrm{Im}\, \mathrm{Tr} = \mathbb{F}_q$ et $\dim_{\mathbb{F}_q}(\mathrm{Ker}\, \mathrm{Tr}) = n - 1$.
2. Montrer que $\mathrm{Im}(\sigma - \mathrm{Id}) \subseteq \mathrm{Ker}\, \mathrm{Tr}$.
3. Montrer que $\mathrm{Ker}(\sigma - \mathrm{Id}) = \mathbb{F}_q$.
4. Montrer que $\mathrm{Ker}\, \mathrm{Tr} = \mathrm{Im}(\sigma - \mathrm{Id})$.

Exercice 6.16. Soient $\mathbb{F}_q$ et $\mathbb{F}_{q^n}$ les sous-corps de $\overline{\mathbb{F}}_p$ à q et q^n éléments respectivement. Soit $f : \mathbb{F}_{q^n} \to \mathbb{F}_{q^n}$ une application $\mathbb{F}_q$-linéaire. Montrer que f est diagonalisable si et seulement si son polynôme minimal divise $X^q - X$ dans $\mathbb{F}_q[X]$.

Exercice 6.17. Soient $\mathbb{F}_q$ et $\mathbb{F}_{q^n}$ les sous-corps de $\overline{\mathbb{F}}_p$ à q et q^n éléments respectivement. Soit $\sigma \in \mathrm{Aut}_{\mathbb{F}_q}(\mathbb{F}_{q^n})$ l'automorphisme de Frobenius donné par $\sigma(x) = x^q$ pour tout $x \in \mathbb{F}_{q^n}$.

1. Montrer que le polynôme minimal de l'application $\mathbb{F}_q$-linéaire σ est $X^n - 1$ (cf. exercice 4.2).
2. Montrer qu'il existe $\alpha \in \mathbb{F}_{q^n}$ tel que $\big(\alpha, \sigma(\alpha), \ldots, \sigma^{n-1}(\alpha)\big)$ est une base de $\mathbb{F}_{q^n}$ sur $\mathbb{F}_q$. Donner la matrice de σ dans cette base.
3. Montrer que l'application $\mathbb{F}_q$-linéaire σ est diagonalisable si et seulement si n divise $q - 1$ (cf. exercice 6.16).

7. Racines de l'unité

Exercice 7.1. Soit K un corps. Pour tout entier $n \geq 1$ on pose

$$\mu_n(K) \underset{\text{def}}{=} \{x \in K \mid x^n = 1\}.$$

1. Soit $x \in \mu_n(K)$ tel que $x \neq 1$. Montrer que $x^{n-1} + \ldots + x + 1 = 0$.
2. Montrer que $\mu_n(K)$ est un sous-groupe fini de $K^\times$ d'ordre divisant n.
3. Montrer que $\mu_n(K)$ est cyclique.
4. Soit m premier à n. Montrer que $\mu_{nm}(K) \simeq \mu_n(K) \times \mu_m(K)$.
5. On suppose K de caractéristique p. Montrer que $\mu_{p^k}(K) = \{1\}$ pour tout $k \geq 0$.

Définition 5. Soient K un corps et $n \geq 1$ un entier. Une *racine n-ième de l'unité* dans K est une racine de $X^n - 1$ dans K, i.e. un élément du groupe $\mu_n(K)$. Une racine *primitive* n-ième de l'unité dans K est un générateur du groupe cyclique $\mu_n(K)$.

Exercice 7.2. Soient K un corps et $n \geq 1$ un entier impair tels que K contient une racine primitive n-ième de l'unité. Montrer que K contient une racine primitive $2n$-ième de l'unité.

Exercice 7.3. Soient K un corps, $\overline{K}$ une clôture algébrique de K, $n \geq 1$ un entier, et $\zeta_n \in \overline{K}$ une racine primitive n-ième de l'unité.

1. Montrer que $K(\zeta_n) = K\big(\mu_n(\overline{K})\big)$.
2. Montrer que $\mathrm{Hom}_K\big(K(\zeta_n), \overline{K}\big) = \mathrm{Aut}_K\big(K(\zeta_n)\big)$.
3. Soit $\sigma \in \mathrm{Aut}_K\big(K(\zeta_n)\big)$. Montrer que $\sigma(\zeta_n)$ est une racine primitive n-ième de l'unité.
4. Montrer que $\mathrm{Aut}_K\big(K(\zeta_n)\big)$ est un sous-groupe de $\mathrm{Aut}\big(\mu_n(\overline{K})\big)$.
5. Montrer que toute racine dans $\overline{K}$ du polynôme minimal de ζ_n sur K est une racine primitive n-ième de l'unité.

Exercice 7.4. Soient $\overline{K}$ un corps algébriquement clos, $n \geq 1$ un entier premier à la caractéristique de $\overline{K}$, et $\zeta_n \in \overline{K}$ une racine primitive n-ième de l'unité.

1. Montrer que $|\mu_n(\overline{K})| = n$.
2. Soit $i \in \mathbb{Z}$. Montrer que ζ_n^i est une racine primitive n-ième de l'unité si et seulement si i est premier à n.
3. Montrer que l'application $\mathbb{Z} \to \mathrm{End}\big(\mu_n(\overline{K})\big)$, $i \mapsto [\zeta_n \mapsto \zeta_n^i]$ induit un isomorphisme de groupes $(\mathbb{Z}/n\mathbb{Z})^\times \simeq \mathrm{Aut}(\mu_n(\overline{K}))$.

Définition 6. Soit $n \geq 1$ un entier. Le *n-ième polynôme cyclotomique* $\Phi_n(X)$ est le polynôme minimal sur $\mathbb{Q}$ d'une racine primitive n-ième de l'unité dans $\overline{\mathbb{Q}}$.

Exercice 7.5. Soient $n \geq 1$ un entier et $\zeta_n \in \overline{\mathbb{Q}}$ une racine primitive n-ième de l'unité.

1. Montrer qu'il existe $\Psi(X) \in \mathbb{Q}[X]$ tel que $X^n - 1 = \Psi(X)\Phi_n(X)$.
2. Montrer que $\Psi(X) \in \mathbb{Z}[X]$ et $\Phi_n(X) \in \mathbb{Z}[X]$.
3. Soit p un nombre premier. On suppose que $\Phi_n(\zeta_n^p) \neq 0$.
   (a) Montrer qu'il existe $P(X) \in \mathbb{Z}[X]$ tel que $\Psi(X^p) = \Phi_n(X)P(X)$.
   (b) Montrer que $\Psi(X)^p \equiv \Phi_n(X)P(X) \bmod p\mathbb{Z}[X]$.
   (c) Montrer que $X^n - 1$ a une racine multiple dans une clôture algébrique de $\mathbb{F}_p$.
   (d) Montrer que p divise n.
4. Soit p un nombre premier ne divisant pas n. Montrer que $\Phi_n(\zeta_n^p) = 0$.

5. Soit $i \in \mathbb{Z}$ premier à n. Montrer que $\Phi_n(\zeta_n^i) = 0$.
6. Montrer que
$$\Phi_n(X) = \prod_{i \in (\mathbb{Z}/n\mathbb{Z})^\times} (X - \zeta_n^i).$$
7. Montrer que $[\mathbb{Q}(\zeta_n) : \mathbb{Q}] = |(\mathbb{Z}/n\mathbb{Z})^\times|$ et que $\Phi_n(X)$ est irréductible dans $\mathbb{Q}[X]$.

Exercice 7.6. Pour tout $n \geq 1$ entier soit $\zeta_n \in \overline{\mathbb{Q}}$ une racine primitive n-ième de l'unité.

1. Déterminer les n tels que $\mathbb{Q}(\zeta_n) \subset \mathbb{R}$.
2. Déterminer les n tels que $[\mathbb{Q}(\zeta_n) : \mathbb{Q}] = 2$.

Exercice 7.7. Soient $n, m \geq 2$ des entiers premiers entre eux et $\zeta_n, \zeta_m \in \overline{\mathbb{Q}}$ des racines primitives n-ième et m-ième de l'unité.

1. Montrer que $\mathbb{Q}(\zeta_n^m) = \mathbb{Q}(\zeta_n)$ et $\mathbb{Q}(\zeta_m^n) = \mathbb{Q}(\zeta_m)$.
2. Montrer que $\mathbb{Q}(\zeta_n, \zeta_m) = \mathbb{Q}(\zeta_n\zeta_m)$.
3. Montrer que $\zeta_n\zeta_m$ est une racine primitive nm-ième de l'unité.
4. Montrer que $[\mathbb{Q}(\zeta_n\zeta_m) : \mathbb{Q}] = [\mathbb{Q}(\zeta_n) : \mathbb{Q}]\,[\mathbb{Q}(\zeta_m) : \mathbb{Q}]$.
5. Montrer que $\mathbb{Q}(\zeta_n)$ et $\mathbb{Q}(\zeta_m)$ sont linéairement disjointes sur $\mathbb{Q}$ (cf. Définition 2).

Exercice 7.8. Soient $n, k \geq 1$ deux entiers et p un nombre premier.

