

112: Corps finis. Applications.

Pierre Lissy

May 6, 2010

On suppose connu les notions de corps, caractéristique d'un corps, extension de corps, clôture algébrique, corps de rupture d'un polynôme irréductible, corps de décomposition.

1 Réalisation des corps finis

1.1 Définition et premières propriétés

Définition 1. *Un corps fini est un corps ayant un nombre fini d'éléments.*

Exemple 1. *les $\mathbb{Z}/p\mathbb{Z}$ avec p premier sont des corps finis de cardinal p . On remarque immédiatement qu'aucun autre $\mathbb{Z}/n\mathbb{Z}$ n'est un corps.*

Remarque 1. *Un corps fini n'est jamais algébriquement clos.*

Proposition 1. *Soit K un corps fini à q éléments. Alors $\forall x \in K, x^q = x$.*

Théorème 1. *Si K est fini, K^* est un groupe cyclique (donc isomorphe à $\mathbb{Z}/(q-1)\mathbb{Z}$)*

Remarque 2. *En fait, on a le théorème plus général suivant: dans un corps, tout sous-groupe fini de K^* est cyclique.*

On peut montrer en utilisant les polynômes cyclotomiques le théorème important suivant:

Théorème 2 (Wedderburn). *La commutativité est une conséquence des autres axiomes de la structure de corps fini.*

1.2 Cardinal d'un corps fini

Proposition 2. *La caractéristique d'un corps fini est toujours différente de 0. On a donc une extension $\mathbb{Z}/p\mathbb{Z} \subset K$.*

Corollaire 1. *Le corps K supposé de caractéristique p peut être vu comme un espace vectoriel sur $\mathbb{Z}/p\mathbb{Z}$. De plus c'est un espace vectoriel de dimension fini et nécessairement $|K| = p^n$ où $n = [K : \mathbb{Z}/p\mathbb{Z}]$*

1.3 Fabrication de tous les corps finis

Théorème 3. *Soit $q = p^n$. Alors il existe un corps de cardinal q et de caractéristique p , on peut prendre par exemple le corps de décomposition du polynôme $X^q - X$ sur $\mathbb{F}_p$. De plus, K est unique à isomorphisme près. Ce corps est noté $\mathbb{F}_q$.*

Remarque 3. *Dans le cas des corps finis, le corps de rupture d'un polynôme irréductible est nécessairement le corps de décomposition de ce polynôme irréductible. En pratique, on préfère écrire les corps finis comme des corps de rupture d'un polynôme irréductible grâce au théorème suivant.*

Théorème 4. *$\mathbb{F}_{p^n}$ est le corps de rupture de tout polynôme irréductible de degré n sur $\mathbb{Z}/p\mathbb{Z}$.*

Exemple 2. $\mathbb{F}_4 \simeq \mathbb{Z}/2\mathbb{Z}[X]/(1 + X + X^2)$ $\mathbb{F}_8 \simeq \mathbb{Z}/2\mathbb{Z}[X]/(1 + X + X^3)$, $\mathbb{F}_9 \simeq \mathbb{Z}/3\mathbb{Z}[X]/(X^2 + 1)$, $\mathbb{F}_{16} \simeq \mathbb{Z}/2\mathbb{Z}[X]/(1 + X + X^4)$.

1.4 Irréductibilité des polynômes à coefficients dans un corps fini

Théorème 5. [5] Un polynôme de degré n irréductible sur $\mathbb{F}_p$ l'est sur $\mathbb{F}_{p^k}$ ssi k et n sont premiers entre eux.

Proposition 3. [2] On note K_p^d le nombre de polynômes de degré d irréductibles unitaires. $X^q - X = \prod_{d|n} \left(\prod_{Q \in K_p^d} Q \right)$.

Application 1. On note $I(n, q)$ le cardinal de K_p^d . On a $p^n = \sum_{d|n} dI(p, d)$, il existe donc toujours un polynôme irréductible de degré n .

Théorème 6. [5] soit q et n premiers entre eux. le n -ième polynôme cyclotomique Φ_n est irréductible sur $\mathbb{F}_q$ ssi q est un générateur du groupe cyclique $\mathbb{Z}/n\mathbb{Z}^*$.

