123 CORPS FINIS. APPLICATIONS.

Soit $\mathcal{P}$ l'ensemble des nombres premiers. Les corps considérés seront supposés commutatifs.

I. Notion de corps fini

[Per96, §3.2, p72–76] [Rom17, Ch13, p415]

I. A. Vocabulaire général sur les corps

Cloture algébrique unique à isomorphisme près (admis).
Corps de rupture / de décomposition.
Théorème de WEDDERBURN

I. B. Premiers résultats

DÉFINITION 1. Un corps fini est un corps de cardinal fini.

PROPOSITION 2. *Pour $p \in \mathcal{P}$, $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ est un corps fini à p éléments.*

PROPOSITION 3. *Soit $\mathbb{K}$ un corps. L'application $\mathbb{Z} \longrightarrow \mathbb{K}, m \longmapsto m1_K$ est un morphisme d'anneaux de noyau $n\mathbb{Z}$ pour un $n \in \mathbb{N}$.*

DÉFINITION 4. L'image de cette application est un sous-corps de $\mathbb{K}$ appelé sous-corps premier. n est appelé caractéristique de $\mathbb{K}$, noté $\mathrm{car}(\mathbb{K})$.

PROPOSITION 5. *Si $\mathbb{K}$ est fini, on a $\mathrm{car}(\mathbb{K}) \in \mathcal{P}$.*

APPLICATION 6. Le sous-corps premier de $\mathbb{K}$ est alors isomorphe à $\mathbb{Z}/p\mathbb{Z}$.

Pour $p \in \mathcal{P}$, on note $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$.

COROLLAIRE 7. *Si $\mathbb{K}$ est un corps fini de caractéristique p, alors $\mathbb{K}$ est un $\mathbb{F}_p$-espace vectoriel où $p = \mathrm{car}(\mathbb{K})$, de cardinal p^n où $n = \dim_{\mathbb{F}_p}(\mathbb{K})$.*

APPLICATION 8. Il n'existe par de corps à 6 éléments.

I. C. Existence et unicité

Soit $p \in \mathcal{P}$ et $n \in \mathbb{N}^*$. Soit $q = p^n$.

DÉFINITION 9. [MORPHISME DE FROBENIUS]
Soit $\mathbb{K}$ un corps de caractéristique p. $\mathrm{Frob} : \mathbb{K} \longrightarrow \mathbb{K}, x \longmapsto x^p$ est un morphisme de corps appelé morphisme de FROBENIUS.

PROPOSITION 10. *Frob est injectif et si $\mathbb{K}$ est fini, c'est un automorphisme.*

PROPOSITION 11. *Pour $\mathbb{K} = \mathbb{F}_p$, on a $\mathrm{Frob} = \mathrm{Id}$.*

PROPOSITION 12. *Soit $\overline{\mathbb{F}_p}$ une clôture algébrique de $\mathbb{F}_p$. Alors l'ensemble des racines de $X^{p^n} - X$ dans $\overline{\mathbb{F}_p}$ est un sous-corps de $\overline{\mathbb{F}_p}$ à $q = p^n$ éléments, contenant $\mathbb{F}_p$.*

COROLLAIRE 13. *Il existe un corps fini à q éléments, unique à isomorphisme près : c'est le corps de décomposition de $X^q - X$ sur $\mathbb{F}_p$. On le note $\mathbb{F}_q$.*

II. Eléments de structure

[Per96, §III.2, p73]

II. A. Structure d'un corps fini

$\mathbb{F}_q$ est un $\mathbb{F}_p$-espace vectoriel de dimension n, donc isomorphe à $\mathbb{F}_p^n$
$\mathbb{F}_q^\times = \mathbb{F}_q^*$ est cyclique, donc isomorphe à $(\mathbb{Z}/(q-1)\mathbb{Z}, +)$
Racine primitive, nombre de racines primitives
Élement primitif : une racine primitive est un élément primitif

II. B. Inclusion entre corps finis

PROPOSITION 14. *Les sous-corps de $\mathbb{F}_{p^n}$ sont les $\mathbb{F}_{p^d}$ pour $d \mid n$.*

