Leçon N° 123 : Corps finis. Applications.

Dans cette leçon $\mathbb{K}$ désigne un corps. $\forall p$ premier, $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$.

I) Généralités.

1) Caractéristique

Définition - Proposition 1 : L'application $\varphi : \mathbb{Z} \to \mathbb{K}$, $n \mapsto n \cdot 1$ est l'unique morphisme d'anneaux de $\mathbb{Z}$ dans $\mathbb{K}$.
$\exists ! n \in \mathbb{N}$ tel que $\ker(\varphi) = n\mathbb{Z}$.
On appelle cet entier n la caractéristique de $\mathbb{K}$. On note $\mathrm{car}(\mathbb{K})$.

Proposition 2 : La caractéristique de $\mathbb{K}$ est soit nulle ou un nombre premier.

Proposition 3 : Si $\mathrm{car}(\mathbb{K}) = 0$, alors $\mathbb{K}$ est infini.

Exemple 4 : $\mathbb{F}_p$ est un corps de caractéristique p, et il est fini.

Contre exemple 5 : $\mathbb{F}_p(X)$ est un corps de caractéristique p mais il est infini.

2) Morphisme de Frobenius

Définition 6 : On appelle sous corps premier de $\mathbb{K}$ le plus petit sous corps de $\mathbb{K}$ (Caractérisant 1).

Exemple 7 : Si $\mathrm{car}(\mathbb{K}) = p$, le sous corps premier de $\mathbb{K}$ est $\mathbb{F}_p$.

Lemme 8 : Si $\mathbb{L}$ est un sur-corps de $\mathbb{K}$ et si $\mathbb{K}$ et $\mathbb{L}$ sont finis, alors si on note $n = \dim_{\mathbb{K}} \mathbb{L}$, on a $|\mathbb{L}| = |\mathbb{K}|^n$.

Proposition 9 : Si $\mathbb{K}$ est fini de $\mathrm{car}(\mathbb{K}) = p > 0$, alors $|\mathbb{K}| = p^n$

Exemple 10 : $\mathbb{R}$ n'admet pas de corps de cardinal 6.

Définition - Proposition 11 : Si $\mathbb{K}$ est un corps de $\mathrm{car}(\mathbb{K}) = p > 0$.
L'application $F : \mathbb{K} \to \mathbb{K}$, $x \mapsto x^p$ est un morphisme de corps appelé le morphisme de Frobenius.

Proposition 12 : Si $\mathbb{K}$ est fini, c'est un automorphisme
Si $\mathbb{K} = \mathbb{F}_p$, c'est l'identité.

3) Existence et unicité des corps finis

Soient $n \in \mathbb{N}^*$, p un nombre premier. On pose $q = p^n$.

Théorème 13 : Il existe un corps $\mathbb{K}$ à q éléments, c'est le corps de décomposition du polynôme $X^q - X$ dans $\mathbb{F}_p$.
$\mathbb{K}$ est unique à isomorphisme près, on le note $\mathbb{F}_q$.

Lemme 14 : Tout diviseur irréductible de $X^q - X$ dans $\mathbb{F}_p[X]$ est de degré divisant n. Réciproquement, $\forall d | n$, tout polynôme unitaire irréductible de degré n dans $\mathbb{F}_p[X]$ divise $X^q - X$

Notation 15 : $A(n,q)$: l'ensemble des polynômes de $\mathbb{F}_p[X]$ irréductibles unitaires et de degré n
$I(n,q) = \#A(n,q)$.

