Leçon 123 - Corps finis. Applications.

Les points pouvant faire un développement sont annotés d'une $(\star)$.

Tout anneau est supposé unitaire. $\mathcal{P}$ désigne l'ensemble des nombres premiers. [Odi23]

I Généralités

I.1 Premières propriétés

Notation 1 *Soit un anneau A, on considère l'application $\varphi_A : \mathbb{Z} \to A$, $n \mapsto n1_A$.*

Prop 2 $\operatorname{Ker}\varphi_A$ *est un idéal de $\mathbb{Z}$, et il existe un unique $k \in \mathbb{N}$ tel que* $\operatorname{Ker}\varphi_A = k\mathbb{Z}$.

Déf 3 *L'entier k est appelé caractéristique de A, noté* $\operatorname{car}(A)$

Prop 4 *i) Si B est un sous-anneau de A, alors* $\operatorname{car}(B) = \operatorname{car}(A)$.

ii) $\operatorname{car}(A) = 0 \iff (\forall n \in \mathbb{N},\ n1_A = 0 \implies n = 0)$

iii) $\operatorname{car}(A) \neq 0 \iff (\exists n \in \mathbb{N}^*,\ n1_A = 0)$

Prop 5 *Si A est un anneau intègre fini, alors* $\operatorname{car}(A) = p \in \mathcal{P}$, *et il existe $n \in \mathbb{N}^*$ tel que $|A| = p^n$*

Cor 6 *Si $\mathbb{K}$ est un corps fini, alors il est nécessairement de cardinal p^n où $p \in \mathcal{P}$, et n un entier non nul.*

Déf 7 *Soit A un anneau commutatif tel que* $\operatorname{car}(A) = p \in \mathcal{P}$. *On définit le morphisme de Frobenius comme étant l'application :*

$$Fr : \begin{cases} A & \longrightarrow & A \\ a & \longmapsto & a^p \end{cases}$$

Prop 8 *i) Fr est un morphisme d'anneau*

ii) Si A est un corps fini, alors Fr est un automorphisme de A

iii) Si $A = \mathbb{Z}/p\mathbb{Z}$, alors $Fr = \mathrm{Id}_A$

Thm 9 *Si $\mathbb{K}$ est un corps, alors tout sous-groupe fini de $(\mathbb{K}^*, \cdot)$ est cyclique. Entre autre, si $\mathbb{K}$ est fini, alors $\mathbb{K}^*$ est cyclique.*

I.2 Constructions des corps finis

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

Thm 10 $\mathbb{Z}/p\mathbb{Z}$ *est un corps.*

Thm 11 (Existence et "unicité" d'un corps fini) *1. Le corps de décomposition sur $\mathbb{Z}/p\mathbb{Z}$ de $X^q - X$ est un corps fini de cardinal q.*

2. Si $\mathbb{K}$ et $\mathbb{K}'$ sont deux corps finis de cardinal q, alors ils sont $\mathbb{Z}/p\mathbb{Z}-$isomorphes.

Notation 12 *On notera $\mathbb{F}_q$ le corps fini de cardinal q, unique à $\mathbb{Z}/p\mathbb{Z}-$isomorphe près.*

Rq 13 $\mathbb{F}_q = \mathbb{F}_p(\alpha_1, \ldots, \alpha_q) = \{\alpha_1, \ldots, \alpha_q\}$ *où $\alpha_1, \ldots, \alpha_q$ sont les racines de $X^q - X \in \mathbb{F}_p[X]$*

Ex 14 $\mathbb{F}_4 = \{0, 1, \alpha, 1+\alpha\}$ *où α est une racine de $X^4 - X$ différente de 0 et 1.*

Thm 15 *Soit α un générateur de $\mathbb{F}_q^*$, alors $\mathbb{F}_q = \mathbb{F}_p(\alpha)$*

Thm 16 *Il existe au moins un polynôme irréductible $P \in \mathbb{F}_p[X]$ de degré n, et on a alors que $\mathbb{F}_q \simeq \mathbb{F}_p[X]/(P)$.*

Ex 17 $X^2 + X + 1$ *est irréductible sur $\mathbb{F}_2$, et il vient que* $\mathbb{F}_4 = \mathbb{F}_2[X]/(X^2 + X + 1)$. *Soit α une racine de $X^2 + X + 1$, alors* $\mathbb{F}_4 = \mathbb{F}_2(\alpha) = \{a + b\alpha : a, b \in \mathbb{F}_2\} = \{0, 1, \alpha, 1+\alpha\}$.