THÉORÈME 15. [THÉORÈME DE LA BASE TÉLESCOPIQUE]
Soient $\mathbb{K}, \mathbb{L}, \mathbb{M}$ des corps, $(e_i)_{i\in I}$ une base de $\mathbb{L}$ sur $\mathbb{K}$, $(f_j)_{j\in J}$ une base de $\mathbb{M}$ sur $\mathbb{L}$. Alors $(e_i f_j)_{(i,j)\in I\times J}$ est une base de $\mathbb{M}$ sur $\mathbb{K}$.
En particulier, lorsque deux des degrés d'extensions sont finis, le troisième aussi et on a $[\mathbb{M} : \mathbb{K}] = [\mathbb{M} : \mathbb{L}][\mathbb{L} : \mathbb{K}]$.

APPLICATION 16. On a alors $[\mathbb{F}_{p^n} : \mathbb{F}_{p^d}] = \frac{n}{d}$.

EXEMPLE 17. Schéma des inclusions des sous-corps de $\mathbb{F}_{2^{20}}$.

II. C. Structure du groupe des isomorphismes

[Rom17, §13.4, p426]

$\mathrm{Aut}(\mathbb{F}_q)$ est un groupe de neutre id
Si $f \in \mathrm{Aut}(\mathbb{F}_q)$, alors $\mathbb{F}_p \subset \{x \in \mathbb{F}_q \mid f(x) = x\}$
$\mathrm{Aut}(\mathbb{F}_q)$ est cyclique d'ordre n, engendré par Frob

III. Applications

III. A. Résolution d'équations de degré 2

[Rom17, §13.6-7, p429-435] [Per96, §III.2, p72-76]

Soit $p \in \mathcal{P}$ et $q = p^n$ où $n \in \mathbb{N}^*$. On note $\mathbb{F}_q^2 = \left\{x^2 \mid x \in \mathbb{F}_q\right\}$ et $\mathbb{F}_q^{*2} = \mathbb{F}_q^2 \cap \mathbb{F}_q^*$.

Proposition 18. *Si $p = 2$, alors $\mathbb{F}_q^2 = \mathbb{F}_q$. Sinon, on a $\left|\mathbb{F}_q^2\right| = \frac{q+1}{2}$.*

Application 19. Pour $a, b \in \mathbb{F}_p^*$ et $c \in \mathbb{F}_p$, $ax^2 + by^2 = c$ admet des solutions dans $\mathbb{F}_p^2$.

On suppose dans la suite p impair.

Lemme 20. *On a $x \in \mathbb{F}_q^{*2} \iff x^{\frac{q-1}{2}} = 1$.*

Exemple 21. -1 est un carré modulo q si et seulement si $q \mid 1 \mod 4$.

Exemple 22. Dans $\mathbb{Z}/7\mathbb{Z}$, 2 est un carré mais par 3.

On aimerait savoir rapidement si un entier a donné est un carré modulo p, donc savoir si $x^2 \equiv a \mod p$ admet ou non une solution entière.

Définition 23. [Symbole de Legendre]
Soit $a \in \mathbb{Z}$, on appelle symbole de Legendre (de a modulo p) l'entier :

$$\left(\frac{a}{p}\right) = \begin{cases} 1 & \text{si } x^2 \equiv a \mod p \text{ est résoluble et } p \nmid a \\ 0 & \text{si } p \mid a \\ -1 & \text{sinon} \end{cases}$$

Proposition 24. *On a $\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \mod p$ pour tout $a \in \mathbb{Z}$.*

Proposition 25. *$\left(\frac{a}{p}\right) = \left(\frac{a+kp}{p}\right)$ pour tout $a, k \in \mathbb{Z}$. On peut donc définir $\overline{x} \in \mathbb{F}_p \longmapsto \left(\frac{x}{p}\right)$. C'est l'unique morphisme de groupes non trivial de $(\mathbb{F}_p^*, \times)$ vers $(\{\pm 1\}, \times)$.*

Remarque 26. Le nombre de solutions de $x^2 = a$ pour $a \in \mathbb{F}_p$ est $1 + \left(\frac{a}{p}\right)$.

Théorème 27. [Loi de réciprocité quadratique]
Soient $p \neq q$ des nombres premiers impairs. Alors $\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}$.

