

FEUILLE TD 5 – ALGÈBRE – CORPS ET THÉORIE DE GALOIS

EXERCICE 1 — CORPS PARFAITS. Soit K un corps. Soit $\sigma : K \rightarrow K$ 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 ALGÈBRIQUEMENT 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 $A := K[(T_{P,i})_{P \in \mathcal{I}, 1 \leq i \leq \deg P}]$ 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 $K[(T_{P,i})_{P \in \mathcal{I}_1, 1 \leq i \leq \deg P}]$. Montrer qu'il existe un morphisme de K -algèbres φ 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 $1 \leq i \leq \deg P$.

3. Montrer que le morphisme $\tilde{\varphi} : A_1[X] \rightarrow L[X]$ induit par φ 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 Ω le corps A/J , qui est une extension de K .

4. Montrer que tout polynôme irréductible de $K[X]$ est scindé sur Ω .
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 -morphisms 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 . 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 $K_1 = K(\theta)$ pour θ un élément algébrique. Donner une condition nécessaire et suffisante sur P pour que K_1 et K_2 soient linéairement disjointes.
2. Montrer que si K_1 ou K_2 est algébrique, la condition est équivalente au fait que $K_1 \otimes_K K_2$ soit un corps.
3. 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 $\mathbf{Q}(j\sqrt{2})$.
4. On note $K_1 K_2$ l'extension de K engendrée par K_1 et K_2 . On appelle $K_1 K_2$ le *compositum* de K_1 et K_2 . On suppose dans cette question que K_1 et K_2 sont deux extensions galoisiennes. Montrer alors que la condition d'être linéairement disjointes est équivalente au fait que $K_1 \cap K_2 = K$.
5. Sous les mêmes hypothèses que la question précédente, montrer qu'on a un isomorphisme entre $\text{Gal}(K_1 K_2 / K)$ et le produit direct de $\text{Gal}(K_1 / K)$ et $\text{Gal}(K_2 / K)$.

EXERCICE 5 — CARACTÉRISATION DES EXTENSIONS SIMPLES D'ARTIN. Soit K un corps infini. Soit L un surcorps de K , on suppose qu'il n'existe qu'un nombre fini 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 $\beta \in K$, 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 α . Soit M une extension intermédiaire entre K et L . On note P le polynôme minimal de α 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 $\mathbb{F}_p(X, Y)$ 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 \mathbb{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 , $\mathbb{Q}(\sqrt{a}, \sqrt{b}) = \mathbb{Q}(\sqrt{a} + \sqrt{b})$.
2. A-t-on que $\mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5}) = \mathbb{Q}(\sqrt{2} + \sqrt{3} + \sqrt{5})$?
3. Calculer le degré de $\sqrt{2} + \sqrt[3]{3}$.
4. Montrer que pour $a_1, \dots, a_\ell \in \mathbb{N}$ et $d_1, \dots, d_\ell \in \mathbb{N}$, on a

$$\mathbb{Q}(\sqrt[d_1]{a_1}, \dots, \sqrt[d_\ell]{a_\ell}) = \mathbb{Q}(\sqrt[d_1]{a_1} + \dots + \sqrt[d_\ell]{a_\ell}).$$

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

1. Montrer que le groupe de Galois de cette extension est égal au produit semi-direct $\langle \alpha \rangle \rtimes \{1, \tau\}$, où τ 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 $\text{Gal}(\mathbb{Q}(i, \sqrt[4]{2})/\mathbb{Q})$.
4. Donner le treillis des extensions de \mathbb{Q} contenues dans $\mathbb{Q}(i, \sqrt[4]{2})$.

EXERCICE 9 — CALCUL DE GROUPES DE GALOIS. Déterminer le groupe de Galois de chacune des extensions de corps ou chacun des polynômes suivants.

1. $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ sur \mathbb{Q} .
2. $X^3 - 10$ sur \mathbb{Q} , puis sur $\mathbb{Q}(\sqrt{2})$.
3. $X^3 - X - 1$ sur \mathbb{Q} .
4. $X^n - t$ sur $\mathbb{C}(t)$, puis sur $\mathbb{R}(t)$.
5. $X^5 - pqX + p$ sur \mathbb{Q} , où p est un nombre premier et $q \geq 2$ 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, \dots, 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 $\text{Gal}(L/K)$ comme un sous-groupe de \mathfrak{S}_n agissant par permutation des racines de P . Montrer qu'un élément σ de $\text{Gal}(L/K)$ fixe d si, et seulement si, $\sigma \in \text{Gal}(L/K) \cap \mathfrak{A}_n$.
3. En déduire que $K(d)$ est l'extension de K correspondant au sous-groupe $\text{Gal}(L/K) \cap \mathfrak{A}_n$ de $\text{Gal}(L/K)$.

