Leçon 125. Extensions de corps. Exemples et applications.

1. Généralités sur les extensions de corps

1.1. Sur-corps et notion de degré

1. Définition. Une *extension de corps* est la donnée de deux corps K et L et d'un morphisme de corps $K \longrightarrow L$. On dira que le corps L est un *sur-corps* de K.

2. Remarque. Le morphisme $K \longrightarrow L$ sera souvent omis et l'extension sera notée sous la forme L/K.

3. Exemple. Pour un corps K, l'application identité $K \longrightarrow K$ définie une extension. Le corps $\mathbf{C}$ est une extension de $\mathbf{R}$.

4. Proposition. Soit $\iota\colon K \longrightarrow L$ une extension de corps. Alors la loi de composition externe $(\lambda, x) \in K \times L \longmapsto \lambda \cdot x \coloneqq \iota(\lambda)x \in L$ munit l'ensemble L d'une structure de K-espace vectoriel.

5. Définition. Une extension L/K est *finie* si le K-espace vectoriel L est de dimension finie. Dans ce cas, son *degré* est la dimension de ce dernier, notée $[L : K]$.

6. Exemple. Les extensions $\mathbf{C}/\mathbf{R}$ et $\mathbf{Q}(i)/\mathbf{Q}$ sont degré 2.

7. Remarque. Dans le cas où les corps K et L sont finis, l'extension L/K est finie et on peut écrire $|L| = |K|^{[L:K]}$.

8. Théorème *(de la base téléscopique)*. Soient M/L et L/K deux extensions. Soient $(e_i)_{i\in I}$ une base du K-espace vectoriel L et $(f_j)_{j\in J}$ une base du L-espace vectoriel M. Alors la famille $(e_i f_j)_{(i,j)\times I\times J}$ est une base du K-espace vectoriel M.

9. Corollaire *(multiplicativité du degré)*. Soient M/L et L/K deux extensions finies. Alors $[M : K] = [M : L][L : K]$.

10. Définition. Une extension L/K est *monogène* s'il existe un existe un élément $\alpha \in L$ tel que le corps L soit le plus petit sous-corps $K(\alpha)$ de L contenant l'élément α.

11. Théorème *(de l'élément primitif)*. Soient K un corps de caractéristique nulle et L/K une extension finie. Alors il existe un élément $\alpha \in K$ tel que $L = K[\alpha]$.

12. Remarque. Le résultat reste vrai si corps K est fini.

1.2. Extensions algébriques

13. Définition. Soit L/K une extension. Un élément $\alpha \in L$ est *algébrique* sur L s'il existe un polynôme non constant $P \in K[X]$ tel que $P(\alpha) = 0$. Dans ce cas, l'ensemble

$$\{P \in K[X] \mid P(\alpha) = 0\}$$

est un idéal de $K[X]$, donc il admet une unique générateur unitaire $\pi_\alpha \in K[X]$, appelée le *polynôme minimal* de l'élément α sur K. Dans le cas contraire, l'élément α est *transcendant* sur K.

14. Remarque. Le polynôme π_α est irréductible sur K.

15. Exemple. Tout élément de K est algébrique sur K. Le nombre $\sqrt{2}$ est algébrique sur $\mathbf{Q}$, mais le nombre π y est transcendant.

16. Définition. Une extension L/K est *algébrique* si et seulement si tout élément du corps L est algébrique sur K.

17. Proposition. Soient L/K une extension et $\alpha \in L$ un élément transcendant. Alors

$$K[\alpha] \simeq K[X] \qquad \text{et} \qquad K(\alpha) \simeq K(X).$$

18. Théorème. Soient L/K une extension et $\alpha \in L$ un élément. Alors les points suivants sont équivalents :
- l'élément α est algébrique sur K ;
- $K[\alpha] = K(\alpha)$;
- le K-espace vectoriel $K[\alpha]$ est de dimension finie.

19. Corollaire. Tout extension finie est algébrique.

20. Théorème. Soit L/K une extension. Alors l'ensemble des éléments de L algébriques sur K est un sous-corps de L.

21. Remarque. L'ensemble $\overline{\mathbf{Q}}$ des nombres complexes algébriques sur $\mathbf{Q}$ est donc un sous-corps de $\mathbf{C}$. Mais cette extension n'est pas fini.

