Théorie des corps

1 Extensions de corps

Exercice 1. *Soit K et L des corps et $f : K \to L$ un morphisme d'anneaux. Montrer que f est injectif.*

Définition 1.1. *Soit K et L des corps. On dit que L est une **extension de corps** de K lorsqu'il existe un morphisme d'anneaux $f : K \to L$. On note alors que L/K est une extension de corps.*

Remarque 1.2. D'après l'exercice précédent, cela revient à supposer que K est inclus dans L.

Si L/K est une extension de corps, alors L est une K-algèbre, en particulier un K-espace vectoriel, ce qui justifie la définition suivante.

Définition 1.3. *On dit que l'extension de corps L/K est **finie** lorsque L est de dimension finie en tant qu'espace vectoriel. On appelle alors **degré**, et on note $[L : K]$, cette dimension. Dans le cas contraire, on dit que l'extension est de **degré infini**.*

Exemple 1.4.

1. K/K est de degré 1 pour n'importe quel corps.
2. $\mathbb{C}/\mathbb{R}$ est de degré 2.

Exercice 2. *Montrer que $\mathbb{R}/\mathbb{Q}$ est de degré infini.*

Théorème 1.5 (de la base télescopique)**.** *Soit L/K et M/L des extensions de corps. Si $(e_i)_{i\in I}$ est une K-base de L et $(f_j)_{j\in J}$ est une L-base de M, alors $(e_i f_j)_{i\in I, j\in J}$ est une K-base de M. En particulier, si L/K et M/L sont des extensions finies, alors M/K aussi et*

$$[M : K] = [M : L][L : K].$$

Exercice 3. *Soit L/K une extension finie. Montrer qu'il existe $n \in \mathbb{N}, \alpha_1, \dots, \alpha_n \in L$ tels que $L = K(\alpha_1, \dots, \alpha_n)$.*

Proposition 1.6. *Soit L/K une extension de corps et $P, Q \in K[X]$ avec $Q \neq 0$. Alors la division euclidienne de P par Q dans $L[X]$ est la même que celle dans $K[X]$.*

Démonstration. La division euclidienne de P par Q nécessite seulement de faire des opérations dans le sous-corps de K engendré par leurs coefficients, qui est également un sous-corps de L. □

Corollaire 1.7. *Soit L/K une extension de corps et $P, Q \in K[X]$ non tous les deux nuls. Alors le PGCD de P et Q dans $L[X]$ est le même que celui dans $K[X]$ (« Le PGCD est invariant par extension de corps »).*

Démonstration. Le PGCD peut être obtenu en appliquant l'algorithme d'Euclide, qui consiste à faire des divisions euclidiennes successives. □

2 Éléments algébriques

Définition 2.1. *Soit L/K une extension de corps. Un élément $\alpha \in L$ est dit* ***algébrique*** *sur K lorsqu'il existe $P \in K[X] \setminus \{0\}$ tel que $P(\alpha) = 0$. Un élément de L qui n'est pas algébrique sur K est dit* ***transcendant*** *sur K. On dit que L/K est* ***algébrique*** *lorsque tous les éléments de L sont algébriques sur K.*

Exemple 2.2. i est algébrique sur $\mathbb{R}$ et sur $\mathbb{C}$. π est algébrique sur $\mathbb{R}$ mais transcendant sur $\mathbb{Q}$ (pas facile).

Proposition 2.3. *Soit L/K une extension de corps et $\alpha \in L$ algébrique sur K. Il existe un unique polynôme unitaire $m_\alpha \in K[X]$, appelé* ***polynôme minimal*** *de α sur K, tel que $\{P \in K[X] \mid P(\alpha) = 0\} = (m_\alpha)$. De plus, m_α est irréductible dans $K[X]$.*

Démonstration. L'ensemble $I = \{P \in K[X] \mid P(\alpha) = 0\}$ est un idéal de $K[X]$ (c'est le noyau du morphisme d'évaluation en α), non trivial car α est algébrique sur K, et puisque $K[X]$ est principal (car euclidien), il est engendré par un polynôme non nul P et ses associés, dont un seul est unitaire. L'un des facteurs irréductibles de m_α est dans I par intégrité de K et est donc divisible par m_α, ce qui veut dire que m_α est irréductible dans $K[X]$. □

Remarque 2.4. m_α est aussi le polynôme unitaire de plus petit degré dans $K[X]$ s'annulant en α.

