123

Corps finis. Exemples et applications.

I Propriétés nécessaires

Théorème préliminaire 1 (Wedderburn) Tout corps fini est commutatif.

Contre-exemple 2 Dans le cas infini, le corps $\mathbb{H} = \left\{ \begin{pmatrix} a & -b \\ b & \bar{a} \end{pmatrix}, a, b \in \mathbb{C} \right\}$ n'est pas commutatif.

Remarque 3 Dans la suite, les corps sont supposés commutatifs.

1) Cardinal

Définition 4 Soit A un anneau intègre et $\varphi : \begin{cases} \mathbb{Z} \longrightarrow A \\ n \longmapsto n.1_A \end{cases}$

Alors $\exists ! p \in \mathbb{N}$, $\operatorname{Ker} \varphi = p\mathbb{Z}$, c'est la caractéristique de A.

Proposition 5 $\operatorname{char}(A) = 0$ ou $\operatorname{char}(A)$ est premier

Remarque 6 Un corps de caractéristique nulle est infini, car il contient $\varphi(\mathbb{Z}) \simeq \mathbb{Z}$.

Proposition 7 Soit K un corps fini de caractéristique p.

- $\exists n \in \mathbb{N}$, $|K| = p^n$
- Si $k \subseteq K$ est un sous corps, $\exists d | n$, $|k| = p^d$

Remarque 8 $\mathbb{Z}/p\mathbb{Z}$ est le sous-corps premier de K.

Définition 9 Soit K un corps de caractéristique p.

$F : \begin{cases} K \longrightarrow K \\ x \longmapsto x^p \end{cases}$ est un morphisme appelé morphisme de Frobenius.

Proposition 10 Si K est fini, F est bijectif

Application 11 (Fermat) Si p est premier et $a \in \mathbb{N}$, $a^{p-1} \equiv 1 \,[p]$

2) Groupe multiplicatif

Définition 12 Si k est un corps, $k^* := k \setminus \{0\}$ est un groupe appelé groupe multiplicatif.

Lemme 13 Si φ est l'indicatrice d'Euler,

$$\forall n \in \mathbb{N}^*, \quad n = \sum_{d | n} \varphi(d)$$

Théorème 14 Si k est un corps fini, avec $|k| = q$, k^* est cyclique. (et donc $k^* \simeq \mathbb{Z}/(q-1)\mathbb{Z}$).

Remarque 15 Il n'y a pas de formule explicite pour un générateur de k^*. Cependant si $\varphi(q-1)/(q-1)$ n'est pas trop petit, tester les éléments un par un jusqu'à trouver un générateur est envisageable.

Exemple 16 $(\mathbb{Z}/7\mathbb{Z})^*$ est engendré par $\bar{3}$.

II Existence et unicité

1) Construction

Définition 17 Une extension L d'un corps K est un corps de rupture du polynome irréductible $P \in K[X]$ s'il contient une racine α de P telle que $L = K[\alpha]$

Théorème 18 Soit p premier et $\mathbb{F}_p := \mathbb{Z}/p\mathbb{Z}$. Si $P \in \mathbb{F}_p[X]$ est irréductible de degré $n \geq 1$, $\mathbb{F}_p[X]/(P)$ est un corps de rupture de P de cardinal p^n.

DEV 1

Exemple 19 X^2+X+1 est irréductible sur $\mathbb{F}_2$ donc $K=\mathbb{F}_2[X]/(X^2+X+1)$ est un corps de rupture de X^2+X+1 de cardinal 4. $K=\mathbb{F}_2[j]=\{0,1,j,j+1\}$ où j vérifie $j^2+j+1=0$.

Lemme 20 Soit $P_n=X^{p^n}-X\in\mathbb{F}_p[X]$. Si P est un diviseur irréductible de P_n dans $\mathbb{F}_p[X]$, son degré divise n.

Réciproquement, si P est irréductible de degré un diviseur de n, alors P divise P_n.