1. Montrer que $X^n - 1 = \prod_{d|n} \Phi_d(X)$.
2. Montrer que $\Phi_p(X) = X^{p-1} + X^{p-2} + \ldots + X + 1$.
3. Montrer que $\Phi_{p^k}(X) = \Phi_p\big(X^{p^{k-1}}\big)$.
4. Soit $n = p_1^{k_1} \ldots p_r^{k_r}$ la décomposition de n en puissances de premiers distincts. Montrer que $\Phi_n(X) = \Phi_{p_1 \ldots p_r}\big(X^{p_1^{k_1-1} \ldots\, p_r^{k_r-1}}\big)$.
5. On suppose que n est impair. Montrer que $\Phi_{2n}(X) = \Phi_n(-X)$.
6. On suppose que p ne divise pas n. Montrer que $\Phi_{pn}(X) = \frac{\Phi_n(X^p)}{\Phi_n(X)}$.

Exercice 7.9. Montrer que

$$\begin{array}{ll}
\Phi_1(X) = X - 1 & \Phi_6(X) = X^2 - X + 1 \\
\Phi_2(X) = X + 1 & \Phi_7(X) = X^6 + X^5 + X^4 + X^3 + X^2 + X + 1 \\
\Phi_3(X) = X^2 + X + 1 & \Phi_8(X) = X^4 + 1 \\
\Phi_4(X) = X^2 + 1 & \Phi_9(X) = X^6 + X^3 + 1 \\
\Phi_5(X) = X^4 + X^3 + X^2 + X + 1 & \Phi_{10}(X) = X^4 - X^3 + X^2 - X + 1.
\end{array}$$

Exercice 7.10. Soit $n \geq 2$ entier et $\zeta_n \in \overline{\mathbb{Q}}$ une racine primitive n-ième de l'unité. Soient $N_{\mathbb{Q}(\zeta_n)/\mathbb{Q}}$ et $\mathrm{Tr}_{\mathbb{Q}(\zeta_n)/\mathbb{Q}}$ la norme et la trace de $\mathbb{Q}(\zeta_n)$ à $\mathbb{Q}$ (cf. définition 4 et exercice 4.5).

1. Montrer que $N_{\mathbb{Q}(\zeta_n)/\mathbb{Q}}(\zeta_n) = 1$.
2. On suppose que $n = p$ est premier.
   (a) Montrer que $\mathrm{Tr}_{\mathbb{Q}(\zeta_p)/\mathbb{Q}}(\zeta_p) = -1$.
   (b) Montrer que $N_{\mathbb{Q}(\zeta_p)/\mathbb{Q}}(\zeta_p - 1) = p$.

Exercice 7.11. Soit K une extension finie de $\mathbb{Q}$.

1. Montrer que $(K^\times)_{\mathrm{tors}}$ est fini.
2. Déterminer $(K^\times)_{\mathrm{tors}}$ pour $K = \mathbb{Q}(i), \mathbb{Q}(\sqrt{-2}), \mathbb{Q}(\sqrt{2}), \mathbb{Q}(\sqrt{-3}), \mathbb{Q}(\sqrt{3}), \mathbb{Q}(\sqrt{-5})$.

Exercice 7.12 (Sommes de Gauss)**.** Soit $p \neq 2$ premier et $\zeta_p \in \overline{\mathbb{Q}}$ une racine primitive p-ième de l'unité. Soit $\left(\frac{x}{p}\right) = x^{\frac{p-1}{2}} \in \{\pm 1\}$ le symbole quadratique en $x \in \mathbb{F}_p^\times$ (exercice 6.6). On pose

$$\delta = \sum_{n \in \mathbb{F}_p^\times} \left(\frac{n}{p}\right) \zeta_p^n \quad \in \mathbb{Q}(\zeta_p).$$

1. Montrer que $\delta^2 = \sum_{n,m \in \mathbb{F}_p^\times} \left(\frac{nm}{p}\right) \zeta_p^{n+m}$ (cf. exercice 6.6).
2. Montrer que $\delta^2 = \sum_{n,m \in \mathbb{F}_p^\times} \left(\frac{n}{p}\right) \zeta_p^{m(n+1)}$ (considérer $(n,m) \mapsto (nm, m)$).
3. Soit $n \in \mathbb{F}_p^\times$ tel que $n \neq -1$. Montrer que $\sum_{m \in \mathbb{F}_p^\times} \zeta_p^{m(n+1)} = -1$.
4. Montrer que $\delta^2 = \left(\frac{-1}{p}\right) p$ (cf. exercice 6.6).
5. Montrer que $\mathbb{Q}\left(\sqrt{(-1)^{\frac{p-1}{2}} p}\right) \subseteq \mathbb{Q}(\zeta_p)$.
6. Soit ζ_4 une racine primitive quatrième de l'unité. Montrer que $\mathbb{Q}(\sqrt{p}) \subseteq \mathbb{Q}(\zeta_p, \zeta_4)$.

Exercice 7.13. Soient $n \geq 2$ un entier premier à p et $\zeta_n \in \overline{\mathbb{F}}_p$ une racine primitive n-ième de l'unité. Montrer que $[\mathbb{F}_p(\zeta_n) : \mathbb{F}_p] = \operatorname{ord}_{(\mathbb{Z}/n\mathbb{Z})^\times}(p \bmod n\mathbb{Z})$.

Exercice 7.14. Soient $p \neq 2$ premier, $\mathbb{F}_{p^2}$ le sous-corps de $\overline{\mathbb{F}}_p$ à p^2 éléments, et $\zeta_8 \in \overline{\mathbb{F}}_p$ une racine primitive huitième de l'unité.

1. Montrer que 8 divise $p^2 - 1$.
2. Montrer que $\zeta_8 \in \mathbb{F}_{p^2}$.
3. Montrer que $\zeta_8 \in \mathbb{F}_p$ si et seulement si 8 divise $p - 1$.
4. Montrer que $\zeta_8 + \zeta_8^{-1} = 2$.
5. Montrer que 2 est un carré dans $\mathbb{F}_p$ si et seulement si $p \equiv \pm 1 \bmod 8\mathbb{Z}$.

Exercice 7.15. Soit p premier tel que $2^{p-1} \equiv 1 \bmod p^2\mathbb{Z}$ (par exemple $p = 1093, 3511$). Soit $\zeta_{p^2} \in \overline{\mathbb{F}}_2$ une racine primitive p^2-ième de l'unité.

1. Montrer que $[\mathbb{F}_2(\zeta_{p^2}) : \mathbb{F}_2] \leq p - 1$.
2. Montrer que $\Phi_{p^2}(X)$ est réductible dans $\mathbb{F}_2[X]$.

8. Normalité

Exercice 8.1. Déterminer le corps de décomposition dans $\overline{\mathbb{Q}}$ sur $\mathbb{Q}$ des polynômes suivants et calculer son degré sur $\mathbb{Q}$.

1. (a) $X^4 - 5X^2 + 6$ (b) $X^4 + 5X^2 + 6$ (c) $X^4 - 5$.
2. (a) $X^4 + 1$ (b) $X^4 + 4$ (c) $(X^4 + 1)(X^4 + 4)$ (d) $(X^4 - 1)(X^4 + 4)$.
3. (a) $X^2 - 2$ (b) $X^2 - 1$ (c) $X^3 - 2$ (d) $(X^3 - 2)(X^2 - 2)$.
4. (a) $X^2 + X + 1$ (b) $X^6 + X^3 + 1$ (c) $X^5 - 7$.

Exercice 8.2. Soient $n \geq 2$ entier et $a \in \mathbb{Q}$ tels que $X^n - a$ est irréductible dans $\mathbb{Q}[X]$. Soient $K \subset \overline{\mathbb{Q}}$ le corps de décomposition de $X^n - a$ sur $\mathbb{Q}$, $\sqrt[n]{a} \in \overline{\mathbb{Q}}$ une racine de $X^n - a$, et $\zeta_n \in \overline{\mathbb{Q}}$ une racine primitive n-ième de l'unité (cf. section 7).

1. Montrer que $K = \mathbb{Q}(\sqrt[n]{a}, \zeta_n)$.
2. Montrer que $n \leq [K : \mathbb{Q}] \leq n(n-1)$.
3. Calculer $[K : \mathbb{Q}]$ lorsque n est un nombre premier.

Exercice 8.3. Déterminer le corps de décomposition de $X^3 - 5$ sur $\mathbb{F}_p$ pour $p = 2, 3, 5, 7$.

Exercice 8.4. Soit $n \geq 1$ entier tel que n et $p-1$ sont premiers entre eux. Montrer que les polynômes $X^n - a$, avec $a \in \mathbb{F}_p^\times$, ont tous le même corps de décomposition sur $\mathbb{F}_p$.

Exercice 8.5. Soit L/K une extension de degré 2. Montrer que L/K est normale.

Exercice 8.6. Montrer que les extensions $\mathbb{Q}(\sqrt{2})/\mathbb{Q}$ et $\mathbb{Q}(\sqrt[4]{2})/\mathbb{Q}(\sqrt{2})$ sont normales et que $\mathbb{Q}(\sqrt[4]{2})/\mathbb{Q}$ ne l'est pas.

Exercice 8.7. Montrer que les extensions $\mathbb{Q}(\sqrt{3})/\mathbb{Q}$ et $\mathbb{Q}\big(\sqrt{\sqrt{3}+1}\big)/\mathbb{Q}(\sqrt{3})$ sont normales et que $\mathbb{Q}\big(\sqrt{\sqrt{3}+1}\big)/\mathbb{Q}$ ne l'est pas.

Exercice 8.8. Soient $\alpha \in \mathbb{R}$ tel que $\alpha^4 = 5$ et $i \in \mathbb{C}$ tel que $i^2 = -1$.