Exercice 4. *Soit L/K et M/L des extensions de corps et $\alpha \in M$ algébrique sur K. Montrer que α est algébrique sur L et donner un lien entre ses polynômes minimaux sur K et sur L respectivement.*

Exercice 5. *Déterminer les polynômes minimaux de i, $\sqrt{2}$, $\sqrt{2+\sqrt{2}}$, $\sqrt{3+2\sqrt{2}}$ sur $\mathbb{Q}, \mathbb{R}$ et $\mathbb{C}$.*

Proposition 2.5. *Soit L/K une extension de corps et $\alpha \in L$. Les propriétés suivantes sont équivalentes :*

1. *α est algébrique sur K.*
2. *$K[\alpha]$ est un K-espace vectoriel de dimension finie.*
3. *$K[\alpha] = K(\alpha)$.*
4. *La famille $(\alpha^n)_{n\in\mathbb{N}}$ est liée sur K.*

Démonstration.

1. $\Rightarrow$ 2. Par définition, $K[\alpha]$ est l'image de $K[X]$ par le morphisme d'évaluation en α. Le premier théorème d'isomorphisme (pour les espaces vectoriels !) donne donc $K[\alpha] \simeq K[X]/(m_\alpha)$. Notons d le degré de m_α. Alors $(\overline{1}, \overline{X}, \ldots, \overline{X}^{d-1})$ est une base de $K[X]/(m_\alpha)$. Le caractère générateur se voit par division euclidienne et le caractère libre se voit par minimalité du degré de m_α. En particulier, $K[\alpha]$ est de dimension finie.

2. $\Rightarrow$ 3. $K[\alpha]$ est une K-algèbre intègre de dimension finie, donc est un corps (l'endomorphisme de multiplication par $x \neq 0$ est injectif, donc surjectif), et c'est clairement le plus petit corps contenant K et α, c'est-à-dire $K(\alpha)$.

3. $\Rightarrow$ 4. α est inversible dans le corps $K(\alpha) = K[\alpha]$ donc il existe $Q \in K[X]$ tel que $\alpha Q(\alpha) - 1 = 0$, ce qui constitue une relation de dépendance linéaire non triviale entre les puissances de α.

4. $\Rightarrow$ 1. Une relation de dépendance linéaire non triviale entre les puissances de α donne une égalité de la forme $P(\alpha) = 0$ avec $P \in K[X] \setminus \{0\}$.

□

Remarque 2.6. On a vu dans la démonstration que le degré de $K[\alpha]$ sur K est exactement le degré du polynôme minimal m_α, aussi appelé le **degré** de α.

Corollaire 2.7. *Soit L/K une extension de corps. L'ensemble des éléments de L algébriques sur K est une extension algébrique de K.*

Démonstration. Pour montrer qu'il s'agit d'un anneau, il suffit de voir que $\alpha+\beta, \alpha\beta \in K(\alpha)(\beta)$ qui est de dimension finie sur K par le théorème de la base télescopique. Enfin si $\alpha \in L$ est algébrique non nul, alors $K[1/\alpha] \subset K(\alpha) = K[\alpha]$ est aussi de dimension finie sur K. □

Exercice 6. *Montrer qu'une extension finie est algébrique. Montrer que la réciproque est fausse.*

3 Corps de rupture et de décomposition

Définition 3.1. *Soit K un corps et $P \in K[X]$ irréductible. On dit qu'une extension de corps L/K est un **corps de rupture** de P sur K lorsque P admet une racine $\alpha \in L$ et que $L = K(\alpha)$.*

Remarque 3.2. ⚠ On ne parlera de corps de rupture que pour des polynômes irréductibles !

Exemple 3.3. $\mathbb{C}$ est un corps de rupture de $X^2 + 1$ sur $\mathbb{R}$.

