Leçon 123. Corps finis. Applications.

I. Corps finis : sous-corps premiers et construction

I.1. Caractéristique, sous-corps premiers et groupe des inversibles

1. Définition. Un *corps fini* est un corps $(K, +, \times)$ dont l'ensemble K est fini.
2. Théorème. Soit $p \geqslant 1$ un entier. L'anneau fini $\mathbf{Z}/p\mathbf{Z}$ est un corps si et seulement si l'entier p est premier. Dans ce cas, ce corps est noté $\mathbf{F}_p$.
3. Exemple. L'anneau $\mathbf{F}_2 \coloneqq \mathbf{Z}/2\mathbf{Z}$ est un corps fini.
4. Définition. Le *sous-corps premier* d'un corps est son plus petit sous-corps.
5. Exemple. Le sous-corps premier du corps $\mathbf{R}$ ou $\mathbf{C}$ est le corps $\mathbf{Q}$.
6. Définition. La *caractéristique* d'un corps K est l'unique générateur $p \in \mathbf{N}$ du noyau du morphisme d'anneaux $n \in \mathbf{Z} \longmapsto n \cdot 1_K$.
7. Théorème. La caractéristique d'un corps est soit nulle, soit un nombre premier.
8. Exemple. Le corps $\mathbf{R}$ ou $\mathbf{C}$ est de caractéristique nulle. Pour un nombre premier p, le corps $\mathbf{F}_p$ sont de caractéristique p.
9. Proposition. Un corps de caractéristique nulle est infini.
10. Contre-exemple. La réciproque est fausse : le corps $\mathbf{F}_p(T)$ est infini et il n'est pas de caractéristique nulle.
11. Proposition. Soit K un corps de caractéristique $p > 0$. Le *morphisme de Frobenius*
$$F\colon x \in K \longmapsto x^p \in K$$
est un morphisme de corps. De plus, si le corps K est fini, alors le morphisme F est un automorphisme.
12. Théorème. Soit K un corps fini de caractéristique $p > 0$. Alors son cardinal $|K|$ est une puissance du nombre p.

I.2. Construction des corps premiers et étude de leurs groupes des inversibles

13. Théorème. Soient p un nombre premier et $n \geqslant 1$ un entier. Notons $q \coloneqq p^n$.
   - Il existe un corps à q éléments et ce dernier est un corps de décomposition du polynôme $X^q - X$ sur $\mathbf{F}_p$.
   - En particulier, il est unique à isomorphisme près. On le note $\mathbf{F}_q$.
14. Remarque. Attention, dès que $n \geqslant 2$, le corps $\mathbf{F}_q$ n'est pas l'anneau $\mathbf{Z}/q\mathbf{Z}$.
15. Exemple. Le corps $\mathbf{F}_4$ s'obtient comme l'anneau quotient $\mathbf{F}_2[X]/(X^2 + X + 1)$.
16. Théorème. Soient $m, n \geqslant 1$ deux entiers. Alors il existe une injection $\mathbf{F}_{p^m} \longrightarrow \mathbf{F}_{p^n}$ si et seulement si $m \mid n$.
17. Exemple. Les sous-corps de $\mathbf{F}_{16}$ sont les corps $\mathbf{F}_2$, $\mathbf{F}_4$ et $\mathbf{F}_{16}$.
18. Théorème. Soit K un corps. Tout sous-groupe fini de $K^\times$ est fini.
19. Corollaire. Soit q une puissance d'un nombre premier. Alors le groupe $\mathbf{F}_q^\times$ est isomorphe au groupe $\mathbf{Z}/(q-1)\mathbf{Z}$.