Lemme 16 : Le polynôme $X^q - X$ est sans facteurs carrés dans $\mathbb{F}_p[X]$ et on a la décomposition en facteurs irréductibles $X^q - X = \prod_{d \text{ un pgcd}} \prod_{P \in A(d,p)} P$

Définition 17 : On définit la fonction de Möbius par :
$\forall n \in \mathbb{N}^*$, $\mu(n) = \begin{cases} 1 \text{ si } n = 1 \\ (-1)^r \text{ si } n = \prod_{i=1}^r p_i \text{ sa décomposition en pgcd} \\ 0 \text{ sinon} \end{cases}$

Lemme 18 : (Formule d'inversion de Möbius) $\forall (u,v) \in (\mathbb{R}^{\mathbb{N}^*})^2$,
$v_n = \sum_{d|n} u_d \ \forall n \in \mathbb{N}^*$ si $\forall n = \sum_{d|n} \mu(d) v_{n/d} \ \forall n \in \mathbb{N}^*$.

Théorème 19 : $\forall n \in \mathbb{N}^*$, $I(n,p) = \frac{1}{n} \sum_{d|n} \mu\left(\frac{n}{d}\right) p^d$
En particulier $I(n,p) \underset{+\infty}{\sim} \frac{p^n}{n}$ et il existe des polynômes irréductibles dans $\mathbb{F}_p[X]$ de tout degré.

Théorème 20 : Le groupe $\mathrm{Aut}(\mathbb{F}_q)$ est cyclique d'ordre n engendré par le morphisme de Frobenius.

Dev 1

Dev 1

leçon 2

Définition 21 : Le n-ième polynôme cyclotomique Φ_n est donné par $\Phi_n(X) = \prod_{y \in \mu_n^*(\mathbb{K})} (X - y)$ où $\mu_n^*(\mathbb{K})$ est l'ensemble des racines primitives n-ièmes de 1.

Lemme 22 : $\forall n \in \mathbb{N}^*$, $X^n - 1 = \prod_{d \mid n} \Phi_d(X)$.

Théorème 23 : (Wedderburn) Tout corps fini est commutatif.

II) Éléments spéciaux de $\mathbb{F}_q$

1) Étude du groupe multiplicatif $\mathbb{F}_q^*$

Lemme 24 : Si $(G, \cdot)$ est un groupe commutatif, $r \geq 2$ et $g_1, \dots, g_r$ des éléments deux-à-deux distincts de G d'ordre respectifs $m_1, \dots, m_r$, $\exists g_0 \in G$ d'ordre égal au ppcm des ordres de $g_1, \dots, g_r$.

Théorème 25 : Si $\mathbb{K}$ est commutatif, tout sous-groupe fini du groupe $(\mathbb{K}^*, \times)$ est cyclique.

Corollaire 26 : $\mathbb{F}_q^*$ est cyclique, isomorphe à $\mathbb{Z}/(q-1)\mathbb{Z}$.
En particulier $q = p^n$.

2) Les carrés de $\mathbb{F}_q$

Soient $n \in \mathbb{N}^*$, p un nombre premier, $q = p^n$.

Notation 27 : $\mathbb{F}_q^2 = \{x \in \mathbb{F}_q \mid \exists y \in \mathbb{F}_q,\ x = y^2\}$.

$\mathbb{F}_q^{*2} = \mathbb{F}_q^2 \cap \mathbb{F}_q^*$.

Proposition 28 :
- Si $p = 2$, alors $\mathbb{F}_q^2 = \mathbb{F}_q$
- Si $p > 2$, alors $|\mathbb{F}_q^2| = \frac{q+1}{2}$ et $|\mathbb{F}_q^{*2}| = \frac{q-1}{2}$

Proposition 29 : Si $p > 2$, $x \in \mathbb{F}_q^{*2}$ ssi $x^{\frac{q-1}{2}} = 1$.

Lemme 30 : Soit G un groupe fini, $X = \{g \in G \mid g^2 = 1\}$, alors $|G| \equiv |X| \ [2]$.

En particulier si $|G|$ est pair, G contient des éléments d'ordre 2.

Corollaire 30 : Si $p > 2$, $-1 \in \mathbb{F}_p^2$ ssi $q \equiv 1 \ [4]$.