Proposition 3.4. *Soit K un corps et $P \in K[X]$ irréductible. Alors il existe un corps de rupture de P sur K. De plus, un tel corps est unique à isomorphisme près.*

Démonstration. Considérons l'anneau-quotient $K[X]/(P)$. Comme P est irréductible et $K[X]$ principal, l'idéal (P) est maximal, et $K[X]/(P)$ est donc un corps L. De plus, $\overline{X}$ est une racine de P dans L, puisque si $P = \sum_{k=0}^{n} a_k X^k$ alors

$$P(\overline{X}) = \sum_{k=0}^{n} a_k \overline{X}^k = \overline{\sum_{k=0}^{n} a_k X^k} = \overline{P} = \overline{0}.$$

Enfin, il est clair que $L = K(\overline{X})$ par double inclusion.

Pour l'unicité, si $K(\alpha)$ est un corps de rupture de P sur K, alors il existe un morphisme de $K[X]$ dans $K(\alpha)$ envoyant X sur α (par propriété universelle de l'anneau des polynômes) et ce morphisme se factorise par un morphisme de $K[X]/(P)$ dans $K(\alpha)$ envoyant $\overline{X}$ sur α (par propriété universelle du quotient). On vérifie alors immédiatement que ce morphisme est un isomorphisme. □

Théorème 3.5 (de l'élément primitif)**.** *Soit K un corps de caractéristique 0 et L/K une extension finie. Alors il existe $\theta \in L$ tel que $L = K(\theta)$.*

Remarque 3.6. Autrement dit, en caractéristique 0, toute extension finie est un corps de rupture. C'est également le cas pour les **corps parfait** (c'en est même une caractérisation), c'est-à-dire de caractéristique 0 ou de caractéristique $p > 0$ avec Frobenius surjectif.

Définition 3.7. *Soit K un corps et $P \in K[X]$. On dit que P est **scindé** lorsqu'il peut s'écrire comme produit de polynômes de degré 1. Une extension de corps L/K est un **corps de décomposition** de P sur K lorsque P est scindé dans $L[X]$ et $L = K(\alpha_1, \dots, \alpha_n)$, où $\alpha_1, \dots, \alpha_n \in L$ sont les racines de P dans L.*

Proposition 3.8. *Soit K un corps et $P \in K[X]$. Alors il existe un corps de décomposition de P sur K. De plus, un tel corps est unique à isomorphisme près.*

Démonstration. On raisonne par récurrence sur le degré de P. Si $\deg P = 1$, alors K est un corps de décomposition de P. Sinon, factorisons P comme produit d'irréductibles

$$P = \prod_{i=1}^{r} P_i^{m_i}$$

dans l'anneau factoriel $K[X]$. Considérons un corps de rupture L de P_1 sur K. Alors $L = K(\alpha)$ avec α une racine de P_1. Par hypothèse de récurrence, il existe une extension M/L telle que $P/P_1^{m_1}$ est scindé dans M et $M = L(\alpha_1, \dots, \alpha_n)$ où $\alpha_1, \dots, \alpha_n$ sont les racines de $P/P_1^{m_1}$ dans M. Alors P est scindé dans M et on a $M = K(\alpha, \alpha_1, \dots, \alpha_n)$ et ces dernières sont les racines de P dans M. L'unicité est fastidieuse, elle consiste à montrer qu'on peut toujours prolonger un isomorphisme de corps à chaque étape de la récurrence. □

Remarque 3.9. ⚠ Le corps de rupture d'un polynôme irréductible n'est pas toujours son corps de décomposition. Par exemple, le corps de rupture de $X^3 - 2$ sur $\mathbb{Q}$ est une extension de degré 3 alors que son corps de décomposition est de degré 6 sur $\mathbb{Q}$.

