123

Corps finis. Applications.

[Rau] XIII.4

Soit A anneau unitaire, intègre. Soit $\mathbb{K}$ corps commutatif, p premier, $n \in \mathbb{N}^*$

I] Notion de corps fini

1] Caractéristique et sous-corps

Définition 1 : On appelle caractéristique de A l'entier $\mathrm{car}(A) = p$ tel que $\ker(\varphi) = p\mathbb{Z}$ avec $\varphi : \begin{array}{ccc} \mathbb{Z} & \to & A \\ n & \mapsto & n.1_A \end{array}$

Proposition 2 : La caractéristique de A est soit 0 soit un premier. Si elle est nulle, alors A est infini.

Contrexemple 3 : La réciproque est fausse.
$\mathbb{F}_p[X]$ est de caractéristique p mais est infini.

Définition 4 : On appelle sous-corps premier de $\mathbb{K}$ son plus petit sous-corps.

Exemple 5 : $\mathbb{Q}$ est le sous-corps premier de $\mathbb{R}$.

Définition 6 : On appelle morphisme de Frobénius l'application $f : \begin{array}{ccc} \mathbb{K} & \to & \mathbb{K} \\ x & \mapsto & x^p \end{array}$ avec $p = \mathrm{car}(\mathbb{K})$.

Exemple 7 : Si $\mathbb{K} = \mathbb{Z}/p\mathbb{Z}$, alors $F = \mathrm{id}_{\mathbb{K}}$.

Théorème 8 : Soit $\mathbb{K}$ corps de cardinal p^n avec $p = \mathrm{car}(\mathbb{K})$, $n \in \mathbb{N}^*$.
Alors : tout sous-corps de $\mathbb{K}$ est de cardinal p^d avec $d \mid n$.
Réciproquement, $\forall d \mid n$, $\exists!\ \mathbb{F}_{p^d} = \{x \in \mathbb{F}_{p^n} \mid x^{p^d} = x\}$ sous-corps de $\mathbb{K}$ de cardinal p^d.

XIII.1 [Rau] XIII.2 [Rau]

2] Existence et unicité

Notation 9 : On note $\mathcal{U}_n(p)$ l'ensemble des polynômes unitaires irréductibles de degré n sur $\mathbb{F}_p$.

Exemple 10 : $\forall \lambda \in \mathbb{F}_p$, $(X - \lambda) \in \mathcal{U}_1(p)$

XIII.4 [Rau]

Théorème 11 : $\forall P \in \mathcal{U}_n(p)$, $\mathbb{F}_p[X]/(P)$ est une $\mathbb{F}_p$-algèbre de dimension n de base $(\overline{X}^k)_{k=0}^{n-1}$ et c'est un corps fini de cardinal p^n

Exemple 12 : $\forall \lambda \in \mathbb{F}_p$, $\mathbb{F}_p[X]/(X - \lambda)$ est un corps isomorphe à $\mathbb{F}_p$.

Lemme 13 : Tout diviseur irréductible de $X^{p^n} - X$ dans $\mathbb{F}_p[X]$ est de degré diviseur n. Réciproquement, $\forall d \mid n$, $\forall P \in \mathcal{U}_d(p)$, $P \mid X^{p^n} - X$.

Théorème 14 : $X^{p^n} - X$ est sans facteurs carrés dans $\mathbb{F}_p[X]$ et

$$X^{p^n} - X = \prod_{d \mid n} \prod_{P \in \mathcal{U}_d(p)} P$$

Théorème 15 : À un isomorphisme près, il n'existe qu'un seul corps à p^n éléments : $\mathbb{F}_{p^n} = \mathbb{F}_p[X]/(P)$ avec $P \in \mathcal{U}_n(p)$.

Exemple 16 : $\mathbb{F}_4 = \mathbb{F}_2[X]/(X^2+1)$ et non pas $\mathbb{Z}/4\mathbb{Z}$!

3] Inclusions entre corps finis

Proposition 17 : $\forall a \in \mathbb{N}^*$, $\forall n, s \in \mathbb{N}$, $(a^s - 1) \mid (a^n - 1)$ ssi $s \mid n$.

Lemme 18 : $\forall n, s \in \mathbb{N}^*$, $X^s - 1 \mid X^n - 1$ dans $\mathbb{K}[X]$ ssi $s \mid n$.

