123 – Corps finis. Applications. .

Références : Rombaldi, Perrin, Gourdon Algèbre, *Corps commutatifs et théorie de Galois* Tauvel.

Cadre : Soit $\mathbb{K}$ un corps commutatif.

1 Caractéristique d'un corps et propriétés

Définition 1. Le morphisme

$$\begin{aligned} \phi : \quad & \mathbb{Z} \to \mathbb{K} \\ & n \mapsto n.1 \end{aligned} \tag{1}$$

est l'unique morphisme de corps de $\mathbb{Z}$ dans K. Son noyau est un idéal de l'anneau principal $\mathbb{Z}$, il existe donc un entier p tel que $ker(\phi) = p\mathbb{Z}$. Cet entier s'appelle caractéristique de p.

Exemple 2. $\mathbb{R}$ est un corps de caractéristique nulle. $\frac{\mathbb{Z}}{p\mathbb{Z}}$ avec p premier est un corps de caractéristique p.

Proposition 3. *La caractéristique d'un corps est nécéssairement 0 ou un nombre premier. Si elle est nulle, il s'agit d'un corps infini.*

Exemple 4. Il est possible d'avoir un corps infini de caractéristique p premier : le corps $\mathbb{F}_p(X)$ des fractions rationnelles à coefficients dans $\mathbb{F}_p$.

Définition 5. Le plus petit sous-corps de $\mathbb{K}$ est appelé sous-corps premier de $\mathbb{K}$. Si la caractéristique de $\mathbb{K}$ est 0, $\mathbb{Q}$ est son sous-corps premier. Si sa caractéristique est p première, son sous corps premier est $\frac{\mathbb{Z}}{p\mathbb{Z}} = \mathbb{F}_p$

Définition 6. Dans un corps $\mathbb{K}$ de caractéristique p première, on définit le morphisme de Frobenius :

$$\begin{aligned} \sigma : \quad & \mathbb{K} \to \mathbb{K} \\ & x \mapsto x^p \end{aligned} \tag{2}$$

Proposition 7. *Le morphisme de Frobenius est un morphisme de corps, il est donc injectif. En particulier, si $\mathbb{K} = \mathbb{F}_p$ avec p premier, alors le morphisme de Frobenius est l'identité.*

Théorème 8 (Théorème de la base téléscopique). *Soit $\mathbb{K} \subset \mathbb{L} \subset \mathbb{M}$ une tour d'extension de corps. Alors on à l'égalité des dimensions :* $[\mathbb{M} : \mathbb{K}] = [\mathbb{M} : \mathbb{L}]\ [\mathbb{M} : \mathbb{L}]$

2 Corps Finis

2.1 Construction des corps finis

Théorème 9. *Soit $\mathbb{F}_q$ un corps finis à q éléments. $(\mathbb{F}_q^*, \times)$ est cyclique à q-1 éléments.*

Théorème 10.
- *1) Soit F un corps à q éléments. Alors il existe un nombre premier p et un entier naturel n tel que $\#(F) = p^n$*
- *2) Soit F le corps de décomposition du polynôme $P = X^{p^n} - X$ dans $\mathbb{F}_p$. Alors F est un corps à $q = p^n$ éléments.*
- *3) Il est unique à isomorphisme près*

Proposition 11. *Soit $\mathbb{F}_{||}$ un corps fini à q éléments. On à $\mathbb{F}_q = \frac{\mathbb{F}_p}{(\pi)}[X]$ pour n'importe quel π polynôme irreductible de degré n de $\mathbb{F}_p[X]$*

Corollaire 12. *Soit F fini à $q = p^n$ éléments. A est un sous-corps de F à $\#(A) = l$ éléments ssi il existe d diviseur de n tel que $l = p^d$*

Exemple 13. Imbrication des sous-corps de $\mathbb{F}_{16}$ (dessin).

Application 14.
- *Théorème de Fermat : Soit p premier, $\forall a \in \mathbb{Z}$, $a^p \equiv a \pmod p$ et $a^{p-1} \equiv 1 \pmod p$ si $a \wedge p = 1$.*
- *Théorème de Wilson : p est premier ssi $(p-1)! \equiv -1 \pmod p$*

2.2 Polynômes irreductibles sur un corps fini

Exemple 15. Soit $\mathbb{F}_q$ un corps fini à q éléments
- $P = X - \lambda$ est irreductible dans $\mathbb{F}_q[X]$ pour tout $\lambda \in \mathbb{F}_q$
- $P = X^2 + aX + b$ est irreductible dans $\mathbb{F}_q[X]$ si il ne possède pas de racine dans $\mathbb{F}_q$.

