Leçon 123 : Corps Finis - Applications

Contexte : Cette leçon s'adresse à un étudiant de L3. On suppose connues les généralités concernant les groupes, les anneaux, les idéaux et les corps, ainsi que les polynômes et les corps des fractions. On suppose une première exposition aux concepts d'extension algébrique, de polynôme minimal associé, de corps de rupture et de factorisation, même si on rappellera les résultats et techniques essentielles.

1. Préambule : caractéristique d'un anneau et conséquences pour le cas d'un corps fini

–

Définition 1. — Caractéristique: homomorphisme d'anneaux canonique φ de $(\mathbb{Z}, +)$ sur A, base de la notation nz. $Ker(\varphi)$ est $\mathbb{Z}$ ou $n\mathbb{Z}$. n (ou sinon 0) est la caractéristique de A, notée $car(A)$.

Proposition 1. — *: l'anneau $A[X]$ a la même caractéristique que A. Tout sous-anneau de A a la même caractéristique que A.*

En particulier lorsque A est en fait un corps fini k nous avons :

–

Proposition 2. — *: $car(k) \neq 0$ car φ n'est pas injective.*

Proposition 3. — *: $car(k) \in P$ car k possède un sous-anneau isomorphe à $\mathbb{Z}/car(k)\mathbb{Z}$ et en tant que sous-anneau d'un corps, il doit être intègre. On notera $p = car(k)$*

Proposition 4. — *corps premier : $\mathbb{F}_p = \mathbb{Z}/car(k)\mathbb{Z}$ est appelé "corps premier" de k. Tout sous-corps de k (donc de caractéristique p) possède $\mathbb{F}_p$ comme sous-corps. Le corps premier est cyclique et donc en particulier commutatif.*

Proposition 5. — *k est un $\mathbb{F}_p$-espace vectoriel de façon naturelle et donc $|k| = p^n$ pour un certain $n \in \mathbb{N}$.*

2. Classification des corps finis

–

Proposition 6. — *: si on a $k \subset l \subset m$ trois corps emboîtés, avec k commutatif, alors l et m sont des k-esp.vec. et, si l est lui aussi commutatif, m est un l-espace vectoriel.*

Proposition 7. — *Théorème de la base télescopique : avec les notations précédentes et en dimension finie, $[m : k] = [m : l] * [l : k]$.*

– Centre de $k^\times$: complété de 0, $Z(k^\times, \cdot)$ est un corps et donc un sur-corps du corps premier. C'est par définition sous-corps commutatif de k et les bases télescopiques s'appliquent.

– Nous avons en fait un résultat plus fort dans le contexte des corps finis.

–

Proposition 8. — *Développement 1 : Théorème de Wedderburn - Tout corps fini est commutatif.*

Proposition 9. — *Le groupe multiplicatif est cyclique. Et donc aussi ses sous-groupes.*
Ce résultat important entraîne deux corollaires :

- Tous les éléments de $\mathbb{F}_q^\times$ sont des racines de l'unité.
- Théorème de l'élément primitif : *toute extension finie de $\mathbb{F}_q$ est une extension simple.*

Proposition 10. — *Classification des corps finis -*
Nous avons vu que pour un corps fini k :

- *$|k| = p^n$, avec p premier dit caractéristique de k.*
  - *$(k, +, \cdot) \simeq (\mathbb{F}_p^n, +, \cdot)$ en tant que $\mathbb{F}_p$-espace vectoriel.*
  - *$(k^\times, \cdot) \simeq (\mathbb{Z}/(p^n - 1)\mathbb{Z}, +)$. Il existe $\varphi(p^n - 1)$ générateurs de $(k^\times, \cdot)$, soit un nombre très variable d'un p à un autre.*
  - *Dans le cas particulier où $n = 1$, $(k, +) \simeq (\mathbb{Z}/p\mathbb{Z}, +)$. Il existe alors $\varphi(p) = p - 1$ générateurs.*
  - *Remarques : le groupe additif n'est pas cyclique lorsque $n \geq 2$.*
    Par ailleurs l'ordre dans lequel les éléments de $k^\times$ s'enchaînent avec la structure cyclique multiplicative ne découle pas aisément de l'ordre naturel de $\mathbb{F}_{p^n}$.
- *Exemples : Structure et générateurs de (F_5, F_9 et F_{19}). Exhiber un polynôme minimal de F_9.*

3. Polynômes sur les corps finis

Il existe un rapport très étroit entre les corps finis et les polynômes sur ces corps et en particulier sur le corps premier.

–

Proposition 11. — *Existence et unicité des corps à p^n éléments.*
C'est un résultat très important. Quels que soient p premier et n naturel, il existe un et un seul corps (à un isomorphisme près), noté $\mathbb{F}_{p^n}$, tel que $Card(\mathbb{F}_{p^n}) = p^n$. Alors $car(k) = p$ et $\mathbb{F}_{p^n}$ est le corps des racines du polynôme $(X^{p^n} - X)$ dont la

dérivée est constante égale à -1. Il n'y a pas d'autres corps finis de caractéristique p.