2 Automorphismes, sous-corps, extensions finies de corps finis

2.1 Automorphismes d'un corps fini

Proposition 4 (Frobenius). Soit K un corps fini de caractéristique p . L'application $x \mapsto x^p$ est un morphisme de corps appelé morphisme de Frobenius. C'est un automorphisme de K et c'est l'identité si k est de cardinal p .

Corollaire 2. Le groupe des automorphismes de K est un groupe cyclique de cardinal n dont le Frobenius est un générateur.

2.2 Carrés d'un corps fini

Théorème 7. Dans un corps fini de caractéristique 2, tout nombre est un carré. Sinon, l'application $x \mapsto x^2$ est un morphisme de groupe surjectif de K^* dans $-1, 1$ donc on a exactement $q + 1/2$ carrés (il faut rajouter 0), et ceux-ci sont caractérisés par l'égalité $x^{\frac{q-1}{2}} = 1$. (si x n'est pas un carré on a $x^{\frac{q-1}{2}} = -1$.)

Corollaire 3. -1 est un carré dans K ssi q est congru à 1 modulo 4.

Application 2 (Théorème des deux carrés). Un entier est somme de deux carrés ssi la valuation de tous les nombres premiers congrus à 3 modulo 4 est paire.

Application 3. Il existe une infinité de nombres premiers vérifiant $p = 4m + 1$.

2.3 Extensions finies

[6]

Définition 2. Une extension finie L d'un corps K est une extension telle que $[L : K]$ est fini (ie L est un K -ev de dim finie. Une extension est séparable ssi tout élément de l'extension admet un polynôme minimal dans $K[X]$. Une extension est normale est une extension. Une extension séparable normale est dite galoisienne.

Théorème 8. Toute extension finie sur un corps fini est galoisienne.

2.4 Sous-corps intermédiaires

Proposition 5. $\mathbb{F}_{p^n} \subset \mathbb{F}_{p^m}$ ssi $n|m$.

Exemple 3. $\mathbb{F}_8$ n'est pas un sous-corps de $\mathbb{F}_{64}$.

Corollaire 4. $\mathbb{F}_{p^n}$ admet un unique sous-corps de cardinal $\mathbb{F}_{p^d}$ avec $d|n$. De plus, ces sous-corps sont les seuls sous-corps de $\mathbb{F}_{p^n}$. Enfin, le groupe des automorphismes de $\mathbb{F}_{p^n}$ laissant invariant $\mathbb{F}_{p^d}$ est un groupe cyclique d'ordre n/d engendré par la puissance d -ième du Frobenius.

Remarque 4. L'énoncé précédent montre qu'on peut trouver une bijection entre les sous-corps de $\mathbb{F}_{p^n}$ et les sous-groupes du groupe G des $\mathbb{F}_{p^d}$ -automorphismes de $\mathbb{F}_{p^n}$: si l'on se donne un sous-groupe H de G , alors on lui associe le corps des invariants (ie le corps tels que chaque élément de H laissent invariant $\mathbb{F}_{p^n}$). On montre en théorie de Galois que ce théorème reste vrai si l'on considère une extension (finie ou infinie) galoisienne (ie normale et séparable) d'un corps non nécessairement fini, ce qui est le cas ici.

3 Etude particulière des $\mathbb{Z}/p\mathbb{Z}$

3.1 Carrés dans $\mathbb{F}_p$

Définition 3. Un résidu quadratique modulo p est un carré de $\mathbb{F}_p$. d'après ce qu'on a vu précédemment il y en a $(p-1)/2$

Proposition 6. a est un résidu quadratique ssi l'équation $x^2 - a = 0$ a une solution dans $\mathbb{F}_p$ ssi il existe un diviseur premier de la forme $x^2 - 5y^2$ avec x et y premiers entre eux.

Définition 4. Symbole de Legendre $\left(\frac{p}{q}\right) = p^{\frac{q-1}{2}}$.

Proposition 7. Le symbole est un morphisme de groupe de $\mathbb{Z}/p\mathbb{Z}$ sur $\{-1, 1\}$. Donc l'ensemble des carrés est un groupe abélien.

