Leçon 123 Corps finis, applications

Dorian Cacitti-Holland

2020-2021

Références.

1. Algèbre et géométrie de Jean-Etienne Rombaldi
2. Extensions de corps - Théorie de Galois de Josette Calais
3. Cours d'algèbre de Daniel Perrin
4. Exercices d'algèbre de Pascal Ortiz
5. Histoires hédonistes de groupes et de géométrie de Caldero et Germoni tome 1

Développements.

1. Premier théorème de Sylow
2. Loi de réciprocité quadratique

Table des matières

1 Notions de corps finis

1.1 Définitions et propriétés

(Chapitres III.2.a du Cours d'algèbre de Daniel Perrin et 4.1 de Extensions de corps de Josette Calais)

On considère K un corps fini.

1. Définition : On appelle sous-corps premier de K le plus petit sous-corps de K
2. Exemple : Le sous-corps premier de $\mathbb{R}$ est $\mathbb{Q}$
3. Définition : La caractéristique de K est l'entier $Car(K) = p$ tel que $ker(\varphi) = p\mathbb{Z}$ avec $\varphi(n) = n.1_K$ morphisme d'anneaux
4. Remarque : $Car(K)$ est soit premier soit nulle, mais comme $\mathbb{Z}$ est infini, $car(K)$ est premier
5. Exemple : $Car(\mathbb{Z}/p\mathbb{Z}) = p$
6. Proposition : Le sous-corps premier de K est $\mathbb{Z}/p\mathbb{Z}$ avec $p = Car(K)$, donc $|K| = p^n$
7. Exemple : Il n'existe pas de corps de cardinal $6 = 3 \times 2$
8. Définition : $F(x) = x^p$ est le morphisme de Frobenius
9. Théorème : F est un automorphisme de corps
10. Exemple : Si $K = \mathbb{Z}/p\mathbb{Z}$ alors $F = id_K$

1.2 Existence et unicité

(Chapitres 13.4 d'Algèbre et géométrie de Jean-Etienne Rombaldi, III.2.b du Cours d'algèbre de Daniel Perrin et 4.3 de Extensions de corps de Josette Calais)

On considère $q = p^n$ avec $p \in \mathbb{N}$ premier.

1. Définition : On note $U_n(p)$ l'ensemble des polynômes unitaires irréductibles de degré n dans $\mathbb{F}_p[X]$ et $I_n(p) = |U_n(p)|$
2. Proposition : Soit $P \in U_n(p)$, alors $\mathbb{F}_p[X]/(P)$ est un $\mathbb{F}_p$-espace vectoriel de dimension n et est un corps de cardinal $q = p^n$
3. Exemple : $\forall \lambda \in \mathbb{F}_p, X - \lambda \in U_1(p)$ donc $I_1(p) = p$ et tous ces corps $\mathbb{F}_p[X]/(X - \lambda)$ sont isomorphes à $\mathbb{F}_p$
4. Exemple : Comme $P = X^2 + \lambda X + \mu$ est irréductible si et seulement si sans racines, $I_2(p) = \frac{p(p-1)}{2}$
5. Lemme : En notant $P_n = X^{p^n} - X = X^q - X$, tout diviseur irréductible de P_n dans $\mathbb{F}_p[X]$ est de degré divisant n, réciproquement pour tout diviseur d de n, tout polynôme $P \in U_n(d)$ divise P_n
6. Théorème : P_n est sans facteur carré dans $\mathbb{F}_p[X]$ et on a la décomposition en irréductibles $P_n = \prod_{d|n} \prod_{P \in U_d(p)} P$
7. Théorème : A isomorphisme près, il existe un unique corps à $q = p^n$ éléments, on le note $\mathbb{F}_p$, il s'agit de $\mathbb{F}_p[X]/(P)$ avec $P \in U_n(p)$, et du corps de décomposition de P_n sur $\mathbb{F}_p$
8. Exemple : $\mathbb{F}_2 = \mathbb{Z}/2\mathbb{Z}, \mathbb{F}_4 = \mathbb{F}_2[X]/(X^2 + 1)$

1.3 Inclusion entre corps finis

(Chapitre 4.4 de Extensions de corps de Josette Calais)