II. Polynômes, algèbre linéaire et bilinéaire sur un corps finis

II.1. Polynômes irréductibles et cyclotomiques, le théorème de Wedderburn

20. Proposition. Un corps fini n'est pas algébriquement clos.
21. Lemme. Soient q une puissance d'un nombre premier et $n \in \mathbf{N}^*$ un entier. Pour un entier $n \in \mathbf{N}$, notons $I(q, d) \subset \mathbf{F}_q[X]$ l'ensemble des polynômes de degré d irréductible sur $\mathbf{F}_q$. Alors
$$X^{q^n} - X = \prod_{d \mid n} \prod_{P \in I(q,d)} P.$$
22. Théorème. Sous les mêmes hypothèses, on a
$$\sum_{d \mid n} d\,|I(q,d)| = q^n \qquad \text{et} \qquad |I(n,q)| = \frac{1}{n} \sum_{d \mid n} \mu\Big(\frac{n}{d}\Big)\, q^d.$$
23. Exemple. On a $|I(2,3)| = \frac{1}{2}(\mu(2) \times 3^1 + \mu(1) \times 3^2) = 3$.
24. Théorème. Soient A un anneau factoriel, K son corps des fractions, $I \subset A$ un idéal, $B \coloneqq A/I$ l'anneau quotient et L son corps des fractions. Soit $P \in A[X]$ un polynôme. S'il est irréductible sur B ou L, alors il est irréductible sur K.
25. Exemple. On prend $A = \mathbf{Z}$. Alors le polynôme $X^3 + 462X^2 + 2433X - 67491$ est irréductible sur $\mathbf{Q}$ puisque sa réduction $X^3 + X + 1$ est irréductible sur $\mathbf{F}_2 = \mathbf{Z}/(2)$.
26. Théorème. Soient $P \in \mathbf{F}_{p^n}[X]$ un polynôme de degré $d > 0$. Les points suivants sont équivalents :
   - il est irréductible sur $\mathbf{F}_{p^n}$;
   - pour tout entier $m \in \mathbf{N}^*$ tel que $n \mid m$ tel que $p^m \leqslant dp^n/2$, il n'admet pas de racines dans $\mathbf{F}_{p^m}$.
27. Exemple. Le polynôme $X^4 + X + 1$ est irréductible sur $\mathbf{F}_2$.
28. Théorème. Les polynômes cyclotomiques $\Phi_n \in \mathbf{Z}[X]$ sont irréductibles sur $\mathbf{Q}$ et sur $\mathbf{Z}$.
29. Corollaire *(Wedderburn)*. Tout corps fini est commutatif.

II.2. Algèbre linéaire : critère de diagonalisabilité et dénombrement

30. Proposition. Soient $n \geqslant 1$ un entier et q une puissance d'un nombre premier. Alors
$$|\mathrm{GL}_n(\mathbf{F}_q)| = (q^n - 1)(q^n - q) \cdots (q^n - q^{n-1}) \quad \text{et} \quad |\mathrm{SL}_n(\mathbf{F}_q)| = \frac{\mathrm{GL}_n(\mathbf{F}_q)}{q-1}.$$
31. Théorème. Le nombre de matrices nilpotentes de taille n à coefficients dans $\mathbf{F}_q$ vaut $q^{n(n-1)}$.
32. Lemme. Un endomorphisme d'un $\mathbf{F}_q$-espace vectoriel de dimension finie est diagonalisable si et seulement s'il est annulé par le polynôme $X^q - X \in \mathbf{F}_q[X]$.
33. Théorème. Le nombre de matrices diagonalisables de $\mathrm{GL}_n(\mathbf{F}_q)$ vaut
$$\sum_{\substack{(n_1, \dots, n_{q-1}) \in \mathbf{N}^{q-1} \\ n_1 + \cdots + n_{q-1} = n}} \frac{|\mathrm{GL}_n(\mathbf{F}_q)|}{|\mathrm{GL}_{n_1}(\mathbf{F}_q)| \cdots |\mathrm{GL}_{n_{q-1}}(\mathbf{F}_q)|}.$$

D1

II.3. Algèbre bilinéaire : classification des formes quadratiques sur un corps finis

34. Définition. Le *discriminant* d'une forme quadratique sur un K-espace vectoriel de dimension finie est la classe de son déterminant dans $K^\times / K^{\times 2}$.
35. Lemme. Soient q une puissance d'un nombre premier et $a, b, c \in \mathbf{F}_q^\times$ trois éléments. Alors l'équation $ax^2 + by^2 = c$ admet une solution dans $\mathbf{F}_q^2 \setminus \{(0,0)\}$.
36. Théorème. Soit q une puissance d'un nombre premier impair. Alors deux matrices symétriques sur $\mathbf{F}_q$ sont congruentes si et seulement si elle ont le même discriminant.