Proposition 8. $\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$.

On a l'important théorème suivant

Théorème 9 (réciprocité quadratique[2]). $\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\left(\frac{p-1}{2}\frac{q-1}{2}\right)}$

Exemple 4. -627 est un carré dans $\mathbb{F}_{17}$. 5 n'est pas un carré dans $\mathbb{F}_{1987}$. -5 est un carré dans $\mathbb{F}_p$ ssi p est un nombre premier de la forme $20k + 1, 3, 7, 9$.

Application 4. Il existe une infinité de nombres premiers de la forme:

1. $6n+1$
2. $10n-1$
3. $4n-1$

Remarque 5. Cas particuliers du théorème de Dirichlet qui dit : si a et b sont premiers entre eux il existe une infinité de nombre premiers de la forme $a+nb$, mais on en connaît toujours pas de démonstration élémentaire dans le cas général.

Par ailleurs, contrairement à l'anneau $\mathbb{Z}$, on a dans $\mathbb{F}_p$

Théorème 10. [1][exo 12-14] Dans $\mathbb{F}_p$ tout élément est somme de deux carrés. On a même qu'il existe toujours une solution à l'équation $ax^2 + by^2 = c$ avec a, b, c non nuls.

3.2 Irréductibilité de polynômes

Théorème 11 (réduction modulo p). Soit p un nombre premier et soit $P \in \mathbb{Z}[X]$, $P = a_n X^n + \dots + a_0$. On pose $\bar{P} = C_p(a_n)X^n + \dots + C_p(a_0)$. Si $\bar{P}$ est irréductible dans $\mathbb{Z}/p\mathbb{Z}[X]$, alors P est irréductible dans $\mathbb{Q}[X]$ (et donc dans $\mathbb{Z}[X]$ si il est primitif).

Exemple 5. $X^3 + 462X^2 + 2433X - 67691$ est irréductible sur $\mathbb{Z}$ (car il l'est sur $\mathbb{Z}/2\mathbb{Z}[X]$)

Exemple 6. Soit p un nombre premier. $X^p - X - 1$ est irréductible sur $\mathbb{Z}$ (car il l'est sur $\mathbb{Z}/p\mathbb{Z}$).

Réciproque fausse: $X^4 + 1$ irréductible sur $\mathbb{F}_p$ mais réductible sur tous les $\mathbb{F}_p$.

Exemple 7. $X^5 + X^2 + X + 2$ irréductible sur $\mathbb{Z}$. $X^5 - 7$ irréductible sur $\mathbb{Z}$.

3.3 Polynômes cyclotomiques

Proposition 9. *Le polynôme cyclotomique sur $\mathbb{F}_p$ est la réduction modulo p du polynôme cyclotomique sur $\mathbb{Q}$ (qui est à coeff dans $\mathbb{Z}$). Le polynôme cyclotomique n'est défini que pour n et p premiers entre eux.*

En utilisant le théorème de Dirichlet on montre:

Théorème 12. *On a les équivalences suivantes.*

1. Φ_n est irréductible sur un certain $\mathbb{F}_p$
2. $\mathbb{Z}/n\mathbb{Z}^*$ est cyclique
3. $n = 2, 4, q^\alpha, 2^q \alpha$ avec q premier impair.

4 Algèbre linéaire, bilinéaire sur les corps finis

4.1 Cardinal d'un ev, des matrices triangulaires supérieures

Théorème 13. *si E est de dim n , on a $\dim(E) = q^n$.*

Théorème 14. *Le cardinal des matrices triangulaires supérieures (resp. strictes) est $p^{n(n+1)/2}$ (resp. $p^{n(n-1)/2}$)*

Application 5. *On peut se servir de ce résultat pour montrer le théorème de Sylow, en effet c'est un sous-groupe de Sylow si q est premier.*

4.2 Permutations linéaires

Théorème 15. S_n s'injecte trivialement dans $GL_n(k)$: il suffit d'envoyer σ sur la matrice des $\delta_{ij}, \sigma(i)$. De telles matrices sont orthogonales.