1. Montrer que $\mathbb{Q}(i\alpha^2)$ est normale sur $\mathbb{Q}$.
2. Montrer que $\mathbb{Q}(\alpha + i\alpha)$ est normale sur $\mathbb{Q}(i\alpha^2)$.
3. Montrer que $\mathbb{Q}(\alpha + i\alpha)$ n'est pas normale sur $\mathbb{Q}$.

Exercice 8.9. Soit $\zeta_3 \in \overline{\mathbb{Q}}$ une racine primitive troisième de l'unité.

1. Montrer que l'extension $\mathbb{Q}(\sqrt[3]{5})/\mathbb{Q}$ n'est pas normale.
2. Montrer que l'extension $\mathbb{Q}(\sqrt[3]{5}, \zeta_3)/\mathbb{Q}$ est normale.

Exercice 8.10. Soit K un corps tel que toute extension de K dans une clôture algébrique $\overline{K}$ est séparable. Soit L une extension finie de K dans $\overline{K}$. Montrer qu'il existe une plus petite extension M de L dans $\overline{K}$ telle que M/K est normale.

Exercice 8.11. Soit $\alpha = \sqrt[4]{2\sqrt{3} + \sqrt[3]{2} - 1} \in \overline{\mathbb{Q}}$.

1. Déterminer la plus petite extension K de $\mathbb{Q}(\alpha^4)$ dans $\overline{\mathbb{Q}}$ telle que $K/\mathbb{Q}$ est normale.
2. Déterminer la plus petite extension L de $\mathbb{Q}(\alpha)$ dans $\overline{\mathbb{Q}}$ telle que $L/\mathbb{Q}$ est normale.

Exercice 8.12. Soient L/K une extension finie et normale et $P(X) \in K[X]$ un polynôme irréductible. Soient $R(X), S(X) \in L[X]$ unitaires irréductibles divisant $P(X)$ dans $L[X]$. Montrer qu'il existe $\sigma \in \mathrm{Aut}_K(L)$ tel que $(\sigma R)(X) = S(X)$.

9. Théorie de Galois

Exercice 9.1. Soit L/K une extension de corps séparable de degré 2. Montrer que L/K est galoisienne.

Exercice 9.2. Soient L/K une extension finie galoisienne et $\alpha \in L$. Montrer que $L = K(\alpha)$ si et seulement si l'application $\mathrm{Gal}(L/K) \to L$, $\sigma \mapsto \sigma(\alpha)$ est injective.

Exercice 9.3. Soient L/K une extension finie galoisienne avec $\mathrm{Gal}(L/K) = \{\sigma_1, \ldots, \sigma_n\}$ et $\alpha_1, \ldots, \alpha_n \in L$. Montrer que $(\alpha_1, \ldots, \alpha_n)$ est une base de L sur K si et seulement si $\det((\sigma_i(\alpha_j))_{1 \leq i,j \leq n}) \neq 0$ (cf. exercice 9.2).

Exercice 9.4. Soient K un corps, $\overline{K}$ une clôture algébrique de K, $\alpha \in \overline{K}$ séparable de polynôme minimal $P_\alpha \in K[X]$, et $L \subseteq \overline{K}$ le corps de décomposition de P_α sur K. Soit

$$P(X) = \prod_{\sigma \in \mathrm{Gal}(L/K)} (X - \sigma\alpha) \in L[X].$$

1. Montrer que $P(X) \in K[X]$.
2. Montrer que $P(X) = P_\alpha(X)^{[L:K(\alpha)]}$.

Exercice 9.5. Soient K un corps, $\overline{K}$ une clôture algébrique de K, et $P(X) \in K[X]$ unitaire séparable. Soient $\alpha_1, \ldots, \alpha_n \in \overline{K}$ tels que $P(X) = \prod_{1 \leq i \leq n}(X - \alpha_i)$ et $L = K(\alpha_1, \ldots, \alpha_n)$. Montrer que les facteurs irréductibles de $P(X)$ dans $K[X]$ correspondent bijectivement aux orbites de $\{\alpha_1, \ldots, \alpha_n\}$ sous $\mathrm{Gal}(L/K)$.

Exercice 9.6. Soient L/K une extension finie galoisienne et $G = \mathrm{Gal}(L/K)$.

1. Montrer qu'il existe $\alpha \in L$ tel que $L = K(\alpha)$.
2. Soit M un corps entre K et L. Montrer qu'il existe $P \in K[X]$ tel que $M = K(P(\alpha))$.
3. Soient $P(X), Q(X) \in K[X]$. Montrer que $K(P(\alpha)) \subseteq K(Q(\alpha))$ si et seulement si $Q(\alpha) = Q(g\alpha)$ implique $P(\alpha) = P(g\alpha)$ pour tout $g \in G$.

Exercice 9.7. Soit $K \subseteq \overline{\mathbb{Q}}$ une extension galoisienne de $\mathbb{Q}$. Soit $\sigma : \mathbb{C} \to \mathbb{C}$, $z \mapsto \bar{z}$ la conjugaison complexe.

1. Montrer que σ est un $\mathbb{Q}$-automorphisme de $\overline{\mathbb{Q}}$ d'ordre 2.
2. Montrer que $\sigma(K) = K$.
3. Soit K^+ le sous-corps de K fixe par σ. Montrer que $[K : K^+] = 1$ ou 2.
4. Montrer que K^+ est le plus grand sous-corps de K contenu dans $\mathbb{R}$.

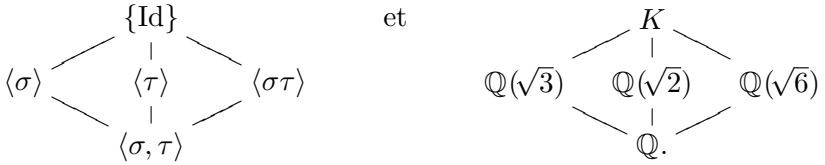
Exercice 9.8. Soit M/K une extension galoisienne telle que $\mathrm{Gal}(M/K) \simeq \mathcal{S}_3$. Déterminer les corps $K \subseteq L \subseteq M$ tels que l'extension L/K est galoisienne.

Exercice 9.9. Soit M/K une extension galoisienne de degré 45. Montrer qu'il existe une extension galoisienne L/K dans M de degré 5.

Exercice 9.10. Soient $n \geq 2$ entier, p premier, et M/K une extension galoisienne de degré p^n. Montrer qu'il existe une extension galoisienne L/K dans M de degré p^m avec $1 \leq m \leq n-1$.

Exercice 9.11. Soit $K = \mathbb{Q}(\sqrt{2}, \sqrt{3}) \subset \overline{\mathbb{Q}}$.

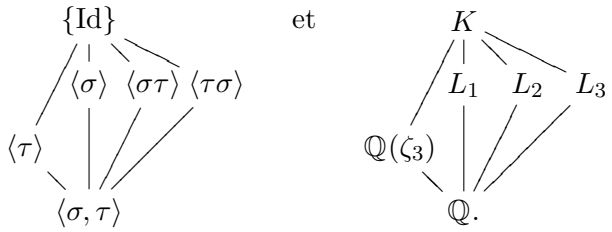
1. Montrer que l'extension $K/\mathbb{Q}$ est galoisienne.
2. Montrer que $\mathrm{Gal}(K/\mathbb{Q}) = \langle \sigma, \tau \rangle \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ où les $\mathbb{Q}$-automorphismes de corps σ, τ sont donnés par $\sigma(\sqrt{2}) = -\sqrt{2}$, $\sigma(\sqrt{3}) = \sqrt{3}$ et $\tau(\sqrt{2}) = \sqrt{2}$, $\tau(\sqrt{3}) = -\sqrt{3}$.
3. Montrer que les trellis des sous-groupes de $\mathrm{Gal}(K/\mathbb{Q})$ et des sous-extensions de $K/\mathbb{Q}$ sont



Exercice 9.12. Soient ζ_3 une racine primitive troisième de l'unité et $K = \mathbb{Q}(\zeta_3, \sqrt[3]{5}) \subset \overline{\mathbb{Q}}$.

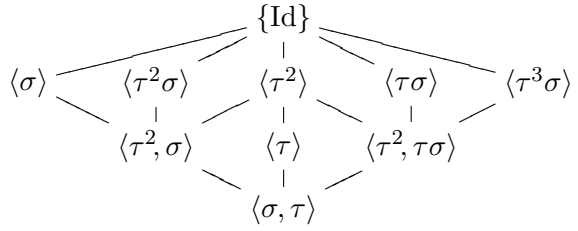
1. Montrer que l'extension $K/\mathbb{Q}$ est galoisienne.
2. Montrer que $\mathrm{Gal}(K/\mathbb{Q}) = \langle \sigma, \tau \rangle \simeq \mathcal{S}_3$ où les $\mathbb{Q}$-automorphismes de corps σ, τ sont donnés par $\sigma(\zeta_3) = \zeta_3^{-1}$, $\sigma(\sqrt[3]{5}) = \sqrt[3]{5}$ et $\tau(\zeta_3) = \zeta_3$, $\tau(\sqrt[3]{5}) = \zeta_3 \sqrt[3]{5}$.