II Etude des corps finis

II.1 Sous-corps d'un corps fini

Lemme 18 *Pour tout $q \in \mathbb{Z}\backslash\{-1, 0, 1\}$, $q^d - 1 \mid q^n - 1 \iff d \mid n$*

Thm 19 *Soient $p \in \mathcal{P}$, $n \in \mathbb{N}^*$ et $q = p^n$. Alors :*

1. *Tout sous-corps k de $\mathbb{F}_q$ est de cardinal p^d où $d \mid n$.*
2. *Réciproquement, pour tout diviseur d de n, $\mathbb{F}_{p^d}$ est l'unique sous-corps de $\mathbb{F}_q$.*

Ex 20 *Sous-corps de $\mathbb{F}_{2^{12}}$ (voir annexe)*

II.2 Carrés dans un corps fini

Soient $q = p^n$ où $p \in \mathcal{P}$, $n \in \mathbb{N}^*$.

Déf 21 *On note* $\mathbb{F}_q^{[2]} = \{x^2 : x \in \mathbb{F}_q\}$ *l'ensemble des carrés de* $\mathbb{F}_q$.

Thm 22 *i) Si* $\mathrm{car}(\mathbb{F}_q) = 2$, *alors* $\mathbb{F}_q^{*[2]} = \mathbb{F}_q^*$.

ii) Si $\mathrm{car}(\mathbb{F}_q) \neq 2$:

(a) $\left|\mathbb{F}_q^{*[2]}\right| = \dfrac{q-1}{2}$ *et pour tout* $\alpha \in \mathbb{F}_q^* \backslash \mathbb{F}_q^{*[2]}$, $\mathbb{F}_q^* = \mathbb{F}_q^{*[2]} \bigsqcup \alpha \mathbb{F}_q^{*[2]}$

(b) $x \in \mathbb{F}_q^{*[2]}$ *si et seulement si* $x^{\frac{q-1}{2}} = 1$

(c) $-1 \in \mathbb{F}_q^{[2]}$ *si et seulement si* $q \equiv 1[4]$

On suppose p impair.

Déf 23 (Symbole de Legendre) *Pour tout* $a \in \mathbb{Z}$ *non divisible par* p, *on pose :*

$$\left(\frac{a}{p}\right) = \begin{cases} 1 \text{ si } \overline{a} \in \mathbb{F}_p^{*[2]} \\ -1 \text{ sinon} \end{cases}$$

Ex 24 $\left(\dfrac{1}{p}\right) = 1$, $\left(\dfrac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$ *et* $\left(\dfrac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$

Prop 25 (Critère d'Euler) *Si* $a \in \mathbb{Z}$ *non divisible par* p, *alors* $\left(\dfrac{a}{p}\right) \equiv a^{\frac{p-1}{2}}[p]$

Rq 26 *Si* $a \equiv b[p]$, *alors* $\left(\dfrac{a}{p}\right) = \left(\dfrac{b}{p}\right)$. *On peut alors voir le symbole de Legendre comme une application définie sur* $\mathbb{F}_p^*$.

Prop 27 $\begin{cases} \mathbb{F}_p^* & \longrightarrow & \{-1,1\} \\ x & \longmapsto & \left(\dfrac{x}{p}\right) \end{cases}$ *est un morphisme de groupe.*

Lemme 28 *Soient* $A, B \in M_n(\mathbb{F}_q)$ *inversibles symétriques. Alors* A *et* B *sont congruentes si et seulement si* $\delta(A) = \delta(B)$, *où* $\delta(A)$ *est la classe de* $\det A$ *dans* $\mathbb{F}_q^*/\mathbb{F}_q^{*[2]}$.