III. Les carrés d'un corps fini

III.1. Définition et premières caractérisations

37. Définition. Un élément x d'un corps K est un *carré* s'il existe un élément $y \in K$ tel que $x = y^2$. On note $K^2 \subset K$ l'ensemble des carrés et on pose $K^{\times 2} := K^2 \cap K^\times$.
38. Proposition. Soit q une puissance d'un nombre premier p.
   - Si $p = 2$, alors $\mathbf{F}_q^{\times 2} = \mathbf{F}_q$.
   - Si $p > 2$, alors $|\mathbf{F}_q^2| = (q+1)/2$ et $|\mathbf{F}_q^{\times 2}| = (q-1)/2$.

39. Exemple. Les carrés dans $\mathbf{F}_9$ sont 0, 1, 4, 9 et 7.
40. Proposition. On suppose que $p > 2$. Pour tout élément $x \in \mathbf{F}_q$, on a

$$x \in \mathbf{F}_q^{\times 2} \quad \Longleftrightarrow \quad x^{(q-1)/2} = 1.$$

41. Exemple. L'élément 2 est un carré dans $\mathbf{F}_7$ puisque $2^{(7-1)/2} = 2^3 = 1$, mais les éléments -1 et 3 n'en sont pas.
42. Corollaire. On suppose que $p > 2$. Alors l'élément $-1 \in \mathbf{F}_q$ est un carré si et seulement si $q \equiv 1 \mod 4$.
43. Application. Il existe une infinité de nombre premier de la forme $4m + 1$ pour un entier $m \in \mathbf{N}$.

III.2. Le symbole de Legendre et la loi de réciprocité quadratique

44. Définition. Soient p un nombre premier impair. Pour tout élément $a \in \mathbf{F}_p$, son *symbole de Legendre* est l'entier

$$\left(\frac{a}{p}\right) := a^{(p-1)/2} = \begin{cases} 1 & \text{si } a \in \mathbf{F}_p^{\times 2}, \\ -1 & \text{si } a \in \mathbf{F}_p^\times \setminus \mathbf{F}_p^{\times 2}, \\ 0 & \text{si } a = 0. \end{cases}$$

45. Exemple. En reprenant l'exemple précédent, on a $(\frac{2}{7}) = 1$ et $(\frac{-1}{7}) = (\frac{3}{7}) = -1$.
46. Proposition. Pour tout élément $a \in \mathbf{F}_p^\times$, on a

$$|\{x \in \mathbf{F}_p \mid ax^2 = 1\}| = 1 + \left(\frac{a}{p}\right).$$

47. Proposition. Pour tout nombre premier impair, on a

$$\left(\frac{-1}{p}\right) = (-1)^{(p-1)/2} \qquad \text{et} \qquad \left(\frac{2}{p}\right) = (-1)^{(p^2-1)/8}.$$

Autrement dit,
   - l'entier -1 est un carré modulo p si et seulement si $p \equiv 1 \mod 4$;
   - l'entier 2 est un carré modulo p si et seulement si $p \equiv \pm 1 \mod 8$;

48. Théorème. L'application

$$a \in \mathbf{F}_p^\times \longmapsto \left(\frac{a}{p}\right) \in \{\pm 1\}$$

est un morphisme de groupes.
49. Théorème *(loi de réciprocité quadratique).* Soient p et q deux nombres premiers impairs. Alors D2

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{(p-1)/2 \times (q-1)/2}.$$

50. Exemple. Avec les quatre derniers points, on trouve

$$\left(\frac{14}{23}\right) = \left(\frac{2}{23}\right)\left(\frac{7}{23}\right) = \left(\frac{7}{23}\right) = -\left(\frac{23}{7}\right) = -\left(\frac{2}{7}\right) = -1.$$

Ainsi l'entier 14 n'est pas un carré modulo 23.

[1] Philippe Caldero et Jérôme Germoni. *Histoires hédonistes de groupes et de géométries*. T. Tome second. Calvage & Mounet, 2015.
[2] Philippe Caldero et Jérôme Germoni. *Nouvelles histoires hédonistes de groupes et de géométries*. T. Tome premier. Calvage & Mounet, 2017.
[3] Xavier Gourdon. *Algèbre*. 2e édition. Ellipses, 2009.
[4] Daniel Perrin. *Cours d'algèbre*. Ellipses, 1996.