Proposition 12. — *- Ce résultat entraîne plusieurs conséquences que l'on peut étendre à $q = p^m$:*

- *Tous les polynômes irréductibles de $\mathbb{F}_q[X]$ de degré n ont des corps de rupture isomorphes entre eux et à $\mathbb{F}_{q^n}$.*
- *Les polynômes irréductibles de $\mathbb{F}_q[X]$ ont tous des racines simples (en tant que diviseurs des $(X^{p^n} - X)$).*
- *Pour tout n, il existe un polynôme irréductible de $\mathbb{F}_q[X]$ de degré n.*
- *Si α est une racine d'un tel polynôme irréductible sur $\mathbb{F}_q[X]$ et de degré n, $\mathbb{F}_{q^n} = \mathbb{F}_p(\alpha) = 0, 1, \alpha, \alpha^2, \alpha^3, \cdots, \alpha^{p^n-2}$*

.

Exercice : Montrer que $X^2 + X + 4$ et $X^2 + 1$ sont deux polynômes irréductibles sur $F_{11}[X]$ ayant des corps de racines isomorphes et construire deux éléments α, β, primitifs dans chaque corps et ayant même polynôme minimal.

Proposition 13. — *Clôture Algébrique de $\mathbb{F}_q$:*

Tout corps fini admet des polynômes sans racines et la clôture algébrique est donc infinie.
Exemple : $(\Pi_{x\in\mathbb{F}_q}(X_x)) + 1$ vaut 1 sur tout $\mathbb{F}_q$.

- *Sous-corps de $\mathbb{F}_{p^n}$: les seuls sous-corps correspondent à F_{p^d} où d divise n. Pour $d = 1$ on a le sous-corps premier.*
  Exemple : $\mathbb{F}_4 \subset \mathbb{F}_8$ mais $\mathbb{F}_8$ n'est pas un sous-corps de $\mathbb{F}_{12}$
- *Le corps fini $\mathbb{F}_{p^{n!}}$ contient tous les corps finis de caractéristique p et de cardinal inférieur ou égal à p^n.*
- *La clôture algébrique de F_p est donnée par $\overline{\mathbb{F}_p} = \bigcup_{n\in\mathbb{N}} \mathbb{F}_{p^{n!}}$*
- *La clôture algébrique de $\mathbb{F}_p$ ne contient que des racines de l'unité.*

Proposition 14. — *Frobenius et applications*

- *Auto-morphisme des F_q donné par $x \mapsto x^p$ grâce à $(a+b)^{p^i} = a^{p^i} + b^{p^i}$ pour tout i.*
- *Si F_q est le corps premier le Frobenius est l'identité.*
- *Si α est une racine d'un polynôme f de degré n irréductible sur $\mathbb{F}_q$, alors tous les $\alpha, \alpha^q, \alpha^{q^2}, \cdots, \alpha^{q^{n-1}}$ sont des racines de f. Ce sont les conjugués de α par rapport à $\mathbb{F}_q$.*
- *Ces racines sont distinctes et sont exactement les n racines de f.*

$$\Pi_\alpha(X) = \Pi_{i=0,n-1}(X - \alpha^{q^i})$$

- *Nous avons vu que $\mathbb{F}_{q^n} = \mathbb{F}_q[\alpha]$ et si π est le polynôme minimal de α avec degré de $\pi = d$, l'ensemble $\Sigma_d = \alpha, \alpha^q, \alpha^{q^2}, \cdots, \alpha^{q^{d-1}}$ est l'ensemble des éléments générateurs du groupe multiplicatif.*

Proposition 15. — *les carrés de $\mathbb{F}_q$*

Remarque 1. — *Dévissage de $(F_q^*, .)$: une manière plus ramassé hors caractéristique 2 consiste à envisager la suite courte exacte :*

$$\{1\} \to Q = \{x \in (F_q^*)/x = y^2\} \to F_q^* \to \{-1, 1\} \to \{1\}$$

En particulier : $x \in Q \iff x^{\frac{q-1}{2}} = 1$
Irréductibilité

1. Quelques propriétés et applications. —

- Codes auto-correcteurs.
- Algorithme de Berlekamp.

Th. 24 : (petit théorème de Fermat) si a premier avec p premier tout court, alors $a^{p-1} \hom 1(p)$.

x. fonction de Mobius ???

loi de réciproque quadratique ??? (dev??)

x. Polynômes cyclotomiques
x. Irréductibilité des polynômes à coefficients entiers.
x. Résolution des équations de degré 2
Sources :

- D. Perrin "Algèbre Générale"
- Dany-Jack Mercier "Corps Finis"
- J. Calais "Théorie de Galois"
- "Invitation à l'Algèbre"

October 29, 2018

Bruno Nitrosso, EPP et CNED