(DEV 1 - Loi de réciprocité quadratique) Soient p, q deux nombres premiers impairs distincts. Alors :

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}$$

Ex 29 $\left(\dfrac{-30}{53}\right) = -1$

II.3 Recherche de polynômes irréductibles de degré fixe

Soient $q = p^n$ où $p \in \mathcal{P}$, $n \in \mathbb{N}^*$.

Lemme 30 *Si* $A = \mathbb{F}_q$, $Fr^n = \mathrm{Id}$

Prop 31 *On considère* $A = \mathbb{F}_q[X]$. *Alors* Fr *est injectif, d'image* $\mathbb{F}_q[X^p]$. *Alors pour tout* $Q \in \mathbb{F}_q[X^p]$, *il existe un unique* $P \in \mathbb{F}_q[X]$ *tel que* $Q(X) = P(X)^p$.

Prop 32 *Soient* $P, Q \in \mathbb{F}_q[X]$ *tels que* $P \notin \mathbb{F}_q[X^p]$ *et* $P = \mathrm{pgcd}(P, P')Q$. *Alors* Q *n'a que des facteurs simples.*

(DEV 2 - Algorithme de Berlekamp) Soit $P \in \mathbb{F}_q[X]$, unitaire de degré $N \geq 1$, à facteurs simples

i) On considère pour tout $0 \leq j \leq N-1$, le reste de la division euclidienne de X^{qj} par P qu'on note $\sum_{i=0}^{N} b_{ij} X^i$. Et on note $B = (b_{ij})_{0 \leq i,j \leq N-1} \in M_N(\mathbb{F}_q)$. Alors soit $H = \sum_{i=0}^{N-1} h_i X^i \in \mathbb{F}_q[X]$. P divise $H^q - H$ si et seulement si $(h_0, \ldots, h_{N-1}) \in \mathrm{Ker}(B - I_N)$

ii) Soit $H \in \mathbb{F}_q[X]$, tel que $P \mid H^q - H$. Alors :

$$P = \prod_{\lambda \in \mathbb{F}_q} \mathrm{pgcd}(P, H - \lambda)$$

iii) Le nombre de facteurs irréductibles de P est $N - \mathrm{rg}(B - I_N)$

Rq 33 *Les trois propriétés introduites dans cette partie nous permettent de toujours se ramener à l'étude d'un polynôme à facteurs simples de $\mathbb{F}_q[X]$. Donc l'algorithme de Berlekamp fonctionne même pour un polynôme à facteurs multiples.*

Algorithme 34 (Berlekamp) *Si $B - I_N$ est de rang $N-1$, alors P est irréductible. Sinon, on choisit un polynôme H non constant tel que P divise $H^n - H$ grâce au calcul du noyau de $B - I_N$. On obtient une factorisation de P en facteurs non tous triviaux. En réitérant l'algorithme sur les facteurs trouvés, on obtient une décomposition en facteurs irréductibles de P.*

App 35 *Soit $N \geq 1$, on note $I_N(q)$ l'ensemble des polynômes irréductibles unitaires de degré N dans $\mathbb{F}_q[X]$. Alors :*

$$X^{q^N} - X = \prod_{d|N} \prod_{P \in I_d(q)} P.$$

En conséquence, en appliquant l'algorithme de Berlekamp à $X^{q^N} - X$, on trouve tous les polynômes irréductibles unitaires de degré N dans $\mathbb{F}_q[X]$.