Application 31 : $\forall (a,b) \in \mathbb{F}_q^*$. $\forall c \in \mathbb{F}_q$, $\exists (x,y) \in \mathbb{F}_q$ tels que $c = ax^2 + by^2$.
En particulier tout élément de $\mathbb{F}_q$ est somme de deux carrés.

Application 32 : Il existe une infinité de nombres premiers de la forme $4n+1$.

III) Symbole de Legendre et loi de réciprocité quadratique

Soit p un nombre premier > 2.

Définition 33 : $\forall a \in \mathbb{F}_p$, on définit le symbole de Legendre par

$$\left(\frac{a}{p}\right) = \begin{cases} 1 & \text{si } a \in \mathbb{F}_p^{*2} \\ -1 & \text{si } a \notin \mathbb{F}_p^{*2} \\ 0 & \text{si } a = 0 \end{cases}$$

Proposition 34 : $\forall a \in \mathbb{F}_p^*$, $a^{\frac{p-1}{2}} = \left(\frac{a}{p}\right)$ dans $\mathbb{F}_p^*$ et $a \mapsto \left(\frac{a}{p}\right)$ est l'unique morphisme de groupe non trivial de $\mathbb{F}_p^*$ sur $\{-1, 1\}$.

Corollaire 35 : $\forall n \in \mathbb{N}^*$, l'application

$$GL_n(\mathbb{F}_p) \longrightarrow \{-1, 1\}, \quad A \longmapsto \left(\frac{\det(A)}{p}\right)$$

est l'unique morphisme de groupes non trivial de $GL_n(\mathbb{F}_p)$ sur $\{-1, 1\}$.

Théorème 36 : (Frobenius-Zolotarev)
$\forall A \in GL_n(\mathbb{F}_p)$, $\varepsilon(A) = \left(\frac{\det(A)}{p}\right)$.

Lemme 37 : Soient p un nombre premier impair et $a \in \mathbb{F}_p^*$.
On a $|\{x \in \mathbb{F}_p ; ax^2 = 1\}| = 1 + \left(\frac{a}{p}\right)$.

Théorème 38 : (Loi de réciprocité quadratique)
Soit q un nombre premier ≥ 3 $\neq p$
Alors $\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}$

IV) Autres applications

Proposition 39 : Soit p un nombre premier.
Soit $P = \sum_{i=1}^{d} a_i X^i \in \mathbb{Z}[X]$.
On note $\overline{P}$ sa réduction modulo p.
Si $\overline{a_d} \neq 0$ et $\overline{P}$ irréductible sur $\mathbb{F}_p$, alors P irréductible sur $\mathbb{Q}$.

Application 40 : $X^3 + 482 X^2 + 2433 - 67691$ est irréductible sur $\mathbb{Z}$.

Contre exemple 41 : La réciproque est fausse avec $X^4 + 1$

Proposition 42 : Soit $q = p^n$ où p nombre premier et $n \in \mathbb{N}^*$.
$|GL_n(\mathbb{F}_q)| = (q^n - 1) \dots (q^n - q^{n-1})$
$|SL_n(\mathbb{F}_q)| = (q^n - 1) \dots (q^n - q^{n-2}) q^{n-2}$.

Lemme 43 : 1) Soit G un groupe avec $|G| = p^\alpha m$ avec $p \nmid m$ et soit H un sous groupe de G. Soit S un p-Sylow de G.
Alors $\exists x \in G$ tq $xSx^{-1} \cap H$ soit un p-Sylow de H.

Application 44 : (Sylow) Soit G un groupe fini et p un diviseur premier de $|G|$, alors G contient au moins un p-Sylow.

Théorème 45 : Le nombre de matrices de représentations de $GL_n(\mathbb{F}_q)$ est $\sum_{n_1, \dots, n_q \atop \sum n_i = n} \frac{|GL_n(\mathbb{F}_q)|}{|GL_{n_i}(\mathbb{F}_q)|}$