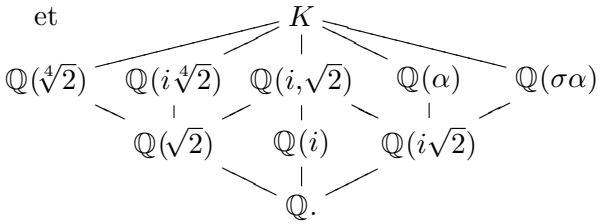
3. Soient $L_1 = \mathbb{Q}(\sqrt[3]{5})$, $L_2 = \mathbb{Q}(\zeta_3\sqrt[3]{5})$ et $L_3 = \mathbb{Q}(\zeta_3^{-1}\sqrt[3]{5})$. Montrer que les trellis des sous-groupes de $\mathrm{Gal}(K/\mathbb{Q})$ et des sous-extensions de $K/\mathbb{Q}$ sont



Exercice 9.13. Soient $K = \mathbb{Q}(i, \sqrt[4]{2}) \subset \overline{\mathbb{Q}}$ et D_8 le groupe dihédral à huit éléments.

1. Montrer que l'extension $K/\mathbb{Q}$ est galoisienne.
2. Montrer que $\mathrm{Gal}(K/\mathbb{Q}) = \langle \sigma, \tau \rangle \simeq D_8$ où les $\mathbb{Q}$-automorphismes de corps σ, τ sont donnés par $\sigma(i) = -i$, $\sigma(\sqrt[4]{2}) = \sqrt[4]{2}$ et $\tau(i) = i$, $\tau(\sqrt[4]{2}) = i\sqrt[4]{2}$.
3. Soit $\alpha = \sqrt[4]{2} + i\sqrt[4]{2} \in K$. Montrer que les trellis des sous-groupes de $\mathrm{Gal}(K/\mathbb{Q})$ et des sous-extensions de $K/\mathbb{Q}$ sont





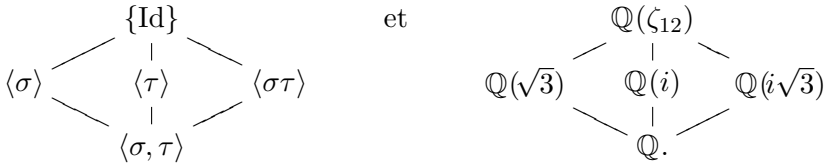
Exercice 9.14. Soient $n \geq 2$ un entier et $\zeta_n \in \overline{\mathbb{Q}}$ une racine primitive n-ième de l'unité (cf. section 7).

1. Montrer que l'extension $\mathbb{Q}(\zeta_n)/\mathbb{Q}$ est galoisienne et que $\mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}) \simeq (\mathbb{Z}/n\mathbb{Z})^\times$.
2. Soit $\mathbb{Q}(\zeta_n)^+$ le sous-corps de $\mathbb{Q}(\zeta_n)$ fixe par la conjugaison complexe (exercice 9.7). Montrer que $\mathbb{Q}(\zeta_n)^+ = \mathbb{Q}(\zeta_n + \zeta_n^{-1}) = \mathbb{Q}(\cos\frac{2\pi}{n})$.

Exercice 9.15. Soit $\zeta_{12} \in \overline{\mathbb{Q}}$ une racine primitive douzième de l'unité (cf. section 7).

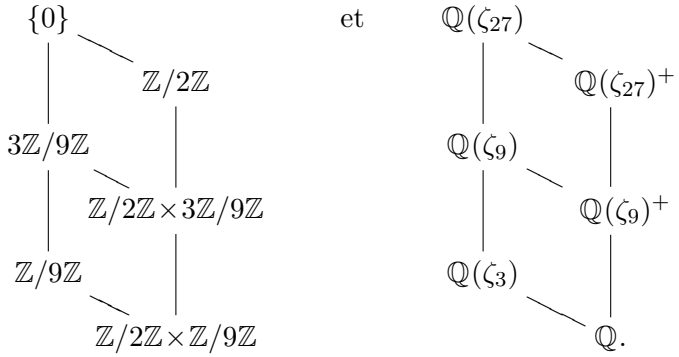
1. Montrer que $\mathrm{Gal}(\mathbb{Q}(\zeta_{12})/\mathbb{Q}) = \langle \sigma, \tau \rangle \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ où les $\mathbb{Q}$-automorphismes de corps σ, τ sont donnés par $\sigma(\zeta_{12}) = \zeta_{12}^{-1}$ et $\tau(\zeta_{12}) = \zeta_{12}^5$.

2. Montrer que les trellis des sous-groupes de $\mathrm{Gal}(\mathbb{Q}(\zeta_{12})/\mathbb{Q})$ et des sous-extensions de $K/\mathbb{Q}$ sont



Exercice 9.16. Soient $\zeta_{27} \in \overline{\mathbb{Q}}$ une racine primitive 27-ième de l'unité (cf. section 7) et $\zeta_9 = \zeta_{27}^3$, $\zeta_3 = \zeta_9^3 \in \overline{\mathbb{Q}}$.

1. Montrer que $\mathrm{Gal}(\mathbb{Q}(\zeta_{27})/\mathbb{Q}) \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/9\mathbb{Z}$ (cf. exercice 9.14).
2. Montrer que ζ_9 (resp. ζ_3) est une racine primitive 9-ième (resp. 3-ième) de l'unité.
3. Pour $n \in \{9, 27\}$ soit $\mathbb{Q}(\zeta_n)^+$ le sous-corps de $\mathbb{Q}(\zeta_n)$ fixe par la conjugaison complexe (cf. exercice 9.7). Montrer que les trellis des sous-extensions de $\mathbb{Q}(\zeta_{27})/\mathbb{Q}$ et des sous-groupes de $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/9\mathbb{Z}$ sont



Exercice 9.17 (Théorème de la base normale)**.** Soient L/K une extension galoisienne de degré $n \geq 1$ avec $\mathrm{Gal}(L/K) = \{\sigma_1, \ldots, \sigma_n\}$.

1. On suppose que K est fini. Montrer qu'il existe $\alpha \in L$ tel que $(\sigma_1\alpha, \ldots, \sigma_n\alpha)$ est une base de L sur K (cf. exercice 6.17).
2. On suppose que K est infini. Soit $(\beta_1, \ldots, \beta_n)$ une base de L sur K. On définit
$$\Delta(X_1, \ldots, X_n) \underset{\text{def}}{=} \det\Big((\sigma_i\sigma_j\beta_1)X_1 + \ldots + (\sigma_i\sigma_j\beta_n)X_n\Big)_{1\leq i,j\leq n}.$$
   (a) Montrer que $\Delta(X_1, \ldots, X_n)^2 \in K[X_1, \ldots, X_n]$.
   (b) Soit $P \in K[X_1, \ldots, X_n]$ tel que $P(x_1, \ldots, x_n) = 0$ pour tous $x_1, \ldots, x_n \in K$. Montrer que $P = 0$. (Comparer avec l'exercice 6.3.)
   (c) Montrer que $\Delta(X_1, \ldots, X_n) \neq 0$.
   (d) Montrer qu'il existe $\alpha \in L$ tel que $(\sigma_1\alpha, \ldots, \sigma_n\alpha)$ est une base de L sur K (cf. exercice 9.3).

Exercice 9.18. Soient M/K une extension galoisienne, $K \subseteq L \subseteq M$ un corps, et
$$H = \{\sigma \in \mathrm{Gal}(M/K) \mid \sigma(L) = L\}.$$

1. Montrer que H est un sous-groupe de $\mathrm{Gal}(M/K)$.
2. Montrer que H est le normalisateur de $\mathrm{Gal}(M/L)$ dans $\mathrm{Gal}(M/K)$.

3. Montrer que $M^H \subseteq L$.
4. Montrer que M^H/K est la plus petite extension telle que L/M^H est galoisienne.

Exercice 9.19. Soit M/K une extension finie galoisienne. Soient L, L' deux extensions de K contenues dans M et $H = \mathrm{Gal}(M/L)$, $H' = \mathrm{Gal}(M/L')$.

1. Montrer que $\mathrm{Gal}(M/LL') = H \cap H'$.
2. Montrer que $\mathrm{Gal}(M/L \cap L') = HH'$.
3. Montrer que $[LL' : L \cap L'] = \#(HH'/H \cap H')$.
4. Montrer que $[L : L \cap L'] = \#(HH'/H)$.
5. Montrer que L et L' sont linéairement disjointes sur $L \cap L'$ si et seulement si $|HH'|\,|H \cap H'| = |H|\,|H'|$.
6. On suppose que $L/L \cap L'$ est galoisienne. Montrer que L et L' sont linéairement disjointes sur $L \cap L'$.

Exercice 9.20. Soit $M \subset \overline{\mathbb{Q}}$ le corps de décomposition du polynôme $X^3 - 2$ sur $\mathbb{Q}$. Soit $\zeta_3 \in \overline{\mathbb{Q}}$ une racine primitive troisième de l'unité.