Théorème 21 P_n est sans facteur carré et

$$P_n=\prod_{d\mid n}\Big(\prod_{\substack{P\text{ irréductible}\\ \deg P=d}}P\Big)$$

Proposition 22 Dénombrement des polynômes irréductibles de degré n dans $\mathbb{F}_p[X]$

Remarque 23 $\forall n\geq 1$, $\exists P$ irréductible de degré n dans $\mathbb{F}_p[X]$.

Théorème 24 Si $q=p^n$ où p est premier et $n\in\mathbb{N}^*$, on peut construire un corps de taille q.

2) Unicité

Théorème 25 Dans le cadre du théorème 24, le corps de cardinal q est unique à isomorphisme près.

Définition 26 On note $\mathbb{F}_q$ l'unique corps de taille q.

Exemple 27 $\mathbb{F}_9$ peut s'écrire sous la forme $\mathbb{F}_3[X]/(X^2+X+1)=\mathbb{F}_3(\alpha)$ ou $\mathbb{F}_3[X]/(X^2-X+1)=\mathbb{F}_3(\beta)$

Ces deux corps sont isomorphes via le morphisme défini par $f(\beta)=\alpha+1$.

Remarque 28 Un corps fini n'est pas algébriquement clos.

Remarque 29 Un corps de caractéristique p premier n'est pas forcément fini. Exemple: la clôture algébrique de $\mathbb{F}_p$.

Exemple 30 Table de multiplication de $\mathbb{F}_8$ (voir annexe 1)

III Carrés dans $\mathbb{F}_q$

1) Dénombrement

Proposition 31 Soit $q=p^n$ avec p premier et $n\geq 2$

On note $d=\text{pgcd}(n,q-1)$ et $P_n=\{x^n, x\in\mathbb{F}_q^*\}$

Alors $|P_n|=\frac{q-1}{d}$

Exemple 32 En particulier, $|P_2|=\frac{q-1}{2}$ et $|\mathbb{F}_q^*\setminus P_2|=\frac{q-1}{2}$

Proposition 33 Les carrés de $\mathbb{F}_q^*$ sont les racines de $X^{\frac{q-1}{2}}-1$.

Corollaire 34 -1 est un carré ssi $q\equiv 1\,[4]$

Exemple 35 -1 est un carré dans $\mathbb{F}_9$ mais pas dans $\mathbb{F}_3$

Application 36 Il existe une infinité de nombres premiers de la forme $4k+1$.

Remarque 37 Le problème général de trouver les puissances n-ièmes est difficile.

2) Résidus quadratiques

a) Symbole de Legendre

Définition 38 Soit p premier et $a \in \mathbb{F}_p^*$. $\left(\frac{a}{p}\right) := \begin{cases} 1 & \text{si } a \in \mathbb{F}_p^2 \\ -1 & \text{sinon} \end{cases}$

Exemple 39 $2 = 3^2 [7]$ donc $\left(\frac{2}{7}\right) = 1$

Théorème 40 $\forall a \in \mathbb{F}_p$, $\left(\frac{a}{p}\right) = (-1)^{\frac{p-1}{2}}$ et $a \mapsto \left(\frac{a}{p}\right)$ est l'unique morphisme $\mathbb{F}_p \longrightarrow \{\pm 1\}$

b) Loi de réciprocité quadratique

DEV 2 [**Théorème 41** p, q premiers, on a $\left(\frac{p}{q}\right) = (-1)^{\frac{(p-1)(q-1)}{4}} \left(\frac{q}{p}\right)$

Propriété 42 (Gauss) p premier impair, alors $\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{2}}$

Exemple 43 $\left(\frac{11}{83}\right) = -\left(\frac{83}{11}\right) = -\left(\frac{6}{11}\right) = -\left(\frac{2}{11}\right)\left(\frac{3}{11}\right)$ $= -1 \times (-1) \left(\frac{11}{3}\right) = -\left(\frac{-1}{3}\right) = 1$ donc 11 est un carré de $\mathbb{F}_{83}$

c) Symbole de Jacobi

Remarque 44 On ne peut appliquer les résultats précédents que si q est premier !

