# Feuille TD 5 – Algèbre – Corps et théorie de Galois

**Exercice 1 — Corps parfaits.** Soit $K$ un corps. Soit $\sigma : K \to K$ un automorphisme de $K$. Soit $L$ un $K$-espace vectoriel.

1. Montrer que $(L, +)$, muni de la loi externe $(\alpha, x) \mapsto \sigma(\alpha) \cdot x$ est aussi un $K$-espace vectoriel, que l'on notera $L'$.
2. Montrer que si $L$ est de dimension finie $d$, alors $L'$ est aussi de dimension $d$.
3. En déduire que si $K$ est un corps parfait de caractéristique $p > 0$, toute extension finie de $K$ est un corps parfait.
4. Le résultat de **3.** reste-t-il vrai pour une extension algébrique (pas forcément finie) ?

**Exercice 2 — Corps algébriquement clos.** Soit $L/K$ une extension de corps. Soit $M$ le sous-corps de $L$ constitué des éléments algébriques sur $K$. On suppose que tout polynôme irréductible de $K[X]$ est scindé sur $L$.

1. Montrer que tout polynôme de $K[X]$ est scindé sur $M$.
2. Soit $F$ une extension finie de $M$. Montrer que tout $x \in F$ est algébrique sur $K$.
3. En déduire que $M$ est un corps algébriquement clos.

**Exercice 3 — Théorème de Steinitz.** Soit $K$ un corps. On note $\mathcal{I}$ l'ensemble des polynômes irréductibles unitaires de $K[X]$. On forme l'anneau de polynômes $A := K[(T_{P,i})_{P\in\mathcal{I}, 1\leqslant i\leqslant \deg P}]$ et pour tout $P \in \mathcal{I}$, on écrit dans $A[X]$ :

$$P - \prod_{i=1}^{\deg P} (X - T_{P,i}) = \sum_{j=0}^{\deg P - 1} a_{P,j} X^j,$$

où les $a_{P,j}$ sont dans $A$. On suppose par l'absurde que l'idéal $I$ de $A$ engendré par les $a_{P,j}$ est $A$ et on va montrer qu'on aboutit à une contradiction.

1. Montrer qu'il existe une partie finie $\mathcal{I}_1$ de $\mathcal{I}$ tels que l'idéal engendré par les $a_{P,j}$ avec $P \in \mathcal{I}_1$ soit égal à $A$.
2. Soit $Q = \prod_{P\in\mathcal{I}_1} P \in K[X]$ et soit $L$ un corps de décomposition de $Q$ sur $K$. Pour $P \in \mathcal{I}_1$, on pose

$$P = \prod_{i=1}^{\deg P} (X - \alpha_{P,i}), \quad \alpha_{P,i} \in L.$$

   Soit $A_1 \subset A$ l'anneau $K[(T_{P,i})_{P\in\mathcal{I}_1, 1\leqslant i\leqslant \deg P}]$. Montrer qu'il existe un morphisme de $K$-algèbres $\varphi$ de $A_1$ dans $L$ qui envoie chaque $T_{P,i}$ sur $\alpha_{P,i}$ pour tout $P \in \mathcal{I}_1$ et tout $i$ avec $1 \leqslant i \leqslant \deg P$.
3. Montrer que le morphisme $\tilde{\varphi} : A_1[X] \to L[X]$ induit par $\varphi$ envoie $P - \prod_{i=1}^{\deg P} (X - T_{P,i})$ sur $0$ (pour tout $P \in \mathcal{I}_1$), et aboutir à une contradiction.

   Soit maintenant $J$ un idéal maximal de $A$ contenant $I$ (qui existe d'après ce qui précède), on note $\Omega$ le corps $A/J$, qui est une extension de $K$.
4. Montrer que tout polynôme irréductible de $K[X]$ est scindé sur $\Omega$.
5. En utilisant l'exercice 2, montrer que $K$ admet une clôture algébrique (*théorème de Steinitz*).
6. Montrer que si $F$ et $F'$ sont deux clôtures algébriques de $K$, elles sont isomorphes (on appliquera le lemme de Zorn aux $K$-morphismes de $E$ dans $F'$, où $E$ est une extension intermédiaire entre $K$ et $F$).