1. Soient $L = \mathbb{Q}(\sqrt[3]{2})$ et $L' = \mathbb{Q}(\zeta_3)$.
   (a) Montrer que $LL' = M$ et $L \cap L' = \mathbb{Q}$.
   (b) Montrer que $\mathrm{Gal}(M/\mathbb{Q}) = \langle \sigma, \tau \rangle$ où les $\mathbb{Q}$-automorphismes de corps σ et τ sont donnés par $\sigma\sqrt[3]{2} = \sqrt[3]{2}$, $\sigma\zeta_3 = \zeta_3^{-1}$ et $\tau\zeta_3 = \zeta_3$, $\tau\sqrt[3]{2} = \zeta_3\sqrt[3]{2}$.
   (c) Montrer que $\mathrm{Gal}(M/\mathbb{Q})$ est isomorphe à $\mathcal{S}_3$.
   (d) Montrer que $\mathrm{Gal}(M/L) = \langle \sigma \rangle$ et $\mathrm{Gal}(M/L') = \langle \tau \rangle$.
   (e) Montrer que L et L' sont linéairement disjointes sur $\mathbb{Q}$.
2. Soit $L'' = \mathbb{Q}(\zeta_3\sqrt[3]{2})$.
   (a) Montrer que $LL'' = M$ et $L \cap L'' = \mathbb{Q}$.
   (b) Montrer que $\mathrm{Gal}(M/L'') = \langle \tau\sigma\tau^{-1} \rangle$.
   (c) Montrer que $\langle \sigma \rangle \cap \langle \tau\sigma\tau^{-1} \rangle = \{\mathrm{Id}_M\}$ et $\langle \sigma, \tau\sigma\tau^{-1} \rangle = \langle \sigma, \tau \rangle$.
   (d) Montrer que L et L'' ne sont pas linéairement disjointes sur $\mathbb{Q}$.

Exercice 9.21. Soient L/K et M/K deux extensions finies avec L/K galoisienne.

1. Montrer que l'extension LM/M est galoisienne.
2. Soient $\sigma \in \mathrm{Gal}(LM/M)$ et $\sigma_{|L}$ sa restriction à L. Montrer que $\sigma_{|L} \in \mathrm{Gal}(L/L \cap M)$.
3. Montrer que $\mathrm{Gal}(LM/M) \to \mathrm{Gal}(L/L \cap M)$, $\sigma \mapsto \sigma_{|L}$ est un isomorphisme de groupes.
4. Montrer que $[LM : L \cap M] = [L : L \cap M]\,[M : L \cap M]$.
5. Montrer que L et K sont linéairement disjointes.

Exercice 9.22. Soient L/K et M/K deux extensions finies galoisiennes.

1. Montrer que l'extension LM/K est galoisienne.
2. Montrer que l'extension $L \cap M/K$ est galoisienne.
3. Montrer que $\rho : \mathrm{Gal}(LM/K) \to \mathrm{Gal}(L/K) \times \mathrm{Gal}(M/K)$, $\sigma \mapsto (\sigma_{|L}, \sigma_{|M})$ est un morphisme de groupes injectif.
4. Montrer que $\Gamma = \{(g, h) \in \mathrm{Gal}(L/K) \times \mathrm{Gal}(M/K) \mid g_{|L\cap M} = h_{|L\cap M}\}$ est un sous-groupe de $\mathrm{Gal}(L/K) \times \mathrm{Gal}(M/K)$.
5. Montrer que ρ induit un isomorphisme de groupes $\mathrm{Gal}(LM/K) \simeq \Gamma$.
6. Montrer que $\mathrm{Gal}(L/L \cap M) \times \mathrm{Gal}(M/L \cap M)$ est un sous-groupe de Γ.
7. Montrer que $\mathrm{Gal}(LM/L \cap M) \simeq \mathrm{Gal}(L/L \cap M) \times \mathrm{Gal}(M/L \cap M)$.

Exercice 9.23. Soient x un élément transcendant sur $\mathbb{C}$ et $L = \mathbb{C}(x)$. Soient $\sigma, \tau \in \mathrm{Aut}_{\mathbb{C}}(L)$ donnés par $\sigma(x) = x^{-1}$ et $\tau(x) = \zeta_3 x$ où $\zeta_3 \in \mathbb{C}$ est une racine primitive troisième de l'unité.

1. Montrer que $\sigma^2 = \tau^3 = \mathrm{Id}$ et $\sigma\tau = \tau^{-1}\sigma$.
2. Soit $G = \langle \sigma, \tau \rangle \subseteq \mathrm{Aut}_{\mathbb{C}}(L)$. Montrer que $G \simeq \mathcal{S}_3$.
3. Soit $K = L^G$. Montrer que L/K est galoisienne de groupe de Galois G.
4. Montrer que $L^{\langle\sigma\rangle} = \mathbb{C}(x + x^{-1})$ et $L^{\langle\tau\rangle} = \mathbb{C}(x^3)$.
5. Montrer que $K = \mathbb{C}(x^3 + x^{-3})$.

Exercice 9.24. Soient F un corps fini à q éléments et $F(X) = \mathrm{Frac}\, F[X]$. Soit G l'ensemble des applications $F(X) \to F(X)$, $f(X) \mapsto f(\frac{aX+b}{cX+d})$ avec $a, b, c, d \in F$ tels que $ad - bc \neq 0$.

1. Montrer que G est un sous-groupe de $\mathrm{Aut}_F(F(X))$ (cf. exercice 2.7).
2. Montrer que G est d'ordre $q^3 - q$.
3. Soit T le sous-groupe de G formé des $f(X) \mapsto f(X + b)$ avec $b \in F$. Montrer que $F(X)^T = F(X^q - X)$.
4. Soit H le sous-groupe de G formé des $f(X) \mapsto f(aX + b)$ avec $a, b \in F$ et $a \neq 0$. Montrer que $F(X)^H = F((X^q - X)^{q-1})$.
5. Soit $f(X) = \frac{(X^{q^2} - X)^{q+1}}{(X^q - X)^{q^2+1}} \in F(X)$. Montrer que $F(X)^G = F(f(X))$.

10. Extensions cycliques

Exercice 10.1. Pour $n \geq 1$ entier soit $\zeta_n \in \overline{\mathbb{Q}}$ une racine primitive n-ième de l'unité.

1. Montrer que l'extension $\mathbb{Q}(\zeta_9)/\mathbb{Q}$ est cyclique de degré 6.
2. Montrer que l'extension $\mathbb{Q}(\zeta_8)/\mathbb{Q}$ est abélienne non cyclique de degré 4.

Exercice 10.2. Soient L/K une extension cyclique de degré $n \geq 2$ et $n = p_1^{m_1} \dots p_r^{m_r}$ la factorisation de n en puissances de premiers distincts. Soient $1 \leq i \leq r$ et $0 \leq s \leq m_i$.

1. Montrer qu'il existe un unique corps $K \subset K_i \subset L$ tel que $\mathrm{Gal}(K_i/K) \simeq \mathbb{Z}/p_i^{m_i}\mathbb{Z}$.
2. Soient $i \neq j$. Montrer que $K_i \cap K_j = K$.
3. Montrer que $L = K_1 \dots K_n$.
4. Montrer que K_i contient une unique extension de K de degré p_i^s.
5. Montrer qu'il existe un unique corps $K \subset L_i \subset L$ tel que $\mathrm{Gal}(L/L_i) \simeq \mathbb{Z}/p_i^{m_i}\mathbb{Z}$.
6. Montrer que L contient une unique extension de L_i de degré p_i^s.

Exercice 10.3. Soit K le sous-corps maximal de $\overline{\mathbb{Q}}$ tel que $\sqrt{2} \notin K$ (un tel corps existe par le lemme de Zorn). Montrer que toute extension finie de K dans $\overline{\mathbb{Q}}$ est cyclique.

Exercice 10.4. Soient K un corps, $\overline{K}$ une clôture algébrique de K et $\sigma \in \mathrm{Aut}_K(\overline{K})$. Soit $L = \overline{K}^{\langle\sigma\rangle}$. Montrer que toute extension finie de L dans $\overline{K}$ est cyclique.

Exercice 10.5. Soient K un corps et $\overline{K}$ une clôture algébrique de K. On suppose que toute extension finie de K dans $\overline{K}$ est cyclique. Montrer qu'il existe $\sigma \in \mathrm{Aut}_K(\overline{K})$ tel que $K = \overline{K}^{\langle\sigma\rangle}$.

Exercice 10.6. Soit $K/\mathbb{Q}$ une extension cyclique de degré $n = 2^r m$ avec $r \geq 1$ et m impair. Soient $\mathbb{Q} \subset L \subset K$ l'unique corps tel que $\mathrm{Gal}(L/\mathbb{Q}) \simeq \mathbb{Z}/2^r\mathbb{Z}$ (cf. exercice 10.2) et L^+ le sous-corps de L fixe par la conjugaison complexe (cf. exercice 9.7). On suppose qu'il existe $d \in \mathbb{Z}$ tel que $d < 0$ et $\mathbb{Q}(\sqrt{d}) \subseteq K$.

1. Montrer que $\mathbb{Q}(\sqrt{d}) \subseteq L$.
2. Montrer que $[L : L^+] = 2$.
3. Montrer que $L = \mathbb{Q}(\sqrt{d})$ et $L^+ = \mathbb{Q}$.
4. Montrer que 4 ne divise pas $[K : \mathbb{Q}]$.

Exercice 10.7. Soient K un corps, $\overline{K}$ une clôture algébrique de K et $\alpha \in \overline{K}$ séparable tel que $[K(\alpha) : K] = p$ premier. Soient $L \subseteq \overline{K}$ le corps de décomposition du polynôme minimal de α sur K et $G = \mathrm{Gal}(L/K)$.