22. Remarque. Soient L/K une extension et $\alpha, \beta \in L$ deux éléments algébriques sur K. Alors un polynôme annulateur de l'élément $\alpha + \beta$ est le polynôme

$$\mathrm{Res}_X(\pi_\alpha(X), \mathrm{Res}_Y(\pi_\beta(Y), Z - X - Y)) \in K[Z].$$

1.3. Clôture algébrique

23. Définition. Un corps K est algébriquement clos si tout polynôme non constant de $K[X]$ admet une racine dans K.

24. Proposition. Soit K un corps. Alors les points suivants sont équivalents :
- le corps K est algébriquement clos ;
- tout polynôme de $K[X]$ est scindé ;
- les polynômes irréductibles de $K[X]$ sont les polynômes de degré un ;
- toute extension algébrique L/K vérifie $L = K$.

25. Théorème *(d'Alembert-Gauss)*. Le corps $\mathbf{C}$ est algébriquement clos.

26. Théorème. Le corps $\overline{\mathbf{Q}}$ est algébriquement clos.

27. Définition. Une *clôture* d'un corps K est une extension algébrique L/K telle que le corps L soit algébriquement clos.

28. Théorème. Un corps K admet une clôture algébrique et il est unique à isomorphismes de corps qui conserve K près.

2. Construction d'extensions par adjonction de racines

2.1. Corps de rupture et de décomposition

29. Définition. Soient K un corps et $P \in K[X]$ un polynôme irréductible sur K. Un *corps de rupture* du polynôme irréductible P sur K est une extension L/K s'écrivant sous la forme $L = K(\alpha)$ pour un élément $\alpha \in L$ vérifiant $P(\alpha) = 0$.

30. Théorème. Soit $P \in K[X]$ un polynôme irréductible sur K. Alors il admet un corps de rupture sur K. De plus, deux tels corps sont isomorphes au corps $K[X]/(P)$.

31. Exemple. Le corps $\mathbf{C} \simeq \mathbf{R}[X]/(X^2 + 1)$ des complexes est un corps de rupture du polynôme $X^2 + 1$ sur $\mathbf{R}$.

32. Définition. Soit $P \in K[X]$ un polynôme. Un *corps de décomposition* du polynôme P sur K est une extension $L \supset K$ telle que
- le polynôme P soit scindé sur L ;
- le corps L est minimal pour le point ci-dessus.

33. Théorème. Tout polynôme de $K[X]$ admet un corps de décomposition sur K, unique à isomorphismes près.

34. Exemple. Le corps $\mathbf{Q}(\sqrt[3]{2}, j)$ est un corps de décomposition du polynôme $X^3 - 2$ sur $\mathbf{Q}$.

2.2. Construction des corps finis

35. Théorème. Soient p un nombre premier et $n \in \mathbf{N}^*$ un entier non nul. Alors il existe un unique corps de cardinal $q \coloneqq p^n$ à isomorphisme près et il s'agit du corps de décomposition du polynôme $X^q - X$ sur $\mathbf{F}_p$. On le note $\mathbf{F}_q$.

36. Exemple. Attention, le corps $\mathbf{F}_q$ ne correspond pas à l'anneau $\mathbf{Z}/q\mathbf{Z}$.

37. Exemple. Le corps $\mathbf{F}_4$ s'obtient comme le quotient $\mathbf{F}_2[X]/\langle X^2 + X + 1\rangle$.

38. Théorème. Le groupe $\mathbf{F}_q^\times$ est isomorphe au groupe cyclique $\mathbf{Z}/(q-1)\mathbf{Z}$.

39. Théorème. Soient $m, n \in \mathbf{N}^*$ deux entiers non nuls. Alors il existe un morphisme de corps $\mathbf{F}_{p^m} \longrightarrow \mathbf{F}_{p^n}$ si et seulement si $m \mid n$.

40. Théorème. Soit $n \in \mathbf{N}^*$ un entier non nuls. Alors l'ensemble $\bigcup_{k \in \mathbf{N}^*} \mathbf{F}_{p^{k!}}$ est une clôture algébrique du corps $\mathbf{F}_{p^n}$.

3. Les extensions de corps en algèbre

3.1. Les polynômes cyclotomiques

41. Notation. On considère un corps K de caractéristique $p \geqslant 0$ et un entier $n > 0$. On suppose que $p \nmid n$.