Exercice 7. *Soit K un corps et $P \in K[X]$ de degré $n \geq 1$. Montrer que le corps de décomposition de P sur K est de degré au plus $n!$ sur K.*

Définition 3.10. *On dit qu'un corps K est **algébriquement clos** lorsqu'il n'admet pas d'autre extension algébrique que lui-même.*

Exercice 8. *Montrer que les propriétés suivantes sont équivalentes :*

1. *K est algébriquement clos.*
2. *Tout polynôme non constant dans $K[X]$ est scindé dans $K[X]$.*
3. *Tout polynôme non constant dans $K[X]$ admet une racine dans K.*
4. *Les polynômes irréductibles de $K[X]$ sont les polynômes de degré 1.*

Exemple 3.11. $\mathbb{C}$ est algébriquement clos (Théorème de d'Alembert-Gauss ou « Théorème fondamental de l'algèbre »).

Définition 3.12. *Soit L/K une extension de corps. On dit que L est un **clôture algébrique** de K lorsque L/K est algébrique et L est un corps algébriquement clos.*

Théorème 3.13 (Steinitz)**.** *Tout corps admet une clôture algébrique. De plus, celle-ci est unique à isomorphisme près.*

Remarque 3.14. Encore une fois, ce résultat fait appel à l'axiome du choix, donc est non constructif.

Définition 3.15. *La clôture algébrique de K est notée $\overline{K}$.*

Exercice 9. *Est-ce que $\overline{\mathbb{Q}} = \mathbb{C}$?*

4 Exercices

Exercice 10. *Après avoir montré qu'ils sont irréductibles dans $\mathbb{Q}[X]$, déterminer les corps de rupture et de décomposition des polynômes*

$$X^2+1, X^2-2, X^3-2, X^4+1.$$

Exercice 11. *En utilisant le fait que $\mathbb{C}$ est algébriquement clos, déterminer les polynômes irréductibles de $\mathbb{R}[X]$.*

Exercice 12. *Soit L/K une extension finie de degré p premier. Montrer qu'il n'existe aucune sous-extension F telle que $K \subsetneq F \subsetneq L$.*

Exercice 13. *Soit K un corps et $P \in K[X]$ de degré n. Montrer que P est irréductible dans $K[X]$ si et seulement s'il n'existe aucune extension L/K avec $[L:K] \leq n/2$ dans laquelle P admet une racine.*

Exercice 14. *Montrer que $\mathbb{Q}(\sqrt{2},\sqrt{3}) = \mathbb{Q}(\sqrt{2}+\sqrt{3})$.*

Exercice 15. *Un corps de rupture est-il unique à unique isomorphisme près ?*

Exercice 16. *Montrer que $\overline{\mathbb{Q}}$ est dénombrable.*

Exercice 17. *Soit L/K une extension de corps et $M \in \mathcal{M}_n(K)$. Montrer que le rang de M, vue comme matrice dans $\mathcal{M}_n(L)$, est égal au rang de M, vue comme matrice dans $\mathcal{M}_n(K)$. Faire de même avec le polynôme caractéristique et le polynôme minimal.*

Remarque. Deux matrices de $\mathcal{M}_n(K)$ semblables dans $\mathcal{M}_n(L)$ le sont dans $\mathcal{M}_n(K)$. Pour le voir, on peut le montrer pour les matrices compagnons et invoquer la réduction de Frobenius.

Exercice 18. *Soit L/K une extension finie. Pour $\alpha \in L$, notons $N_{L/K}(\alpha)$ le déterminant de l'application K-linéaire $x \mapsto \alpha x$.*

1. *Montrer que pour tout $\alpha \in L$, $N_{L/K}(\alpha) \in K$ et que pour tout $\alpha, \beta \in L$, $N_{L/K}(\alpha\beta) = N_{L/K}(\alpha)N_{L/K}(\beta)$.*
2. *Déterminer $N_{L/K}$ lorsque $K = \mathbb{R}$ et $L = \mathbb{C}$.*
3. *Déterminer $N_{L/K}$ lorsque $K = \mathbb{Q}$ et $L = \mathbb{Q}(\sqrt{d})$ avec $d \in \mathbb{Z}$ (on note $\sqrt{d} = i\sqrt{|d|}$ lorsque $d < 0$).*
4. *Supposons que $L = K(\alpha)$. Déterminer $N_{L/K}(\alpha)$.*