1. Montrer que l'orbite de α sous G est d'ordre p.
2. Soit $H = \mathrm{Stab}_G(\alpha)$. Montrer que $K(\alpha) = L^H$ et que $G/H \simeq \mathbb{Z}/p\mathbb{Z}$.
3. Soit $g \in G$. Montrer que $\mathrm{Stab}_G(g\alpha) = gHg^{-1}$.
4. On suppose qu'il existe $g \in G$ tel que $g \notin H$ et $gHg^{-1} = H$.
   (a) Montrer que H est normal dans G.
   (b) Montrer que L est la plus petite extension galoisienne de K contenant α.
   (c) Montrer que $H = G$.
5. On suppose qu'il existe $\beta \in \mathrm{Orb}_G(\alpha)$ tel que $\beta \neq \alpha$ et $\beta \in K(\alpha)$.
   (a) Montrer que $K(\beta) = K(\alpha)$.
   (b) Montrer que $K(\alpha) = L$.
   (c) Montrer que $K(\alpha)/K$ est cyclique.

Exercice 10.8 (Théorème de Hilbert 90)**.** Soit L/K une extension cyclique de degré $n \geq 2$ avec $\mathrm{Gal}(L/K) = \langle\sigma\rangle$. Soient $\alpha \in L$ et $N_{L/K}(\alpha) = \prod_{0\leq i\leq n-1} \sigma^i\alpha \in K$ (cf. section 4).

1. On suppose qu'il existe $\beta \in L^\times$ tel que $\alpha = \beta/\sigma\beta$. Montrer que $N_{L/K}(\alpha) = 1$.
2. On suppose que $N_{L/K}(\alpha) = 1$. Pour $0 \leq k \leq n-2$ soit $\alpha_k = \prod_{0\leq i\leq k} \sigma^i(\alpha) \in L$.
   (a) Montrer que l'application $\chi_\alpha : L \to L$, $x \mapsto x + \alpha_0\sigma(x) + \ldots + \alpha_{n-2}\sigma^{n-1}(x)$ est non nulle (cf. exercice 4.2).
   (b) Soient $\gamma \in L$ tel que $\chi_\alpha(\gamma) \neq 0$ et $\beta = \chi_\alpha(\gamma)$. Montrer que $\alpha = \beta/\sigma\beta$.

Exercice 10.9 (Théorie de Kummer)**.** Soient K un corps, $\overline{K}$ une clôture algébrique de K, et $n \geq 2$ un entier premier à la caractéristique de K. On suppose que K contient une racine primitive n-ième de l'unité ζ_n.

1. Soit L/K une extension cyclique de degré n dans $\overline{K}$ avec $\mathrm{Gal}(L/K) = \langle\sigma\rangle$.
   (a) Montrer que $N_{L/K}(\zeta_n^{-1}) = 1$.
   (b) Montrer qu'il existe $\alpha \in L^\times$ tel que $\sigma\alpha = \zeta_n\alpha$ (cf. exercice 10.8).
   (c) Montrer que $L = K(\alpha)$.
   (d) Montrer que $\alpha^n \in K$.
2. Soient $a \in K$ et $\alpha \in \overline{K}$ une racine de $X^n - a$.
   (a) Montrer que l'extension $K(\alpha)/K$ est galoisienne.
   (b) Montrer que l'extension $K(\alpha)/K$ est cyclique de degré $d \mid n$.
   (c) Montrer que $\alpha^d \in K$.

Exercice 10.10 (Hilbert 90, forme additive)**.** Soit L/K une extension cyclique de degré $n \geq 2$ avec $\mathrm{Gal}(L/K) = \langle\sigma\rangle$. Soient $\alpha \in L$ et $\mathrm{Tr}_{L/K}(\alpha) = \sum_{0\leq i\leq n-1} \sigma^i\alpha \in K$ (cf. section 4). Soient $\alpha_k = \sum_{0\leq i\leq k} \sigma^i(\alpha) \in L$ $(0 \leq k \leq n-2)$ et $\gamma \in L$ tel que $\mathrm{Tr}_{L/K}(\gamma) \neq 0$ (cf. exercice 4.4).

1. On suppose qu'il existe $\beta \in L$ tel que $\alpha = \beta - \sigma\beta$. Montrer que $\mathrm{Tr}_{L/K}(\alpha) = 0$.

2. On suppose que $\mathrm{Tr}_{L/K}(\alpha) = 0$. Soit $\beta = \mathrm{Tr}_{L/K}^{-1}(\gamma)(\gamma + \alpha_0\sigma(\gamma) + \ldots + \alpha_{n-2}\sigma^{n-1}(\gamma))$. Montrer que $\alpha = \beta - \sigma\beta$.

Exercice 10.11 (Théorie d'Artin-Schreier)**.** Soient K un corps de caractéristique p et $\overline{K}$ une clôture algébrique de K.

1. Soit L/K une extension cyclique de degré p dans $\overline{K}$ avec $\mathrm{Gal}(L/K) = \langle\sigma\rangle$.
   (a) Montrer que $\mathrm{Tr}_{L/K}(-1) = 0$.
   (b) Montrer qu'il existe $\alpha \in L$ tel que $\sigma\alpha = \alpha + 1$ (cf. exercice 10.10).
   (c) Montrer que $L = K(\alpha)$.
   (d) Montrer que $\alpha^p - \alpha \in K$.
2. Soient $a \in K$ et $\alpha \in \overline{K}$ une racine de $X^p - X - a$.
   (a) Montrer que $X^p - X - a$ est soit irréductible soit totalement scindé dans $K[X]$.
   (b) On suppose que $X^p - X - a$ est irréductible dans $K[X]$. Montrer que l'extension $K(\alpha)/K$ est cyclique de degré p.

11. Groupes de Galois de polynômes

Exercice 11.1. Déterminer le groupe de Galois des polynômes suivants sur chacun des corps indiqués.

1. $X^3 + 2X^2 + 3X + 2$ sur $\mathbb{Q}$, $\mathbb{Q}(\sqrt{-7})$ et $\mathbb{Q}(\sqrt{7})$.
2. $X^3 - 10$ sur $\mathbb{Q}$ et $\mathbb{Q}(\sqrt{-3})$.
3. $X^4 - 5$ sur $\mathbb{Q}$, $\mathbb{Q}(\sqrt{5})$, $\mathbb{Q}(\sqrt{-5})$ et $\mathbb{Q}(i)$.
4. $X^4 + 2$ sur $\mathbb{Q}$ et $\mathbb{Q}(i)$.
5. $(X^2 - 2)(X^2 - 3)(X^2 - 5)(X^2 - 7)$ sur $\mathbb{Q}$.
6. $(X^3 - 2)(X^3 - 3)(X^2 - 2)$ sur $\mathbb{Q}(\sqrt{-3})$.

Exercice 11.2. Soit t un élément transcendant sur $\mathbb{C}$.

1. Soit $n \geq 1$ un entier. Montrer que le groupe de Galois sur $\mathbb{C}(t)$ de $X^n - t$ est isomorphe à $\mathbb{Z}/n\mathbb{Z}$.
2. Montrer que le groupe de Galois sur $\mathbb{R}(t)$ de $X^4 - t$ est isomorphe au groupe dihédral à huit éléments D_8.

Exercice 11.3 (Groupe de Galois d'un polynôme de degré trois)**.** Soient K un corps de caractéristique différente de 3 et $\overline{K}$ une clôture algébrique de K.

1. Soient $a_0, a_1, a_2 \in K$ et $Q(X) = X^3 + a_2X^2 + a_1X + a_0 \in K[X]$. Montrer qu'il existe $a, b \in K$ tels que $X^3 + aX + b$ et $Q(X)$ ont le même corps de décomposition dans $\overline{K}$ sur K (calculer $Q(X - \frac{a_2}{3})$).

Soient $a, b \in K$ et $P(X) = X^3 + aX + b \in K[X]$. Soient $\alpha, \beta, \gamma \in \overline{K}$ tels que $P(X) = (X - \alpha)(X - \beta)(X - \gamma)$. On pose

$$\Delta = -4a^3 - 27b^2 \ \in K \quad \text{et} \quad \delta = (\alpha - \beta)(\alpha - \gamma)(\beta - \gamma) \ \in \overline{K}.$$

2. (a) Montrer que $\alpha + \beta + \gamma = 0$, $\alpha\beta + \alpha\gamma + \beta\gamma = a$, et $\alpha\beta\gamma = -b$.
   (b) Vérifier l'égalité $(2x+y)^2(x+2y)^2(x-y)^2 = 4(x^2+xy+y^2)^3 - 27(x+y)^2x^2y^2$.
   (c) Montrer que $\Delta = \delta^2$.

On suppose que la caractéristique de K est différente de 2 et de 3.

3. On suppose que Δ est un carré dans K, c'est-à-dire $\delta \in K$.

   (a) Montrer que $\beta+\gamma \in K(\alpha)$ et $\beta-\gamma \in K(\alpha)$.
   (b) Montrer que $\alpha \in K \Rightarrow \beta \in K$ et $\gamma \in K$.
4. On suppose que Δ est un carré dans K. Montrer que $P(X)$ est soit irréductible soit totalement scindé dans $K[X]$.
5. Soit $L = K(\alpha, \beta, \gamma)$. On suppose que $P(X)$ est irréductible dans $K[X]$.
   (a) On suppose que Δ n'est pas un carré dans K. Montrer que $\mathrm{Gal}(L/K) \simeq \mathcal{S}_3$.
   (b) On suppose que Δ est un carré dans K. Montrer que $\mathrm{Gal}(L/K) \simeq \mathbb{Z}/3\mathbb{Z}$.
6. Déterminer le groupe de Galois sur $\mathbb{Q}$ de X^3-2X+1, X^3-X+1 et X^3-3X+1.