Théorème 16 (Frobenius-Zolotarev). *On considère un élément de $Gl_n(\mathbb{F}_p)$, notamment il peut être vu comme une permutation de F_p . Alors $\varepsilon(u) = \det(u)/p$ (symbole de Legendre)*

4.3 Groupes linéaire et spécial linéaire

Théorème 17.

$$\begin{aligned} |GL_n(\mathbb{F}_{q^n})| &= (q^n - 1) \dots (q^n - q^{n-1}), \\ |SL_n(\mathbb{F}_{q^n})| &= (q^n - 1) \dots (q^n - q^{n-2}) q^{n-1}, \\ |PGL_n(\mathbb{F}_{q^n})| &= (q^n - 1) \dots (q^n - q^{n-2}) q^{n-1}, \\ |PSL_n(\mathbb{F}_{q^n})| &= (q^n - 1) \dots (q^n - q^{n-2}) q^{n-1} / \text{pgcd}(n, q - 1). \end{aligned}$$

Théorème 18. 1. $GL_2(\mathcal{F}_2) \simeq PGL_2(\mathcal{F}_2) \simeq SL_2(\mathcal{F}_2) \simeq PSL_2(\mathcal{F}_2) \simeq \mathcal{S}_3$

2. $PGL_2(\mathcal{F}_3) \simeq \mathcal{S}_4$

3. $PSL_2(\mathcal{F}_3) \simeq \mathcal{A}_4$

4. $PGL_2(\mathcal{F}_4) \simeq PSL_2(\mathcal{F}_4) \simeq \mathcal{A}_5$

5. $PSL_2(\mathcal{F}_5) \simeq \mathcal{A}_5$

On peut montrer plus généralement:

Théorème 19. $PSL_2(\mathbb{F}_q)$ est simple pour $q \geq 4$.

Enfin on a

Théorème 20. *Tout groupe simple d'ordre 128 est isomorphe à $PSL_2(\mathbb{F}_7)$, ce qui est notamment le cas de $PSL_3(\mathbb{F}_2)$.*

4.4 Formes quadratiques

[4][page 129]

Définition 5. Soit E un k -ev de dimension n . Q est une forme quadratique sur E non dégénérée ssi son noyau (ie le noyau de sa forme polaire) est réduit à $\{0\}$. On se donne une bonne fois pour toutes une base B de E , Le discriminant d'une forme quadratique dans cette base est le déterminant de n'importe quelle matrice de la forme polaire de Q dans cette base.

Théorème 21. Dans un corps fini de caractéristique différente de deux, on considère un élément non nul qui n'est pas un carré. Alors toute forme quadratique non dégénérée sur un ev E de dimension n a une matrice de la forme Id ou $\begin{pmatrix} 1 & 0 & \dots & 0 \\ & & \dots & \\ 0 & & & \alpha \end{pmatrix}$ selon que son discriminant soit un carré ou non. De plus dans le cas où l'ev est de dimension impaire les deux classes de congruence sont isomorphes.

Définition 6. On appelle forme sesquilinéaire hermitienne relative à un automorphisme de k noté σ est une application $f : E \times E \rightarrow k$ vérifiant:

1. $x \mapsto f(x, y)$ est linéaire
2. $y \mapsto f(x, y)$ est additive et $f(\lambda x, y) = \sigma(\lambda)f(x, y)$ (semi-linéaire par rapport à σ .)
3. $f(y, x) = \sigma(f(x, y))$.

Théorème 22. soit k un corps fini de caractéristique différente de 2. Alors si k admet une involution σ non triviale, $k = \mathbb{F}_p^2$, inversément dans $k = \mathbb{F}_p^2$ involution non triviale donnée par $\sigma(x) = x^q$. De plus le corps des invariants pour cette involution est $\mathbb{F}_q$. Dans ce cas, une forme hermitienne relative à σ peut s'écrire dans une certaine base comme la matrice Id : il y a une seule classe de congruence.

References

- [1] Combes
- [2] Gourdon algèbre
- [3] Objectif agrégation
- [4] Perrin
- [5] Ortiz
- [6] Lang