1. Lemme : Soit $a > 1, n, s > 0$ des entiers, alors $a^s - 1 \mid a^n - 1 \iff s \mid n$
2. Proposition : Soit $n > 1, s > 0$ des entiers, alors $X^s - 1 \mid X^n - 1$ dans $K[X]$ si et seulement si $s \mid n$
3. Théorème : Soit p premier et $n \in \mathbb{N}^*$, alors il existe une bijection entre les sous-corps de $\mathbb{F}_{p^n}$ et l'ensemble des diviseurs de n, plus précisément $\mathbb{F}_{p^s}$ est un sous-corps de $\mathbb{F}_{p^n}$ si et seulement si $s \mid n$
4. Théorème de la base télescopique : Soit K, L, M des corps tels que $(e_i)_{i\in I}$ soit une base de L sur K et $(f_j)_{j\in J}$ une base de M sur L, alors $(e_i f_j)_{(i,j)\in I\times J}$ est une base de M sur K, ainsi $[M : K] = [M : L][L : K]$
5. Corollaire : Soit $s \mid n$, alors $[\mathbb{F}_{p^n} : \mathbb{F}_{p^s}] = \frac{n}{s}$
6. Exemple : Les sous-corps de $\mathbb{F}_{1024}$ sont $\mathbb{F}_2, \mathbb{F}_4, \mathbb{F}_{32}, \mathbb{F}_{1024}$
7. Théorème de l'élément primitif pour les corps finis : Il existe $\alpha \in \mathbb{F}_{q^n}$ tel que $\mathbb{F}_{q^n} = \mathbb{F}_q(\alpha)$
8. Exemple : $\mathbb{F}_4 = \mathbb{F}_2[X]/(X^2 + X + 1)$, alors en notant a l'image de $X \in \mathbb{F}_2[X]$ dans le quotient $\mathbb{F}_4$, alors $\mathbb{F}_4 = \mathbb{F}_2(a)$

2 Notions de groupes liés au corps

2.1 Groupe des inversibles

(Chapitres III.2.c du Cours d'algèbre de Daniel Perrin et 4.2 de Extensions de corps de Josette Calais)

1. Lemme : Soit G un groupe mutliplicatif fini d'ordre m, si pour tout $d \mid m$, le nombre de $x \in G$ tels que $x^d = 1$ est au plus égal à d, alors G est cyclique
2. Lemme : $m = \sum_{d\mid m} \varphi(d)$ avec φ la fonction d'Euler
3. Théorème : $\mathbb{F}_{p^n}^*$ est cyclique d'ordre $p^n - 1$
4. Exemple : $\mathbb{F}_4 = \mathbb{Z}/3\mathbb{Z}$
5. Corollaire : Soit K un corps, alors tout sous-groupe fini de K^* est cyclique
6. Remarque : On ne sait pas en général trouver explicitement un générateur $\mathbb{F}_{p^n}^*$
7. Exemple : Le générateur de $\mathbb{F}_2^*$ est 1, le générateur de $\mathbb{F}_3^*$ est $-1 = 2$, les générateurs de $\mathbb{F}_5^*$ sont 2 et $3 = 2^3$ (Exercice III.12 de Exercices d'algèbre de Pascal Ortiz)

2.2 Groupe des automorphismes

(Chapitre 13.4 d'Algèbre et géométrie de Jean-Etienne Rombaldi)

1. Définition $Aut(\mathbb{F}_q)$ est le groupe des automorphismes de corps $\mathbb{F}_p$-linéaires
2. Exemple : $id_{\mathbb{F}_{p^n}} \in Aut(\mathbb{F}_{p^n})$ et il s'agit du neutre pour la loi du groupe qui est la composition

3. Exemple : Le morphisme de Frobenius définit précédemment $F \in Aut(\mathbb{F}_{p^n})$
4. Proposition : $o(F) = n$
5. Proposition : En notant $\mathbb{F}_{p^n} = \mathbb{F}_p[X]/(P)$ avec $P \in U_n(p)$, l'application $\varphi : \gamma \in Aut(\mathbb{F}_{p^n}) \longmapsto \gamma(\overline{X}) \in \mathbb{F}_{p^n}$ réalise une injection de $Aut(\mathbb{F}_{p^n})$ sur les racines de P dans $\mathbb{F}_{p^n}$
6. Corollaire : Le groupe $Aut(\mathbb{F}_{p^n})$ est cyclique engendré par l'automorphisme de Frobenius F

2.3 Groupe linéaire

(Chapitres IV.5 du Cours d'algèbre de Daniel Perrin et 5.6 d'Algèbre et géométrie de Jean-Etienne Rombaldi)

On considère E un $\mathbb{F}_p$-espace vectoriel.