Exercice 11.4. Soient $P(X) = X^4-4X^2-1 \in \mathbb{Q}[X]$ et $K \subset \overline{\mathbb{Q}}$ le corps de décomposition de $P(X)$ sur $\mathbb{Q}$.

1. (a) Montrer que $P(X)$ a deux racines réelles $\pm\alpha \in \overline{\mathbb{Q}}$ ainsi que deux racines non réelles $\pm\beta \in \overline{\mathbb{Q}}$ et les déterminer.
   (b) Montrer que $P(X)$ est irréductible dans $\mathbb{Q}[X]$.
2. Soient $\sigma, \rho \in \mathrm{Gal}(K/\mathbb{Q})$ donnés par $\sigma(\alpha) = \beta$, $\sigma(\beta) = \alpha$ et $\rho(\alpha) = -\beta$, $\rho(\beta) = \alpha$.
   (a) Montrer que $\mathrm{ord}(\sigma) = 2$ et $\mathrm{ord}(\rho) = 4$.
   (b) Montrer que $\sigma\rho\sigma^{-1} = \rho^{-1}$.
   (c) Montrer que $\langle\sigma, \rho\rangle$ est isomorphe au groupe dihédral à huit éléments D_8.
3. (a) Montrer que $\mathrm{ord}(\sigma\rho) = \mathrm{ord}(\rho\sigma) = 2$.
   (b) Montrer que $K^{\langle\rho\sigma\rangle} = \mathbb{Q}(\alpha)$ et $K^{\langle\sigma\rho\rangle} = \mathbb{Q}(\beta)$.
   (c) Montrer que $[K : \mathbb{Q}] = 8$.
   (d) Montrer que $\mathrm{Gal}(K/\mathbb{Q}) = \langle\sigma, \rho\rangle$.
4. (a) Montrer que $\langle\rho\sigma, \sigma\rho\rangle$ est isomorphe à $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.
   (b) Montrer que $K^{\langle\rho\sigma,\sigma\rho\rangle} = \mathbb{Q}(\sqrt{5})$.
   (c) Montrer que $\mathbb{Q}(\alpha\beta) = \mathbb{Q}(i)$ et déterminer $\mathrm{Gal}(K/\mathbb{Q}(i))$.

Exercice 11.5. Soit $P(X) = X^4 + aX^2 + b \in \mathbb{Q}[X]$ irréductible. Soient $\pm\alpha, \pm\beta \in \overline{\mathbb{Q}}$ les racines de $P(X)$ et $K = \mathbb{Q}(\alpha, \beta) \subset \overline{\mathbb{Q}}$ son corps de décomposition sur $\mathbb{Q}$.

1. Montrer que $[\mathbb{Q}(\alpha) : \mathbb{Q}(\alpha^2)] = [\mathbb{Q}(\alpha^2) : \mathbb{Q}] = 2$.
2. (a) Montrer que $\alpha^2\beta^2 = b$ et $\alpha^2 + \beta^2 = -a$.
   (b) Montrer que $\mathbb{Q}(\alpha^2) = \mathbb{Q}(\beta^2) = \mathbb{Q}(\sqrt{a^2-4b})$ et $\mathbb{Q}(\alpha\beta) = \mathbb{Q}(\sqrt{b})$.
   (c) Montrer que $\mathbb{Q}(\alpha) = \mathbb{Q}(\beta)$ si et seulement si $\mathbb{Q}(\alpha\beta) \subseteq \mathbb{Q}(\alpha^2)$.
   (d) Montrer que $\mathbb{Q}(\alpha\beta) = \mathbb{Q}(\alpha^2)$ si et seulement si $\sqrt{\frac{a^2-4b}{b}} \in \mathbb{Q}$.
3. On suppose que $\sqrt{\frac{a^2-4b}{b}} \notin \mathbb{Q}$ et $\sqrt{b} \notin \mathbb{Q}$. Montrer que $\mathrm{Gal}(K/\mathbb{Q}) \simeq D_8$.
4. On suppose que $\sqrt{\frac{a^2-4b}{b}} \in \mathbb{Q}$. Montrer que $\mathrm{Gal}(K/\mathbb{Q}) \simeq \mathbb{Z}/4\mathbb{Z}$.
5. On suppose que $\sqrt{b} \in \mathbb{Q}$. Montrer que $\mathrm{Gal}(K/\mathbb{Q}) \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.
6. Déterminer le groupe de Galois sur $\mathbb{Q}$ de X^4-5, X^4+5X+5 et X^4+1.

Exercice 11.6. Soient $\alpha = \sqrt{6+3\sqrt{2}+2\sqrt{3}+2\sqrt{6}} \in \overline{\mathbb{Q}}$ et $\delta = \alpha^2 \in \overline{\mathbb{Q}}$. Soit $P(X) = X^4 - 24X^3 + 108X^2 - 144X + 36$.

1. Vérifier que $P(\delta) = 0$.
2. Montrer que $\mathbb{Q}(\delta) = \mathbb{Q}(\sqrt{2}, \sqrt{3})$.
3. Montrer que $P(X)$ est le polynôme minimal de δ sur $\mathbb{Q}$ et que $N_{\mathbb{Q}(\delta)/\mathbb{Q}}(\delta) = 36$.
4. Montrer que δ n'est pas un carré dans $\mathbb{Q}(\delta)$ (cf. exercice 4.6).
5. Montrer que $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 8$ et que $P(X^2)$ est irréductible dans $\mathbb{Q}[X]$.

6. Soient $u = 6+3\sqrt{2}-2\sqrt{3}-2\sqrt{6}$, $v = 6-3\sqrt{2}+2\sqrt{3}-2\sqrt{6}$, $w = 6-3\sqrt{2}-2\sqrt{3}+2\sqrt{6}$. Calculer δu, δv, δw et montrer qu'ils sont des carrés dans $\mathbb{Q}(\delta)$.
7. Montrer que l'extension $\mathbb{Q}(\alpha)/\mathbb{Q}$ est galoisienne.
8. Montrer que $\mathrm{Gal}(\mathbb{Q}(\alpha)/\mathbb{Q})$ est isomorphe au groupe des quaternions. (Difficile.)

Exercice 11.7. Soient K un corps, $\overline{K}$ une clôture algébrique de K et $P(X) \in K[X]$ séparable de degré $n \geq 2$. Soient $\alpha_1, \ldots, \alpha_n \in \overline{K}$ les racines de $P(X)$ et $L = K(\alpha_1, \ldots, \alpha_n)$ le corps de décomposition de $P(X)$ sur K. On suppose que $[L : K] = n!$.

1. Montrer que $\mathcal{S}_n \to \mathrm{Gal}(L/K)$, $\sigma \mapsto (\alpha_i \mapsto \alpha_{\sigma(i)})$ est un isomorphisme de groupes.
2. Montrer que $P(X)$ est irréductible dans $K[X]$.
3. Pour $1 \leq i \leq n$ soit $H_i = \{\sigma \in \mathcal{S}_n \mid \sigma(i) = i\}$. Soit $\sigma \in \mathcal{S}_n$.
   (a) Montrer que H_i est un sous-groupe de $\mathcal{S}_n$ d'ordre $(n-1)!$.
   (b) Soient $i \neq j$. Montrer que $H_i \neq H_j$.
   (c) Montrer que $\sigma H_i \sigma^{-1} = H_{\sigma(i)}$.
   (d) Montrer que $\sigma H_i \sigma^{-1} = H_i$ si et seulement si $\sigma \in H_i$.
4. Soient $\alpha = \alpha_1$ et $H = H_1$.
   (a) Montrer que $\mathrm{Gal}\big(L/K(\alpha)\big) \simeq H$.
   (b) Montrer que $\mathrm{Aut}_K\big(K(\alpha)\big) \simeq N/H$ où N est le normalisateur de H dans $\mathcal{S}_n$.
   (c) Montrer que $\mathrm{Aut}_K\big(K(\alpha)\big) = \{\mathrm{Id}\}$.

Exercice 11.8. Soit $P(X) \in \mathbb{Q}[X]$ un polynôme irréductible de degré p premier ayant $p-2$ racines réelles et 2 racines non réelles. Soit K le corps de décomposition de $P(X)$ sur $\mathbb{Q}$.

1. Montrer que $\mathrm{Gal}(K/\mathbb{Q})$ contient un élément d'ordre p.
2. (a) Montrer que les éléments d'ordre p dans $\mathcal{S}_p$ sont les p-cycles.
   (b) Soient $\tau \in \mathcal{S}_p$ un p-cycle et $\sigma \in \mathcal{S}_p$ une transposition. Montrer que $\mathcal{S}_p = \langle \sigma, \tau \rangle$.
3. Montrer que $\mathrm{Gal}(K/\mathbb{Q})$ est isomorphe à $\mathcal{S}_p$.

Exercice 11.9. Montrer que le groupe de Galois de $X^5 - 4X + 2$ sur $\mathbb{Q}$ est isomorphe à $\mathcal{S}_5$ (cf. exercice 11.8).