42. Définition. Une *racine n-ième de l'unité* est un élément $\xi \in K$ tel que $\xi^n = 1$. Elle est *primitive* si $\xi^d \neq 1$ pour $d < n$. On note $\mu_n(K)$ (resp. $\mu_n^\times(K)$) les ensembles de racines n-ième (resp. primitives).

43. Définition. Soit K_n un corps de décomposition du polynôme $X^n - 1$ sur K. Le *n-ième polynôme cyclotomique* est le polynôme

$$\Phi_{n,K} \coloneqq \prod_{\xi \in \mu_n^\times(K_n)} (X - \xi) \in K_n[X].$$

44. Remarque. Le polynôme $\Phi_{n,K}$ est unitaire de degré $\varphi(n) = |(\mathbf{Z}/n\mathbf{Z})^\times|$.

45. Proposition. On a

$$X^n - 1 = \prod_{d \mid n} \Phi_{d,K}.$$

46. Exemple. On peut calculer $\Phi_{1,\mathbf{Q}} = X - 1$, $\Phi_{2,\mathbf{Q}} = X + 1$ et $\Phi_{3,\mathbf{Q}} = X^2 + X + 1$.

47. Théorème *(Wedderburn)*. Tout corps fini est commutatif.

48. Proposition. On a $\Phi_n \coloneqq \Phi_{n,\mathbf{Q}} \in \mathbf{Z}[X]$. Soit $\sigma \colon \mathbf{Z} \longrightarrow K$ l'unique morphisme d'anneaux que l'on étend en un morphisme d'anneaux $\sigma \colon \mathbf{Z}[X] \longrightarrow K[X]$ en envoyant l'indéterminée X sur elle-même. Alors $\Phi_{n,K} = \sigma(\Phi_{n,\mathbf{Q}})$.

49. Théorème. Le polynôme $\Phi_n \coloneqq \Phi_{n,\mathbf{Q}}$ est irréductible sur $\mathbf{Z}$ et donc sur $\mathbf{Q}$.

50. Corollaire. Soit $\xi \in \mu_n^\times(\mathbf{C})$. Alors son polynôme minimal sur $\mathbf{Q}$ est le polynôme Φ_n. En particulier, on a $[\mathbf{Q}(\zeta) : \mathbf{Q}] = \varphi(n)$.

3.2. Construction à la règle et au compas

51. Notation. On fixe un ensemble $E \subset \mathbf{R}^2$ contenant au moins deux éléments. Notons $F \subset \mathbf{R}$ l'ensemble des abscisses et ordonnées des points de l'ensemble E. On pose $\mathbf{K} \coloneqq \mathbf{Q}(F)$.

52. Définition. Un point du plan $\mathbf{R}^2$ est *constructible en une étape* à partir de E s'il est une intersection
- d'une droite d'extrémités dans E et d'un cercle de centre dans E ;
- de deux droites distincts d'extrémités dans E ;
- ou de deux cercles distincts de centres dans E dont les rayons sont des distances entre de points de E.

Il est *constructible en n étapes* à partir de E s'il existe n points $P_1, \ldots, P_n = P$ du plan tels que, pour tout entier $i \in [\![1, n]\!]$, le point P_i soit constructible en une étape à partir de l'ensemble $E \cup \{P_1, \ldots, P_j\}$.

53. Proposition. Soit $(p, q) \in \mathbf{R}^2$ un point constructible en une étape à partir de E. Alors le corps $\mathbf{K}(p, q)$ est le corps $\mathbf{K}$ ou une extension quadratique de $\mathbf{K}$.

54. Théorème. Soit $(p, q) \in \mathbf{R}^2$ un point constructible en une étape à partir des points $(0, 0)$ et $(1, 0)$. Alors il existe une tour d'extensions $\mathbf{K}_m / \cdots / \mathbf{K}_0$ telle que
- on ait $(p, q) \in \mathbf{K}_m \subset \mathbf{R}$;
- pour tout indice $i \in [\![1, m-1]\!]$, on a $[\mathbf{K}_{i+1} : \mathbf{K}_i] = 2$.

[1] Michèle Audin. *Géométrie*. EDP Sciences, 2006.
[2] Josette Calais. *Extensions de corps*. Ellipses, 2006.
[3] Xavier Gourdon. *Algèbre*. 2e édition. Ellipses, 2009.
[4] Daniel Perrin. *Cours d'algèbre*. Ellipses, 1996.