1. Lemme : Soit $p \in [\![1, n]\!]$, alors il existe $q^{\frac{p(p-1)}{2}} \prod_{k=n-(p-1)}^{n} (q^k - 1)$ familles formées de p vecteurs linéairement indépendants dans E
2. Théorème : $|GL(E)| = q^{\frac{n(n-1)}{2}} \prod_{k=1}^{n} (q^k - 1)$
3. Corollaire : $|SL(E)| = q^{\frac{n(n-1)}{2}} \prod_{k=2}^{n} (q^k - 1)$
4. Lemme : Le sous groupe de $GL_n(\mathbb{F}_p)$ formé des matrices triangulaires supérieures de diagonale unitaire est un p-Sylow de $GL_n(\mathbb{F}_p)$
5. Lemme : Soit G groupe de cardinal p^α avec p premier et $m \wedge p = 1$, alors G est isomorphe à un sous-groupe de $GL_n(\mathbb{F}_p)$
6. Application : Théorème de Sylow (premier) : Soit G un groupe de cardinal $p^\alpha m$ avec p premier et $m \wedge p = 1$, alors G admet un p-Sylow
7. Corollaire : Théorème de Sylow (second) : Soit H p-sous-groupe de G, alors H est inclus dans un p-Sylow de G, de plus les p-Sylow sont tous conjugués et leur nombre n_p vérifie $n_p \mid n, n_p \equiv 1[p]$

3 Carrés d'un corps fini et loi de réciprocité quadratique

3.1 Symbole de Legendre

(Chapitres 13.6 d'Algèbre et géométrie de Jean-Etienne Rombaldi, III.2.d du Cours d'algèbre de Daniel Perrin)

1. Théorème : Il existe $\frac{q-1}{2}$ carrés et $\frac{q-1}{2}$ non carrés dans $\mathbb{F}_q^*$
2. Théorème de caractérisation des carrés : Si $p > 2$ premier, soit $x \in \mathbb{F}_q$, alors x est un carré dans $\mathbb{F}_q^*$ si et seulement si $x^{\frac{q-1}{2}} = 1$
3. Corollaire : -1 est un carré dans $\mathbb{F}_q$ si et seulement si $q \equiv 1[4]$
4. Application : Il existe une infinité de nombre premiers $p \equiv 1[4]$

5. Définition : On dit que a non multple de p est un résidu quadratique modulo p si $\overline{a}$ est un carré dans $\mathbb{F}_p^*$ et on note $\left(\frac{a}{p}\right) = 1$ si a est résidu quadratique et $\left(\frac{a}{p}\right) = -1$ sinon, appelé symbole de Legendre
6. Exemple : $4^2 \equiv 1[5]$, donc 4 est un résidu quadratique modulo 5
7. Proposition : Soit $a \in \mathbb{F}_p^*$, alors $a^{\frac{p-1}{2}} \equiv \left(\frac{a}{p}\right)[p]$ et $a \in \mathbb{F}_p^* \longmapsto \left(\frac{a}{p}\right) \in \{-1, 1\}$ est l'unique morphisme de groupes non trivial
8. Exemple : $2^{\frac{5-1}{2}} = 2^2 = 4 \equiv -1[5]$, donc 2 n'est pas un résidu quadratique modulo 5
9. Corollaire : Si $n = \pm\prod_{i=1}^{r} p_i^{\alpha_i}$ alors $\left(\frac{n}{p}\right) = (\pm 1)^{\frac{p-1}{2}} \prod_{i=1}^{r} \left(\frac{p_i}{p}\right)^{\alpha_i}$
10. Proposition : $\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$

