123 CORPS FINIS. APPLICATIONS.

Cadre : un corps est par définition un anneau commutatif non nul A tel que $A^\times = A \setminus \{0\}$

Il est dit fini lorsque son cardinal est fini.

I / Structures autour des corps finis

Rq 1 Il existe des corps finis. En effet

Prop 2 p est premier $\Leftrightarrow \mathbb{Z}/p\mathbb{Z}$ est intègre $\Leftrightarrow \mathbb{Z}/p\mathbb{Z}$ est un corps

Dans la suite de la partie I, K désigne un corps fini.

1) Caractéristique et cardinal

Prop 3. $\varphi : \begin{cases} \mathbb{Z} \longrightarrow K \\ k \mapsto k.1 \end{cases}$ est un morphisme d'anneaux de noyau $p\mathbb{Z}$. p est un nombre premier

Def 4 On nomme "caractéristique de K", noté $\mathrm{car}(K)$, l'entier p

Rq 5 $\mathbb{Z}/p\mathbb{Z}$ est le sous corps premier de K.

Prop 6 K est un $\mathbb{Z}/p\mathbb{Z}$ espace vectoriel de dimension finie.

Cor 7 : Il existe $n \geq 1$ tel que $\#K = p^n$

Ex 8 : Il n'existe pas de corps à 6 éléments.

2) Structure du groupe des inversibles $K^\times$

Prop 9 $K^\times$ est cyclique. $K^\times \simeq \mathbb{Z}/(p^n-1)\mathbb{Z}$

Rq 10 : En fait, tout sous groupe de $K^\times$ est cyclique

Prop 10. Plus généralement, tout sous groupe fini de $L^\times$ pour L, corps quelconque (même infini) est cyclique.

Ex 11 : $\mathbb{Z}/12\mathbb{Z}^\times$ est cyclique engendré par $\overline{5}$.

3) Automorphismes de K

[DEM] p 211

Prop 12. $\varphi : \begin{cases} K \longrightarrow K \\ x \mapsto x^p \end{cases}$ est un automorphisme de K.

Def 12. Ce morphisme est nommé morphisme de Frobenius.

Rq 13. Si $K = \mathbb{Z}/p\mathbb{Z}$, le petit théorème de Fermat assure que φ = identité

Prop 14. La condition $x^p = x$ équivaut à $x \in \mathbb{Z}/p\mathbb{Z}$

Si $Q \in K[X]$, $Q(X^p) = Q(X)^p$ ssi les coefficients de Q sont dans $\mathbb{Z}/p\mathbb{Z}$

Prop 15. Soit $\alpha \in K$ et n le degré de α sur $\mathbb{Z}/p\mathbb{Z}$. Alors n est le plus petit entier tel que $\alpha^{p^n} = \alpha$ et le polynôme minimal de α sur $\mathbb{Z}/p\mathbb{Z}$ est $(X-\alpha)(X-\alpha^p)\dots(X-\alpha^{p^{n-1}})$.

Prop 16 Soit f un automorphisme de K. Alors il existe $a \geq 0$ tel que pour tout $x \in K$, $f(x) = x^{(p^a)}$

Cor 17. $\mathrm{Aut}(K) = \langle \varphi \rangle \simeq \mathbb{Z}/n\mathbb{Z}$.

4) Existence, unicité, sous corps d'un corps fini

Th 18 Pour tout p premier et tout $n \geq 1$, il existe un corps de cardinal p^n. Il est unique à isomorphisme près et on le note $\mathbb{F}_{p^n}$.

Rq 19 : Cet isomorphisme n'est en revanche pas unique

[DEM] p223

Prop 20. $\forall n \geq 1$, $\forall p$ premier, il existe un polynôme irréductible de degré n dans $\mathbb{F}_p[X]$ (le polynôme minimal d'un générateur de $\mathbb{F}_{p^n}^\times$ convient par exemple). On peut donc construire $\mathbb{F}_{p^n}$ comme quotient de $\mathbb{F}_p[X]$ par un tel polynôme irréductible.

Ex 21 X^2+X-1 est irréductible dans $\mathbb{F}_3[X]$ donc $\mathbb{F}_9 \simeq \dfrac{\mathbb{F}_3[X]}{(X^2+X-1)}$

Prop 22. $\mathbb{F}_p$ d est un sous corps de $\mathbb{F}_{p^m}$ ssi $d \mid m$.
Dans ce cas, $\mathbb{F}_{p^d}$ est l'ensemble des points fixes de φ^d où $\varphi : \mathbb{F}_{p^m} \longrightarrow \mathbb{F}_{p^m}$ est le Frobenius

Ex 23 Les sous corps de $\mathbb{F}_{16}$ sont $\mathbb{F}_2$, $\mathbb{F}_4$, $\mathbb{F}_{16}$.