Exercice 19. *Montrer que si K est un corps fini et L/K est une extension finie, alors il existe $\theta \in L$ tel que $L = K(\theta)$.*

Exercice 20. *Soit $P \in \mathbb{C}[X]$ unitaire et non constant. Nous allons montrer que P admet une racine dans $\mathbb{C}$.*

1. *Montrer que l'on peut supposer que P est à coefficient réels.*
2. *On note $d = 2^n q$, avec $n, q \in \mathbb{N}$ et q impair, le degré de P. On va montrer le résultat par récurrence sur l'exposant n : Justifier le cas $n = 0$.*

3. *Supposons $n \in \mathbb{N}^*$ et le fait que tout polynôme réel de degré $2^k q'$ avec $k < n$ et q' impair admet une racine dans $\mathbb{C}$. Soit K le corps de décomposition de P sur $\mathbb{C}$ et écrivons*

$$P = \prod_{i=1}^{d} (X - \alpha_i)$$

dans $K[X]$. Pour $x \in \mathbb{R}$ et $1 \leq i \leq j \leq d$, posons $\beta_{i,j}(x) = \alpha_i + \alpha_j + x\alpha_i\alpha_j$ et

$$Q_x = \prod_{1 \leq i \leq j \leq d} (X - \beta_{i,j}(x)).$$

Justifier que, pour tout $x \in \mathbb{R}$, $Q_x \in \mathbb{R}[X]$.

4. *Montrer que, pour tout $x \in \mathbb{R}$, Q_x admet une racine dans $\mathbb{C}$.*

5. *En déduire qu'il existe $i \leq j$ tels que $\alpha_i + \alpha_j \in \mathbb{C}$ et $\alpha_i\alpha_j \in \mathbb{C}$.*

6. *Conclure que $\alpha_i, \alpha_j \in \mathbb{C}$.*

Remarque. Le corps $\mathbb{R}$ a la propriété particulière que tout polynôme de degré impair y admet une racine, à cause du théorème des valeurs intermédiaires. Cette propriété est en fait équivalente au fait que $\mathbb{R}$ est un **corps réel clos**, c'est-à-dire que sa clôture algébrique est de degré 2 sur $\mathbb{R}$. Ainsi, il est impossible de démontrer le théorème de d'Alembert-Gauss « sans analyse ».

Exercice 21. *Soit L/K une extension finie et Ω/K une extension, avec Ω algébriquement clos (on ne dit pas que Ω est une clôture algébrique de K !).*

1. *Montrer qu'il existe un corps intermédiaire $K \subset F \subset L$ et un morphisme de corps $f : F \to \Omega$ maximal pour la relation $(F, f) \preccurlyeq (F', f')$ définie par $F \subset F'$ et $f'_{|F} = f$.*

2. *Montrer que $F = L$. En déduire que toute extension finie de K se plonge dans Ω.*

   Remarque. *C'est en fait vrai pour tout extension algébrique, mais on a besoin du lemme de Zorn. C'est comme cela que l'on montre l'unicité de la clôture algébrique d'un corps.*

3. *Supposons maintenant que $L = K(\alpha)$ est le corps de rupture du polynôme irréductible $P \in K[X]$, avec $P(\alpha) = 0$ (c'est par exemple le cas si K est de caractéristique 0 ou est fini). Montrer que les morphismes de corps de L dans Ω correspondent aux racines de P dans Ω.*

4. *En déduire que si P est scindé dans L, alors l'ensemble des morphismes de corps de L dans Ω est un groupe fini d'ordre au plus $[L : K]$. À quelle condition est-il d'ordre $[L : K]$?*

Remarque. Sous les bonnes hypothèses (extension normale — P scindé — et séparable — P n'a que des racines simples), on a donc montré que le **groupe de Galois** G de L/K est d'ordre $[L : K]$. La **correspondance de Galois** donne une bijection décroissante entre les extensions intermédiaires $L/K/F$ et les sous-groupes de G. La correspondance va plus loin puisqu'elle identifie les extensions intermédiaires telles que F/K est galoisienne aux sous-groupes distingués de G !