Définition 45 pour $a, q \in \mathbb{N}$, on pose
$$\left(\frac{a}{q}\right) = \begin{cases} 0 & \text{si } a \wedge q \neq 1 \\ \prod\limits_{\substack{p \mid q \\ p \text{ premier}}} \left(\frac{a}{p}\right)^{v_p(q)} & \text{sinon} \end{cases}$$

Proposition 46 $\left(\frac{ab}{n}\right) = \left(\frac{a}{n}\right)\left(\frac{b}{n}\right)$ et $\left(\frac{a}{mn}\right) = \left(\frac{a}{m}\right)\left(\frac{a}{n}\right)$

Théorème 47 $\forall m, n \in \mathbb{N}$, $\left(\frac{m}{n}\right)(-1)^{(m-1)(n-1)/4} = \left(\frac{n}{m}\right)$

Application 48 Si $\left(\frac{a}{n}\right) \neq 1$, a n'est pas un carré modulo n. La réciproque est fausse : $\left(\frac{2}{9}\right) = 1$ alors que 2 n'est pas un carré modulo 9

IV Espaces vectoriels sur $\mathbb{F}_q$

Propriété 49 $|GL_n(\mathbb{F}_q)| = (q^n - 1)(q^n - q) \cdots (q^n - q^{n-1})$ et $|SL_n(\mathbb{F}_q)| = \frac{1}{q-1} |GL_n(\mathbb{F}_q)|$

Application 50 (Sylow) Soit G un groupe de cardinal n et p un facteur premier de n. Alors G admet un p-Sylow.

Propriété 51 Il existe un morphisme injectif $PGL_2(\mathbb{F}_q) \longrightarrow \mathfrak{S}_{q+1}$

Application 52 $PGL_2(\mathbb{F}_3) \simeq \mathfrak{S}_4$

$PGL_2(\mathbb{F}_4) = A_4$, $PGL_2(\mathbb{F}_5) = \mathfrak{S}_5$

	1	α	$\alpha+1$	α^2	α^2+1	$\alpha^2+\alpha$	$\alpha^2+\alpha+1$
1	1	α	$\alpha+1$	α^2	α^2+1	$\alpha^2+\alpha$	$\alpha^2+\alpha+1$
α	α	α^2	$\alpha^2+\alpha$	$\alpha+1$	1	$\alpha^2+\alpha+1$	α^2+1
$\alpha+1$	$\alpha+1$	$\alpha^2+\alpha$	α^2+1	$\alpha^2+\alpha+1$	α^2	1	α
α^2	α^2	$\alpha+1$	$\alpha^2+\alpha+1$	$\alpha^2+\alpha$	α	α^2+1	1
α^2+1	α^2+1	1	α^2	α	$\alpha^2+\alpha+1$	$\alpha+1$	$\alpha^2+\alpha$
$\alpha^2+\alpha$	$\alpha^2+\alpha$	$\alpha^2+\alpha+1$	1	α^2+1	$\alpha+1$	α	α^2
$\alpha^2+\alpha+1$	$\alpha^2+\alpha+1$	α^2+1	α	1	$\alpha^2+\alpha$	α^2	$\alpha+1$

ANNEXE 1 Table de multiplication de $\mathbb{F}_8$
vu comme $\mathbb{F}_8 = \mathbb{F}_2[X]/(X^3+X+1) = \mathbb{F}_2[\alpha]$
où $\alpha^3+\alpha+1=0$

Références

- Cours d'algèbre, Daniel Perrin
- Exercices d'algèbre, Ortiz
- Cours d'algèbre, Demazure
- Mathématiques pour l'agrégation, algèbre et géométrie, Rombaldi