3.2 Loi de réciprocité quadratique

(Chapitres 13.7 d'Algèbre et géométrie de Jean-Etienne Rombaldi, III.2.d du Cours d'algèbre de Daniel Perrin et V.C de Histoires hédonistes de groupes et de géométries de Caldero et Germoni)

1. Lemme : Soit $a \in \mathbb{F}_p^*$, alors $|\{x \in \mathbb{F}_p, ax^2 = 1\}| = 1 + \left(\frac{a}{p}\right)$
2. Proposition : Soit p et q deux nombres premiers distincts et $X := \left\{(x_1, ..., x_p) \in \mathbb{F}_q^p, \sum_{i=1}^{p} x_i^2 = 1\right\}$, alors $|X| \equiv \left(\frac{p}{q}\right) + 1[p]$
3. Proposition : On a également $|X| = \left(q^d + (-1)^{\frac{p-1}{2}\frac{q-1}{2}}\right) q^d$ avec $d = \frac{p-1}{2}$
4. Corollaire : Loi de réciprocité quadratique : $\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}$
5. Exemple : $\left(\frac{219}{383}\right) = 1$ donc 219 est un résidu quadratique modulo 383

4 Racines de l'unité et polynômes cyclotomiques

4.1 Racines n-ièmes de l'unité

(Chapitre 6.1 de Extensions de corps de Josette Calais)

1. Définition : Une racine n-ième de l'unité de $\mathbb{F}_q$ est une racine de $X^n - 1$ dans $\mathbb{F}_q[X]$
2. Remarque : Si $p \mid n$ alors $n = kp^m$ avec $k, n \in \mathbb{N}^*$ tel que p ne divise pas k, ainsi $X^n - 1 = (X^k - 1)^{p^m}$, ainsi on suppose pour la suite que p ne divise pas n
3. Proposition : L'ensemble U_n des racines n-ièmes de l'unité est un sous-groupe cyclique de $\mathbb{F}_q^*$, et on appelle racine n-ième primitive de l'unité tout générateur de U_n, et leur ensemble est noté Ω_n
4. Remarque : Soit $\omega \in U_n$, alors ω est une racine n-ième primitive de l'unité si et seulement si $o(\omega) = n$
5. Exemple : Soit $\omega = -1 \in \mathbb{F}_3$, alors ω est une racine 2-ième primitve de l'unité

4.2 Polynômes cyclotomiques

(Chapitres 6.2, 6.3 et 6.5 de Extensions de corps de Josette Calais)

1. Définition : $\phi_n = \prod_{\omega \in \Omega_n} (X - \omega)$ est appelé le n-ième polynôme cyclotomique de $\mathbb{F}_q[X]$
2. Exemple : Dans $\mathbb{F}_2$ on a $\phi_7 = X^6 + X^5 + X^4 + X^3 + X^2 + X + 1$
3. Lemme : Soit A anneau commutatif unitaire et $p \in A[X]$ de coefficient dominant inversible dans A, alors pour tout $f \in A[X]$, il existe $q, r \in A[X]$ tels que $f = pq + r$ avec $r = 0$ ou $deg(r) < deg(p)$
4. Théorème : ϕ_n est unitaire dans $\mathbb{F}_p[X]$
5. Remarque : Les polynômes dans $\mathbb{F}_p[X]$ permettent d'en déduire des résultats sur les polynômes cyclotomiques sur $\mathbb{Q}$
6. Théorème : Les polynômes cyclotomiques sur $\mathbb{Q}$ sont unitaires et irréductibles dans $\mathbb{Z}[X]$
7. Théorème : Il existe $\omega \in \Omega_{q-1}$ tel que $\mathbb{F}_q = \mathbb{F}_p(\omega)$
8. Remarque : Les polynôme cyclotomiques sur $\mathbb{F}_q$ ne sont pas nécessairement irréductibles
9. Exemple : Si $p = 3$ et $q = p^2 = 9$, alors $1 \leq 2 < 6 = \varphi(9) = \varphi(q - 1)$, donc le degré du polynôme minimal de $\omega \in \Omega_{q-1}$ sur $\mathbb{F}_p$ est strictement inférieur au degré de ϕ_{q-1}, ainsi ϕ_{q-1} n'est pas nécessairement irréductible