Proposition 28. *Pour p premier impair, on a $\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$. Ainsi 2 est un carré modulo p si et seulement si $p \equiv \pm 1 \mod 8$.*

On peut donc calculer $\left(\frac{n}{p}\right)$ pour tout entier n :

Exemple 29. $\left(\frac{26}{307}\right) = \left(\frac{2}{307}\right)\left(\frac{13}{307}\right) = -(-1)^{\frac{13-1}{2}\frac{307-1}{2}}\left(\frac{307}{13}\right) = -\left(\frac{8}{13}\right) = -\left(\frac{2}{13}\right)\left(\frac{4}{13}\right) = -1$
Ainsi 26 n'est pas un carré modulo 307.

III. B. Irréductibilité dans $\mathbb{Z}[X]$ et $\mathbb{Q}[X]$, réduction modulo p

[Per96, §3.3-3.4, p76-85]

Proposition 30. *Un polynôme de degré supérieur ou égal à 1 est irréductible dans $\mathbb{Z}[X]$ si et seulement si il est de contenu 1 et irréductible dans $\mathbb{Q}[X]$.*

Proposition 31. [Critère d'Eisenstein]
Soit $P = \sum_{i=0}^r a_i X^i \in \mathbb{Z}[X]$. Soit $p \in \mathcal{P}$. Si $p \nmid a_r$, $\forall i < r, p \mid a_i$ et $p^2 \nmid a_0$, alors P est irréductible dans $\mathbb{Q}[X]$.

Exemple 32. Si $m \in \mathbb{Z}$ a un facteur premier sans carré alors $X^n - m$ est irréductible dans $\mathbb{Z}[X]$ pour tout $n \in \mathbb{N}$.

Proposition 33. *Soit $p \in \mathcal{P}$ et $P = \sum_{i=0}^r a_i X^i \in \mathbb{Z}[X]$. Soit $\overline{P}$ la réduction de P modulo p. Si $p \nmid a_n$ et si $\overline{P}$ est irréductible dans $\mathbb{F}_p[X]$, alors P est irréductible dans $\mathbb{Q}[X]$.*

Exemple 34. $X^3 + 462X^2 + 2433X - 67691$ est irréductible dans $\mathbb{Z}[X]$, tout comme $X^p - X - 1$ pour tout $p \in \mathcal{P}$.

Définition 35. [Polynômes cyclotomiques]
On définit le n-ième polynôme cyclotomique $\Phi_n \in \mathbb{C}_n[X]$ par $\Phi_n(X) = \prod_{\zeta \in \mathbb{U}_n^\times}(X - \zeta)$.

Proposition 36. $\Phi_n \in \mathbb{Z}[X]$.

Théorème 37. [Irréductibilité de Φ_n] *Φ_n est irréductible sur $\mathbb{Z}$ et donc sur $\mathbb{Q}$.*

Liens entre irréductibilité et degré des extensions [Per96, p78-79]

SPEECH

Dans la première partie, on essaie de comprendre ce qu'est un corps fini. Les outils principaux étant les notions de caractéristique et de sous-corps premier, le morphisme de FROBENIUS. Cela va mener à l' unicité du corps de cardinal p^d à isomorphisme près.
Ensuite, on regarde la structure de ces corps finis, avec notamment les racines primitives et les éléments primitifs. Le problème est qu'il n'y a pas de méthode générale pour exhiber une racine primitive. On s'intéresse aux sous-corps d'un corps fini et aux degrés des différentes extensions et on étudie également le lien entre les automorphismes du corps et le morphisme de FROBENIUS.
La dernière partie s'intéresse aux applications des corps finis, avec la résolution d'équations de degré 2 dans ces corps (loi de réciprocité quadratique), et les critères d'irréductibilité de polynômes.

COMMENTAIRES

Voir aussi le [Dem09].

BIBLIOGRAPHIE

[Dem09] M. DEMASURE : *Cours d'algèbre*. Cassini, 2009.

[Per96] D. PERRIN : *Cours d'algèbre*. Ellipses, 1996.

[Rom17] J.-E. ROMBALDI : *Mathématiques pour l'agrégation : Algèbre et géométrie*. De Boeck, 2017.