**Exercice 4 — Extensions linéairement disjointes.** Soit $K$ un corps. Soient $K_1$, $K_2$ deux extensions de $K$ (c'est-à -dire que ce sont des corps qui sont en même temps des $K$-algèbres). On dit que $K_1$ et $K_2$ sont *linéairement disjointes* sur $K$ si la $K$-algèbre $K_1 \otimes_K K_2$ est un anneau intègre.

1. On suppose que $K_1 \simeq K[X]/(P)$, où $P$ est un polynôme irréductible sur $K$. Donner une condition nécessaire et suffisante sur $P$ pour que $K_1$ et $K_2$ soient linéairement disjointes.
2. Les extensions $\mathbf{Q}(i)$ et $\mathbf{Q}(\sqrt{2})$ sont-elles linéairement disjointes sur $\mathbf{Q}$ ? Même question pour $\mathbf{Q}(\sqrt[3]{2})$ et $\mathbf{Q}(j\sqrt[3]{2})$.

**Exercice 5 — Théorème de l'élément primitif.** Soit $K$ un corps infini. Soit $L$ un surcorps de $K$, on suppose qu'il n'existe qu'un nombre finis de corps $M$ avec $K \subseteq M \subseteq L$. On veut montrer qu'il existe $a \in L$ tel que $L = K(a)$.

1. Montrer que l'extension $L/K$ est finie.
2. On suppose que $L = K(\alpha_1, \alpha_2)$ avec $\alpha_1, \alpha_2 \in K$. En considérant les corps $K(\alpha_1 + \beta\alpha_2)$ avec $\alpha \in K$, montrer que l'un de ces corps est égal à $L$.

3. En déduire le résultat annoncé.
4. Soit réciproquement $L = K(\alpha)$ une extension de $K$ engendrée par un élément algébrique $\alpha$. Soit $M$ une extension intermédiaire entre $K$ et $L$. On note $P$ le polynôme minimal de $\alpha$ sur $K$ et $P_M$ son polynôme minimal sur $M$. Montrer que $P_M$ divise $P$ dans $L[T]$ et que l'application $M \mapsto P_M$ est injective.
5. En déduire qu'il n'y a qu'un nombre fini de telles extensions intermédiaires $M$.
6. Montrer que $\mathbf{F}_p(X, Y)$ admet une extension finie qui n'est pas engendrée par un élément (autrement dit le théorème de l'élément primitif tombe en défaut sur ce corps imparfait).

**Exercice 6 — Un exemple classique.** Montrer que le polynôme $X^4 + 1$ est irréductible sur $\mathbf{Q}$. Soit $L$ un corps de rupture pour ce polynôme. Comment $X^4 + 1$ se factorise-t-il sur $L$ ?

**Exercice 7 — Quelques exemples explicites.**

1. Montrer que pour tous nombres rationnels $a$ et $b$, $\mathbf{Q}(\sqrt{a}, \sqrt{b}) = \mathbf{Q}(\sqrt{a} + \sqrt{b})$.
2. A-t-on que $\mathbf{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5}) = \mathbf{Q}(\sqrt{2} + \sqrt{3} + \sqrt{5})$ ?
3. Calculer le degré de $\sqrt{2} + \sqrt[3]{3}$.

**Exercice 8.** On considère l'extension $\mathbf{Q}(i, \sqrt[4]{2})$ de $\mathbf{Q}$.

1. Montrer que le groupe de Galois de cette extension est égal au produit semi-direct $\langle\alpha\rangle \rtimes \{1, \tau\}$, où $\tau$ est la conjugaison complexe et où $\alpha(\sqrt[4]{2}) = i\sqrt[4]{2}$ et $\alpha(i) = i$.
2. Montrer que cette extension est galoisienne.
3. Donner le treillis des sous-groupes de $\mathrm{Gal}(\mathbf{Q}(i, \sqrt[4]{2})/\mathbf{Q})$.
4. Donner le treillis des extensions de $\mathbf{Q}$ contenues dans $\mathbf{Q}(i, \sqrt[4]{2})$.

**Exercice 9 — Calcul de groupes de Galois.** Déterminer le groupe de Galois de chacune des extensions de corps ou chacun des polynômes suivants.