III Applications

III.1 Dénombrement en algèbre linéaire

Soient $n \in \mathbb{N}^*$, $\mathbb{F}_q$ un corps fini de cardinal q.[CG17]

Prop 36 *Soit E un $\mathbb{F}_q-$espace vectoriel de dimension n.*

1. *Le nombre de bases de E est $g_n = |GL_n(\mathbb{F}_q)| = (q^n-1)(q^n-q)\cdots(q^n-q^{n-1})$.*
2. *Si $m \leq n$, le nombre de familles libres de E à m éléments est $\dfrac{g_n}{q^{m(n-m)} g_{n-m}}$.*
3. *Si $m \geq n$, le nombre de familles génératrices de E à m éléments est $\dfrac{g_m}{q^{n(m-n)} g_{m-n}}$.*

Prop 37

1. *Notons $\mathbb{P}_n(\mathbb{F}_q) = \{D \overset{sev}{\subseteq} \mathbb{F}_q^{n+1} : \dim D = 1\}$. Alors $|\mathbb{P}_n(\mathbb{F}_q)| = \sum_{k=1}^{n} q^k$*
2. *$|SL_n(\mathbb{F}_q)| = \dfrac{g_n}{q-1}$*
3. *Notons $\mathcal{N}_n(\mathbb{F}_q)$ l'ensemble des matrices nilpotentes de $M_n(\mathbb{F}_q)$. Alors $|\mathcal{N}_n(\mathbb{F}_q)| = q^{n(n-1)}$*

Thm 38 *$A \in M_n(\mathbb{F}_q)$ est diagonalisable, si et seulement si, $A^q = A$.*

III.2 Irréductibilité dans $\mathbb{Z}[X]$

Soit $P \in \mathbb{Z}[X]$.

Prop 39 *S'il existe $p \in \mathcal{P}$ tel que p ne divise pas le coefficient dominant de p, et que $P \mod p$ est irréductible dans $\mathbb{F}_p[X]$, alors P est irréductible.*

Ex 40 *$P(X) = X^7 + 2X^5 + 1$ est irréductible modulo 3 dans $\mathbb{F}_3[X]$, et donc P est irréductible dans $\mathbb{Z}[X]$.*

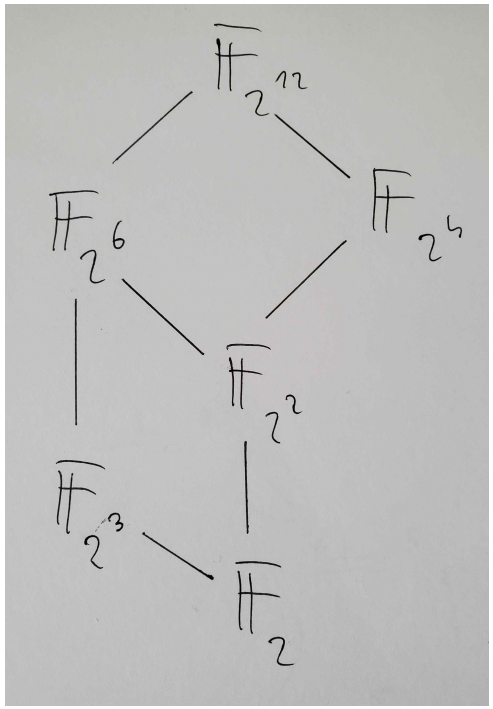
Prop 41 *Si P n'a pas de racines rationnelles, qu'il existe p premier ne divisant pas le terme dominant de P, et tel que $P \mod p$ est produit de deux facteurs irréductibles dans $\mathbb{F}_p[X]$, dont un de degré 1, alors P est irréductible.*

Ex 42 *En raisonnant modulo 5, $P(X) = X^9 + X^4 + X^3 + 5X^2 + 11$ est irréductible dans $\mathbb{Z}[X]$.*

Thm 43 *Les polynômes cyclotomiques sont irréductibles dans $\mathbb{Z}[X]$.*

C-ex 44 *Pour tout nombre premier p, $\Phi_4 \mod p$ n'est pas irréductible dans $\mathbb{F}_p[X]$.*

Annexe



Ex 20 : Les sous-corps de $\mathbb{F}_{2^{12}}$

Bibliographie

[CG17] Philippe Caldero et Jérôme Germoni. *Nouvelles histoires hédonistes de groupes et de géométries, tome second*. Calvage & Mounet, 2017.

[Odi23] Alain Ninet Odile Fleury Loic Foissy. *Algèbre et calcul formel*. 2eme edition. ellipses, 2023.