Proposition 16. *On se place dans $\mathbb{F}_p[X]$, p premier.*
- *Tout diviseur irreductible de $P_n = X^{p^n} - X$ est de degré d qui divise n.*
- *Réciproquement, tout polynôme irreductible de degré d qui divise n est un diviseur de P_n.*

Théorème 17. *On à la décomposition :* $\prod_{d|n} \prod_{P\ irre\ de\ deg\ d} P = P_n$

Exemple 18. Pour construire $\mathbb{F}_4$, on cherche un polynôme irreductible de degré 2 dans $\mathbb{F}_2$. On prend : $P = X^2 + X + 1$, et on obtient $\mathbb{F}_{\not 4} = \{\overline{0}, \overline{1}, \overline{X}, \overline{X+1}\}$ où $\overline{X}$ est racine de $P = X^2 + X + 1$.

2.3 Carrés dans un corps finis

Théorème 19. *Soit $\mathbb{F}_q$ un corps de cardinal $q = p^n$. On note $P_r = \{x^r \mid x \in \mathbb{F}_q^*\}$ et $\delta = r \wedge (q-1)$. Alors*

- *P_r est un sous-groupe de cardinal $\dfrac{q-1}{\delta}$ du groupe multiplicatif $\mathbb{F}_q^*$*
- *$P_r = \{x \in \mathbb{F}_q^* \mid x^{\frac{q-1}{\delta}} - 1 = 0\}$*

Théorème 20. *Soit p un nombre premier impair et $\mathbb{F}_q$ un corps à $q = p^n$ éléments.*

- *L'ensemble $P_2 = \{x^2, x \in \mathbb{F}_q\}$ est un sous-groupe de $\mathbb{F}_q^*$, de cardinal $\frac{q-1}{2}$. (Il y a donc $\frac{q+1}{2}$ dans $\mathbb{F}_q$.*
- *Il y a $\frac{q-1}{2}$ non-carrés dans $\mathbb{F}_q^*$.*
- *Les carrés de $\mathbb{F}_q^*$ sont les racines du polynômes $X^{\frac{q-1}{2}} - 1$. Les non-carrés de $\mathbb{F}_q^*$ sont les racines du polynômes $X^{\frac{q-1}{2}} + 1$.*

Exemple 21. Cela nous donne un critère pour savoir si un élement est un carré ! Par exemple, si p=7 premier, dans $\mathbb{F}_7$, 2 est un carré et 3 n'en est pas un.

Corollaire 22. *Soit $q = p^n$, alors -1 est un carré dans $\mathbb{F}_q$ ssi q est congru à 1 modulo 4.*

Corollaire 23.
- *Le produit de 2 non-carrés est un carré*
- *Le produit de 2 carrés est un carré*
- *Le produit d'un carré et d'un non-carré est un non-carré*

Proposition 24. *Soient a, b dans $\mathbb{F}_q^*$ ($q = p^n$) et c dans $\mathbb{F}_q$. Alors l'équation $c = ax^2 + by^2$ admet des solutions1, on trouve que tout dans $\mathbb{F}_q$. (Si on prend a et b égal à 1, on trouve que tout élément de $\mathbb{F}_q$ est somme de deux carrés.)*

Théorème 25 (Réduction des formes quadratiques sur un corps finis). *Soit q une forme quadratique sur E, de rang r et α un non-carré de $\mathbb{F}_q^*$ fixé. Alors il existe une base B tel que la matrice de q dans cette base soit de la forme :* $\begin{pmatrix} I_{r-1} & 0 & 0 \\ 0 & \delta & 0 \\ 0 & 0 & O_{n-r} \end{pmatrix}$ *avec $\delta \in \{1, \alpha\}$.*

Définition 26. Symbole de Legendre : pour tout a dans $\mathbb{F}_q^*$, le symbole de Legendre est l'entier $\left(\frac{a}{p}\right)$ qui vaut 1 si a est un carré dans $\mathbb{F}_q^*$ et -1 sinon.

Proposition 27. *Pour tout a dans $\mathbb{F}_q^*$, on à $a^{\frac{p-1}{2}} = \left(\frac{\bar{a}}{p}\right)$ dans $\mathbb{F}_q^*$.*

Proposition 28. *L'application*

$$f : \begin{array}{l} \mathbb{F}_q^* \to \{-1, 1\} \\ a \mapsto \left(\frac{a}{p}\right) \end{array} \tag{3}$$

est l'unique morphisme de groupe non-trivial de $\mathbb{F}_q^*$ sur $\{-1, 1\}$.