EXERCICE 11. Soit $P \in \mathbb{R}[X]$ un polynôme de degré 3 et de discriminant Δ . 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 $\mathbf{C}(t)$ le corps des fractions rationnelles à coefficients dans \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 — EXAMEN 2020. Soient K un corps et L une extension finie et galoisienne de K . On pose $G = \text{Gal}(L/K)$. Soient F_1, F_2 deux extensions de K avec $K \subseteq F_i \subseteq L$ pour $i \in \{1, 2\}$. On pose $G_i = \text{Gal}(L/F_i)$ pour $i \in \{1, 2\}$ de sorte que G_1, G_2 soient deux sous-groupes de G .

1. On suppose que $F_1 \cap F_2 = K$. Montrer que la partie $G_1 \cup G_2$ engendre le groupe G .
2. Montrer réciproquement que si $G_1 \cup G_2$ engendre le groupe G , alors $F_1 \cap F_2 = K$.

Dans toute la suite, on note F le sous-corps de L engendré par $F_1 \cap F_2$.

3. Montrer que $F = L$ si, et seulement si, $G_1 \cap G_2 = \{\text{Id}\}$.
4. On suppose que F_1, F_2 sont des extensions galoisiennes de K qui vérifient $F_1 \cap F_2 = K$ et $F = L$. Montrer que le groupe G est isomorphe au produit direct $G_1 \times G_2$.
5. Montrer que le résultat de la question précédente ne vaut plus forcément si F_1 et F_2 ne sont pas supposées galoisiennes sur K .
6. On revient au cas général où F_1, F_2 sont des extensions intermédiaires quelconques entre K et L . Montrer qu'il existe un morphisme surjectif de K -algèbres de $F_1 \otimes_K F_2$ dans F , mais que ces deux K -algèbres peuvent ne pas être isomorphes.

EXERCICE 15 — EXAMEN 2021. Soit K un corps. On considère une extension galoisienne L de K et on pose $G = \text{Gal}(L/K)$. Soit p un nombre premier. On suppose que $|G| = p^m a$ avec $m \in \mathbf{N}$ et a un entier non divisible par p .

1. Montrer qu'il existe une extension F de K telle que $[F : K] = a$.
2. Soient F, F' deux extensions de degré a de K avec $F, F' \subseteq L$. Montrer qu'il existe $\sigma \in G$ tel que $\sigma(F) = F'$.
3. On suppose G abélien. On note e l'exposant de G . Soit d un diviseur de e . Montrer qu'il existe une extension galoisienne $E \subseteq L$ de K telle que $\text{Gal}(L/E) \cong \mathbf{Z}/d\mathbf{Z}$.
4. Le résultat de la question précédente vaut-il encore si G n'est plus supposé abélien?

EXERCICE 16 — EXAMEN 2022. 1. Soit K un corps et n un nombre premier. Montrer que si le polynôme $X^n - 1$ est scindé sur une extension L de K de degré n , il est scindé sur K .

2. Montrer que le résultat précédent tombe en défaut pour $n = 4$.
3. Soit L une extension galoisienne finie d'un corps K , de groupe de Galois $G = \text{Gal}(L/K)$. On considère \mathcal{E} l'ensemble des extensions intermédiaires M , c'est-à-dire des corps M vérifiant $K \subseteq M \subseteq L$. Montrer qu'il existe $M_1 \in \mathcal{E}$ tel que M_1 soit une extension galoisienne de K avec $\text{Gal}(M_1/K)$ abélien et tel que tout $M \in \mathcal{E}$ qui a la même propriété soit contenu dans M_1 .
4. On prend $K = \mathbf{Q}$ et $L = \mathbf{Q}(j, \sqrt[3]{2})$, où j est une racine primitive cubique de l'unité. Quelle est l'extension M_1 de la question précédente?
5. On reprend les notations de 3. mais on suppose seulement que L est séparable (pas nécessairement galoisienne) sur K . Montrer que le résultat de 3. vaut encore.

EXERCICE 17 — 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.