Théorème 19 : Soit $n, s \in \mathbb{N}^*$.
Alors : $\mathbb{F}_{p^s}$ est un sous-corps de $\mathbb{F}_{p^n}$ ssi $s \mid n$

Proposition 20 : $\forall s \mid n$, $[\mathbb{F}_{p^n} : \mathbb{F}_{p^s}] = \frac{n}{s}$

Exemple 21 : Les sous-corps de $\mathbb{F}_{32}$ sont : $\mathbb{F}_2$; $\mathbb{F}_4$; $\mathbb{F}_8$; $\mathbb{F}_{16}$ et $\mathbb{F}_{32}$.

Théorème 22 : (de l'élément primitif) $\exists x \in \mathbb{F}_{p^n} \setminus$

$$\mathbb{F}_{p^n} = \mathbb{F}_p(x)$$

IV.4 [Cal]

II] Notion de groupe lié au corps

1] Groupe des inversibles

[Cal] IV.2

Lemme 23: Soit G groupe multiplicatif d'ordre m tel que: $\forall d|m,\ |\{x\in G \mid x^d=1\}|\leq d$
Alors: G est cyclique

Lemme 24: $\forall m\in\mathbb{N}^*,\ m=\sum_{d|m}\varphi(d)$ avec φ indicatrice d'Euler

Théorème 25: $\mathbb{F}_{p^n}^*$ est d'ordre p^n-1

Exemple 26: $(\mathbb{F}_{2^2})^\times \simeq \mathbb{Z}/3\mathbb{Z}$

Corollaire 27: Pour tout $\mathbb{K}$ corps, tout sous-groupe fini de $\mathbb{K}^\times$ est cyclique.

2] Groupe des automorphismes

[Rau] XIII.4

Remarque 28: $F\in \mathrm{Aut}(\mathbb{F}_{p^n})$ avec $\mathrm{Aut}(\mathbb{F}_{p^n})$ groupe des automorphismes de $\mathbb{F}_{p^n}$.

Proposition 29: $\forall x,y\in\mathbb{F}_{p^n},\ \forall d\in\mathbb{N}^*,\ (x-y)^{p^d}=x^{p^d}-y^{p^d}$

Proposition 30: Soit $\mathbb{K}=\mathbb{F}_p[X]/(P)$ avec $P\in\mathcal{U}_n(p)$.
Alors: l'application φ: $\mathrm{Aut}(\mathbb{K})\to\{x\in\mathbb{K}\mid P(x)=0\}$, $\sigma\mapsto\sigma(\overline{X})$ est injective.

Théorème 31: $\mathrm{Aut}(\mathbb{F}_{p^n})$ est cyclique engendré par F le morphisme de Frobénius.

III] Symbole de Legendre et application

1] Symbole de Legendre

[Rau] XIII.5

Théorème 32: (1) Il y a $\frac{p+1}{2}$ carrés et $\frac{p-1}{2}$ non-carrés dans $\mathbb{F}_p$.
(2) Les carrés de $\mathbb{F}_p^\times$ sont les racines de $X^{\frac{p-1}{2}}-1$ et les non-carrés sont les racines de $X^{\frac{p-1}{2}}+1$.

Corollaire 33: -1 est carré dans $\mathbb{F}_p$ ssi $p\equiv 1[4]$

[Rau] XIII.6

Définition 34: On dit que $k\in\mathbb{Z}$ tel que $p\nmid k$ est résidu quadratique modulo p si $\overline{k}$ est un carré dans $\mathbb{F}_p^*$.
On appelle symbole de Legendre pour $a\in\mathbb{F}_p^*$,
$$\left(\frac{a}{p}\right)=\begin{cases}1 & \text{si } a \text{ est carré dans } \mathbb{F}_p^*\\ -1 & \text{sinon}\end{cases}$$

Proposition 35: (1) $\forall a\in\mathbb{F}_p^*,\ a^{\frac{p-1}{2}}\equiv\left(\frac{a}{p}\right)$ dans $\mathbb{F}_p^*$.
(2) L'application $\mathbb{F}_p^*\to\{\pm1\}$, $a\mapsto\left(\frac{a}{p}\right)$ est l'unique morphisme de groupes non-trivial de $\mathbb{F}_p^*$ dans $\{\pm1\}$.

Exemple 36: $2^{\frac{5-1}{2}}=4\equiv -1[5]$ donc 2 n'est pas carré modulo 5

Proposition 37: $\left(\frac{2}{p}\right)=(-1)^{\frac{p^2-1}{8}}$

2] Loi de réciprocité quadratique et application

[Rau] XIII.7

Lemme 38: Le nombre de solutions de $ax^2=1$ dans $\mathbb{F}_p^\times$ est $\left(\frac{a}{p}\right)+1=\begin{cases}2 & \text{si } a \text{ est un carré dans } \mathbb{F}_p^\times\\ 0 & \text{sinon}\end{cases}$.