3 Application des corps finis

3.1 Polynômes dans $\mathbb{Z}[X]$ et $\mathbb{Q}[X]$

Proposition 29. *Soit p premier.*
- *Soit A et B dans $\mathbb{Z}[X]$, alors $\overline{(A+B)^p} = \overline{A^p} + \overline{B^p}$ dans $\mathbb{F}_p[X]$.*
- *Si A est dans $\mathbb{Z}[X]$ et $B = A^p$, alors on à l'égalité dans $\mathbb{F}_p[X]$: $\overline{B}(X) = \overline{A}(X^p)$*

Théorème 30.
- *Soit P un polynôme de degré supérieur ou égal à 1 de $\mathbb{Z}[X]$. On à : P est irreductible dans $\mathbb{Z}[X]$ ssi P est irreductible dans $\mathbb{Q}[X]$ et son contenu vaut 1.*
- *Si P, Q sont deux polynômes unitaires de $\mathbb{Q}[X]$ tel que le produit PQ soit dans $\mathbb{Z}[X]$, alors P et Q sont dans $\mathbb{Z}[X]$*

Théorème 31 (Critère d'irreductibilité d'Eisenstein).

Soit $P = \sum_{k=0}^{n} a_k X^k \in \mathbb{Z}[X]$ et p un nombre premier. On suppose que $p | a_i \forall i \in \{0, ..., n-1\}$, p ne divise pas a_n et p^2 ne divise pas a_0. Alors P est un polynôme irreductible de $\mathbb{Q}[X]$.

Exemple 32. On peut trouver des polynômes irreductibles de n'importe quel degré n dans $\mathbb{Q}[X]$ avec $P_n(X) = X^n - p$.

Théorème 33 (Réduction modulo p). *Soit $P = \sum_{i=0}^{n} a_k X^k$ non constant dans $\mathbb{Z}[X]$, p premier, $\bar{P} = \sum_{i=0}^{n} \bar{a_k} X^k$. Si p ne divise pas a_n et $\bar{P}$ est irreductible dans $\mathbb{F}_p[X]$, alors P est irreductible dans $\mathbb{Q}[X]$*

Application 34. *Le polynôme $X^3 + 462X^2 + 2433X - 67691$ est irreductible sur $\mathbb{Z}[X]$ (et donc sur $\mathbb{Q}[X]$.*

Définition 35. On définit le nème polynôme cyclotomique Φ_n tout en introduisant les racines nèmes primitives de l'unité. Le degré de Φ_n est $\varphi(n)$

Théorème 36. *On a $X^n - 1 = \Pi_{d|n}\Phi_d(X)$ et $\Phi_n(X)$ est unitaire dans $\mathbb{Z}[X]$*

Théorème 37. *Pour tout entier naturel n plus grand que 1, Φ_n est irreductible dans $\mathbb{Z}[X]$, donc dans $\mathbb{Q}[X]$*

Corollaire 38. *Cela nous donne l'accès au degré d'une extension cyclotomique : Soit ω une racine nème première de l'unité, on a $[\mathbb{Q}(\omega) : \mathbb{Q}] = \phi(n)$*

Application 39 (Progression arithmétique de Dirichlet). *Soit $a \in \mathbb{N}^*$. Il existe une infinité de nombre premiers tel que $p \equiv 1 \pmod{a}$*

3.2 Matice à coefficients dans un corps finis

Cadre : Soit $\mathbb{F}_q$ un corps à q éléménts

Proposition 40. $|Gl_n(\mathbb{F}_q)| = \prod_{k=0}^{n-1} (q^n - q^k) = q^{\frac{n(n-1)}{2}} \Pi_{k=1}^{n} q^k - 1$
$|Sl_n(\mathbb{F}_q)| = q_{k=2}^{\frac{n(n-1)}{2}} {}^{n-1}(p^n - p^k)$
$|T_n(\mathbb{F}_q)| = q^{\frac{n(n-1)}{2}}$ *(Matrice triangulaire supérieure à diagonale unité), c'est un p-sylow de $Gl_n(\mathbb{F}_q)$*

Application 41 (1er et 2ème théorème de Sylow). *Soit G un groupe d'ordre $n = p^a m$ avec p qui ne divise pas m. Alors il existe un sous-groupe de G d'ordre p^a.*

De plus, tout les p-Sylows de G sont conjugués

Théorème 42. *On note $D_n(\mathbb{F}_{||})$ l'ensemble des automorphismes diagonalisables de $Gl_n(\mathbb{F}_q)$. Alors :*

$$|D_n(\mathbb{F}_{||})| = \sum_{n_1,\dots,n_{q-1}|n_1+..+n_{q-1}=n} \frac{|Gl_n(\mathbb{F}_q)|}{\Pi_{i=1}^{q-1}|Gl_{n_i}(\mathbb{F}_q)|}$$