Exercice 11.10 (Équation générale de degré n)**.** Soient $\mathbb{K}/K$ une extension de corps, $n \geq 1$ un entier, $x_1, \ldots, x_n \in \mathbb{K}$ algébriquement indépendants sur K (cf. définition 3), et $s_1, \ldots, s_n \in \mathbb{K}$ les expressions polynômiales symmétriques élémentaires en les $x_1, \ldots, x_n$: $s_1 = x_1 + \ldots + x_n, \ldots, s_n = x_1 \ldots x_n$. On pose $E = K(x_1, \ldots, x_n)$, $F = K(s_1, \ldots, s_n)$, et

$$\Pi(X) = (X - x_1) \ldots (X - x_n) \ \in E[X].$$

1. Montrer que $\Pi(X) = X^n + \sum_{1 \leq i \leq n} (-1)^i s_i X^{n-i}$.
2. Montrer que $\mathcal{S}_n$ s'identifie à un sous-groupe de $\mathrm{Aut}_K(E)$ par $\sigma \mapsto (x_i \mapsto x_{\sigma(i)})$.
3. Montrer que $F \subseteq E^{\mathcal{S}_n}$.
4. Montrer que $[E : E^{\mathcal{S}_n}] = n!$ et $[E : F] \leq n!$.
5. Montrer que $E^{\mathcal{S}_n} = F$.
6. Montrer que le groupe de Galois de $\Pi(X)$ sur F est $\mathcal{S}_n$.

Exercice 11.11 (Spécialisation de l'équation générale)**.** On reprend les hypothèses et notations de l'exercice 11.10. Soient $\overline{K}$ la clôture algébrique de K dans $\mathbb{K}$ et $\alpha_1, \ldots, \alpha_n \in \overline{K}$ séparables sur K. On pose $O_E = K[x_1, \ldots, x_n]$, $O_F = K[s_1, \ldots, s_n]$, et $M = K(\alpha_1, \ldots, \alpha_n)$.

Soit φ le morphisme de K-algèbres donné par

$$\begin{aligned}\varphi : O_E &\longrightarrow \overline{K} \\ x_i &\longmapsto \alpha_i\,,\ 1 \leq i \leq n.\end{aligned}$$

1. Montrer que $\operatorname{Ker}\varphi$ est un idéal maximal de O_E.
2. Soit $P(X) = X^n + a_{n-1}X^{n-1} + \ldots + a_0 \in \overline{K}[X]$ le polynôme obtenu en appliquant φ aux coefficients de $\Pi(X)$. Montrer que $\varphi(s_i) = (-1)^i a_{n-i}$ pour tout $1 \leq i \leq n$.
3. Montrer que $\varphi(O_E) = M$ et $\varphi(O_F) = K(a_1, \ldots, a_n) = L$.
4. Montrer que $O_E \cap F = O_F$.
5. Montrer que l'application de restriction $\operatorname{Aut}_F(E) \to \operatorname{Aut}_{O_F}(O_E)$, $\sigma \mapsto \sigma_{|O_E}$ est un isomorphisme de groupes.
6. Soit $G = \{\sigma \in \mathcal{S}_n \mid \sigma(\operatorname{Ker}\varphi) = \operatorname{Ker}\varphi\}$. Montrer que G est un sous-groupe de $\mathcal{S}_n$.
7. Montrer que l'application $\psi : G \to \operatorname{Gal}(M/L)$, $\sigma \mapsto \varphi \circ (\sigma_{|O_E} \bmod \operatorname{Ker}\varphi) \circ \varphi^{-1}$ est un morphisme de groupes surjectif.
8. Soit $H = \{\sigma \in G \mid \operatorname{Im}(\sigma_{|O_E} - \mathrm{Id}) \subseteq \operatorname{Ker}\varphi\}$. Montrer que $\operatorname{Ker}\psi = H$.
9. Montrer que ψ induit un isomorphisme de groupes $G/H \simeq \operatorname{Gal}(M/L)$.

Exercice 11.12. On reprend les exercices 11.10 et 11.11 avec $K = \mathbb{Q}$, $\mathbb{K} = \mathbb{C}$ et $n = 2$.

1. On prend $\alpha_1, \alpha_2 \in \mathbb{Q}$, d'où $M = L = \mathbb{Q}$.
   (a) Montrer que $\operatorname{Ker}\varphi = (x_1 - \alpha_1, x_2 - \alpha_2)$.
   (b) On suppose que $\alpha_1 = \alpha_2$. Montrer que $G = H = \mathcal{S}_2$.
   (c) On suppose que $\alpha_1 \neq \alpha_2$. Montrer que $G = H = \{\mathrm{Id}\}$.
2. On prend $\alpha_1 = \sqrt{2}$ et $\alpha_2 = \sqrt{3}$.
   (a) Montrer que $L = M = \mathbb{Q}(\sqrt{2}, \sqrt{3})$.
   (b) Montrer que $\operatorname{Ker}\varphi = (x_1^2 - 2, x_2^2 - 3)$.
   (c) Montrer que $G = H = \{\mathrm{Id}\}$.
3. On prend $\alpha_1 = \sqrt{2}$ et $\alpha_2 = -\sqrt{2}$.
   (a) Montrer que $M = \mathbb{Q}(\sqrt{2})$ et $L = \mathbb{Q}$.
   (b) Montrer que $\operatorname{Ker}\varphi = (x_1 + x_2, x_1x_2 + 2)$.
   (c) Montrer que $G = \mathcal{S}_2$ et $H = \{\mathrm{Id}\}$.

Exercice 11.13. On reprend les exercices 11.10 et 11.11 avec $K = \mathbb{Q}$, $\mathbb{K} = \mathbb{C}$ et $n = 3$.

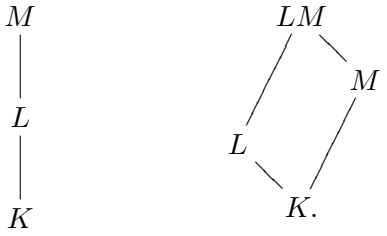
1. On prend $\alpha_1 = 1$, $\alpha_2 = i$ et $\alpha_3 = -i$.
   (a) Montrer que $P(X) = (X-1)(X^2+1)$, $L = \mathbb{Q}$, $M = \mathbb{Q}(i)$ et $\operatorname{Gal}(M/L) \simeq \mathbb{Z}/2\mathbb{Z}$.
   (b) Montrer que $\operatorname{Ker}\varphi = (x_1 - 1, x_2 + x_3, x_2x_3 - 1)$.
   (c) Montrer que $G = \langle(23)\rangle$ et $H = \{\mathrm{Id}\}$.
2. Soit $\zeta_3 \in \overline{\mathbb{Q}}$ une racine primitive troisième de l'unité. On prend $\alpha_1 = \sqrt[3]{2}$, $\alpha_2 = \zeta_3\sqrt[3]{2}$ et $\alpha_3 = \zeta_3^{-1}\sqrt[3]{2}$.
   (a) Montrer que $P(X) = X^3 - 2$, $L = \mathbb{Q}$, $M = \mathbb{Q}(\zeta_3, \sqrt[3]{2})$ et $\operatorname{Gal}(M/L) \simeq \mathcal{S}_3$.
   (b) Montrer que $\operatorname{Ker}\varphi = (x_1 + x_2 + x_3, x_1x_2 + x_2x_3 + x_1x_3, x_1x_2x_3 - 2)$.
   (c) Montrer que $G = \mathcal{S}_3$ et $H = \{\mathrm{Id}\}$.
3. Soit $\zeta_9 \in \overline{\mathbb{Q}}$ une racine primitive neuvième de l'unité. On prend $\alpha_1 = \zeta_9 + \zeta_9^{-1}$, $\alpha_2 = \zeta_9^2 + \zeta_9^{-2}$ et $\alpha_3 = \zeta_9^4 + \zeta_9^{-4}$.
   (a) Montrer que $P(X) = X^3 - 3X - 1$, $L = \mathbb{Q}$, $M = \mathbb{Q}(\alpha_1)$ et $\operatorname{Gal}(M/L) \simeq \mathbb{Z}/3\mathbb{Z}$.
   (b) Montrer que $\operatorname{Ker}\varphi = (x_1^2 - x_2 - 2, x_2^2 - x_3 - 2, x_1^3 - x_1 - 2)$.
   (c) Montrer que $G = \langle(123)\rangle$ et $H = \{\mathrm{Id}\}$.

12. Stabilité

Définition 7. Une classe $\mathcal{C}$ d'extensions de corps est *distinguée* si elle satisfait les deux conditions suivantes :

(1) Soient $K \subseteq L \subseteq M$ des extensions de corps. On a $M/K \in \mathcal{C}$ si et seulement si $M/L \in \mathcal{C}$ et $L/K \in \mathcal{C}$.
(2) Soient $K \subseteq L$ et $K \subseteq M$ des extensions de corps avec L et M contenus dans un corps commun. Si $L/K \in \mathcal{C}$ alors $LM/M \in \mathcal{C}$.

Ces deux situations sont illustrées par les diagrammes



Noter que les conditions (1) et (2) impliquent

(3) Soient $K \subseteq L$ et $K \subseteq M$ des extensions de corps avec L et M contenus dans un corps commun. Si $L/K \in \mathcal{C}$ et $M/K \in \mathcal{C}$ alors $LM/K \in \mathcal{C}$.

Exercice 12.1.

1. Montrer que les classes d'extensions suivantes sont distinguées.
   (a) Extensions finies.
   (b) Extensions algébriques.
   (c) Extensions séparables.
2. Montrer que les classes d'extensions suivantes ne sont pas distinguées.
   (a) Extensions normales.
   (b) Extensions galoisiennes.
   (c) Extensions abéliennes.