Théorème 39: (Loi de réciprocité quadratique) Soit $p\neq q$ premiers impairs
Alors: $\left(\frac{q}{p}\right)=(-1)^{\frac{p-1}{2}\frac{q-1}{2}}\left(\frac{p}{q}\right)$

[Tsen]

Définition 40: Soit E un $\mathbb{K}$-espace vectoriel, H hyperplan de E, G son supplémentaire. La dilatation f de base H, direction G de rapport $\lambda\in\mathbb{K}^*$ est telle que $\forall h\in H, \forall u\in G,\ f(h+u)=h+\lambda u$.

Lemme 41: Soit $\mathbb{K}$ corps à ≥ 3 éléments, V un $\mathbb{K}$-espace vect.
Alors: les dilatations engendrent $GL(V)$

Lemme 42: Soit $\mathbb{K}$ corps fini.
Alors: $\exists a\in\mathbb{K}^*)\ \mathbb{K}^*=\langle a\rangle$

Théorème 43: (de Frobénius-Zolotarev) Soit p premier impair et V un $\mathbb{F}_p$-espace vectoriel de dimension n.
Alors: $\forall u\in GL(V),\ \varepsilon(u)=\left(\frac{\det(u)}{p}\right)$.

IV] Quelques applications aux polynômes sur un corps fini

1] Polynômes cyclotomiques

Définition 44: On note $\mu_n = \{z \in \mathbb{C}^* \mid z^n = 1\}$ l'ensemble des racines n-ièmes de l'unité et on note également : $\mu_n^* = \{z \in \mathbb{C}^* \mid \forall p \wedge n = 1,\ p < n \Rightarrow z^p \neq 1 \text{ et } z^n = 1\}$ l'ensemble des racines primitives n-ièmes de l'unité.
On appelle n-ième polynôme cyclotomique :

$$\Phi_n(X) = \prod_{\zeta \in \mu_n^*} (X - \zeta)$$

Théorème 45: $X^n - 1 = \prod_{d \mid n} \Phi_d(X)$

Théorème 46: Φ_n est à coefficients entiers, unitaire et irréductible dans $\mathbb{Z}[X]$.

[Per]

2] Factorisation de polynômes

Soit $q = p^n$

Proposition 47: L'application $S : \begin{array}{ccc} \mathbb{F}_q[X] & \to & \mathbb{F}_q[X] \\ Q & \mapsto & Q^q \end{array}$ est un $\mathbb{F}_q$-endomorphisme de $\mathbb{F}_q[X]$.

Lemme 48: Soit L une extension de $\mathbb{F}_q$ et $x \in L$.
Alors : $x^q = x$ ssi $x \in \mathbb{F}_q$.

Théorème 49: (de Berlekamp) Soit $P \in \mathbb{F}_q[X]$ sans facteurs carrés et $P = \prod_{i=1}^{r} P_i$ sa décomposition en irréductibles dans $\mathbb{F}_q[X]$.
Alors : (1) Si $r = 1$, alors P est irréductible
(2) Sinon, $\exists a \in \mathbb{F}_q)\ \exists V \in \mathbb{F}_q[X]$ | $PGCD(P; V - a)$ est facteur non-trivial de P.

[Isen]

3] Résolubilité d'équations

Théorème 50: (petit théorème de Fermat) Soit p premier,
Alors : $\forall a \in \mathbb{F}_p^*,\ a^{p-1} \equiv 1\ [p]$.

Théorème 51: (de Sophie-Germain) Soit p premier impair, $q = 2p + 1$ premier.
Alors : $\nexists (x;y;z) \in \mathbb{Z}^3$ | $\begin{cases} xyz \neq 0\ [p] \\ x^p + y^p + z^p = 0 \end{cases}$

[FGN Al 1]

Références :

[Ram] Mathématiques par l'agrégation Algèbre et Géométrie – Rombaldi

[Cal] Extensions de corps, théorie de Galois – Calais

[Isen] L'oral à l'agrégation de mathématiques – Isenmann

[Per] Cours d'algèbre – Perrin

[FGN A1-1] Exercices de mathématiques oraux X-ENS Algèbre 1 – Francinou