1. $\mathbf{Q}(\sqrt{2}, \sqrt{3})$ sur $\mathbf{Q}$.
2. $X^3 - 10$ sur $\mathbf{Q}$, puis sur $\mathbf{Q}(\sqrt{2})$.
3. $X^3 - X - 1$ sur $\mathbf{Q}$.
4. $X^n - t$ sur $\mathbf{C}(t)$, puis sur $\mathbf{R}(t)$ (où $t$ est transcendant sur $\mathbf{C}$).
5. $X^5 - pqX + p$ sur $\mathbf{Q}$, où $p$ est un nombre premier et $q \geqslant 2$ est un entier.

**Remarque** : Le livre *Algebra* de Serge Lang contient des dizaines d'exercices de ce type.

**Exercice 10 — Discriminants.** Soit $K$ un corps de caractéristique différente de 2, et soit $P \in K[X]$ un polynôme séparable. Soit $L$ un corps de décomposition de $P$ sur $K$, et soient $r_1, \ldots, r_n$ les racines de $P$ dans $L$. On rappelle que le discriminant de $P$ est un élément de $K$ qui peut être défini par

$$\Delta = \prod_{i<j} (r_i - r_j)^2.$$

1. Soit $d = \prod_{i<j}(r_i - r_j) \in L$. Montrer que l'extension $K(d)/K$ est galoisienne de degré 1 ou 2.
2. On voit $\mathrm{Gal}(L/K)$ comme un sous-groupe de $\mathfrak{S}_n$ agissant par permutation des racines de $P$. Montrer qu'un élément $\sigma$ de $\mathrm{Gal}(L/K)$ fixe $d$ si, et seulement si, $\sigma \in \mathrm{Gal}(L/K) \cap \mathfrak{A}_n$.
3. En déduire que $K(d)$ est l'extension de $K$ correspondant au sous-groupe $\mathrm{Gal}(L/K) \cap \mathfrak{A}_n$ de $\mathrm{Gal}(L/K)$.

**Exercice 11.** Soit $P \in \mathbf{R}[X]$ un polynôme de degré 3 et de discriminant $\Delta$. Montrer que

1. $P$ a des racines multiples si $\Delta = 0$;
2. $P$ a trois racines réelles distinctes si $\Delta > 0$; et
3. $P$ a deux racines complexes conjuguées et une racine réelle si $\Delta < 0$.

**Exercice 12.** Soient $t$ un élément transcendant sur $\mathbf{C}$, et $K = \mathbf{C}(t)[u]/(u^2 + t^2 - 1)$.

1. Montrer que $K$ est un corps, que l'on notera $\mathbf{C}(t, u)$.
2. Montrer que l'extension $\mathbf{C}(t, u)$ de $\mathbf{C}(t^n, u^n)$ est galoisienne, et calculer son groupe de Galois.
3. Montrer que l'élément $u_n = \frac{1}{2}((t + iu)^n + (t - iu)^n)$ est dans $\mathbf{C}(t^n, u^n)$, pour tout entier strictement positif $n$.
4. Utiliser les questions précédentes pour montrer que $\cos(nx)$ s'exprime comme fonction rationnelle de $\cos^n(x)$ et $\sin^n(x)$.

**Exercice 13.** Soit $K$ un corps de caractéristique $p \neq 0$, et soit $a$ un élément de $K$ qui ne peut pas s'écrire comme $b^p - b$, avec $b \in K$. Trouver le groupe de Galois du polynôme $X^p - X - a$.

**Exercice 14 — Théorème de Wedderburn.** Tout anneau à division fini est commutatif. Un *anneau à division* est un anneau (non nécessairement commutatif) dont tous les éléments non nuls admettent un inverse. Soit $A$ un anneau à division fini et soit $Z(A)$ son centre (c'est un corps). Soit $n$ la dimension de $A$ sur $Z(A)$, et soit $q$ l'ordre de $Z(A)$.

1. En utilisant l'équation des classes, montrer que

$$q^n - 1 = q - 1 + \sum \frac{q^n - 1}{q^d - 1},$$

où la somme est prise sur les représentants d'éléments non dans $Z(A)^\times$, et $d$ est la dimension du centralisateur de cet élément sur $Z(A)$.

2. Montrer qu'alors $\Phi_n(q)$ divise $q - 1$.

3. Montrer que si $n > 1$, alors $\Phi_n(q) > q - 1$.
*Indication : utiliser la décomposition de $\Phi_n(X)$ en facteurs linéaires dans $\mathbf{C}[X]$.*

4. Conclure que $A = Z(A)$ et que $A$ est un corps.