Prop 24 $\bigcup_{m \in \mathbb{N}} \mathbb{F}_{p^{m!}}$ est une clôture algébrique de tout corps fini de caractéristique p.

II / Polynômes sur les corps finis

1) Polynômes irréductibles sur $\mathbb{F}_q$, $q = p^n$

[PER] p77 Prop 24+1/2 Soit $Q = \sum_{i=1}^{m} a_i X^i \in \mathbb{Z}[X]$ et p premier. Si $\overline{Q} = \sum_{i=1}^{m} \overline{a_i} X^i$ est irréductible dans $\mathbb{Z}/p\mathbb{Z}[X]$ et $\deg(Q) = \deg(\overline{Q})$ alors Q est irréductible dans $\mathbb{Z}[X]$.
Connaître les polynômes irréductibles de $\mathbb{F}_p[X]$ peut montrer l'irréductibilité dans $\mathbb{Z}[X]$

Ex 25 $P = 3X^3 + 7X + 1$ est irréductible dans $\mathbb{Z}[X]$ (et dans $\mathbb{Q}[X]$) car en réduisant modulo 2, on a $\deg(P) = \deg(\overline{P})$ et $X^3 + X + 1$ est irréductible dans $\mathbb{F}_2[X]$.

[PER] p78 Lt ex 26 : $X^4 + 1$ est irréductible sur $\mathbb{Z}$ mais est réductible sur $\mathbb{F}_p$ pour tout premier p.

[PER] p78 Prop 27 Soit $P \in k[X]$ de degré m. P est irréductible sur k $\iff$ P n'a pas de racines dans les extensions K de k telles que $[K : k] \leq \frac{m}{2}$

Ex 28 $X^4 + X + 1$ est irréductible dans $\mathbb{F}_2$.

[EAL1] Th 29 Pour $d \geq 1$, on note $P_d = \{$polynômes irréductibles de degré d dans $\mathbb{F}_q[X]\}$. Alors $X^{q^m} - X = \prod_{d \mid m} \prod_{P \in P_d} P$, pour tout $m \in \mathbb{N}^*$

[EAL1] Prop 30 $\# P_m = \frac{1}{m} \sum_{d \mid m} \mu\left(\frac{m}{d}\right) q^d$ où μ est la fonction de Möbius

Prop 31 Critère d'irréductibilité de Rabin. Soit $P \in \mathbb{F}_q[X]$ unitaire et de degré m.
P est irréductible sur $\mathbb{F}_q$ $\iff$ $\begin{cases} P \mid X^{(q^m)} - X \\ \text{pour tout facteur premier } l \text{ de } m, \\ \quad \operatorname{Pgcd}(P, X^{(q^{m/l})} - X) = 1. \end{cases}$

2) Algorithme de factorisation de Berlekamp

[DA] p245 Algo 32 : Soit $P \in \mathbb{F}_q[X]$ sans facteurs carrés et notons $x = X \bmod P$ dans $\mathbb{F}_q[X]/(P)$.
Entrée de l'algorithme : P. Sortie = les facteurs irréductibles $P_1, \dots, P_n$ de P ($P = P_1 \times \cdots \times P_n$). Déroulement :

① Calculer dans la base $(1, x, \dots x^{\deg(P)-1})$ la matrice de $S_p - Id$ où $S_p : Q \in \mathbb{F}_q[X]/(P) \longmapsto Q^q \bmod P$.

② Calculer $\dim(\ker(S_p - Id))$. Elle vaut n. Si $n = 1$, P est irréductible et on s'arrête. Sinon

③ Calculer $V \in \ker(S_p - Id)$ non constant modulo P.
Alors $P = \prod_{a \in \mathbb{F}_q} \operatorname{pgcd}(P, V - a)$ et parmi ces facteurs, au moins un n'est pas trivial. On réapplique l'algorithme à tous les facteurs non triviaux de ce produit. (DEV 1)

3) Équations sur un corps fini $\mathbb{F}_q$ où $q = p^\alpha$.

[SER] p12 Th 33 (Chevalley-Warning)
Soit $m, n \in \mathbb{N}^*$ et $f_1, \dots f_n \in \mathbb{F}_q[X_1, \dots X_m]$ tels que $\sum_{i=1}^{n} \deg(f_i) < m$
Notons $Z = \{x \in \mathbb{F}_q^m \mid \forall i \in [\![1, n]\!], f_i(x) = 0\}$.
Alors $\# Z \equiv 0 \bmod p$ (DEV 2)

cor 34 Sous les mêmes hypothèses que Th 33, si les f_i sont sans terme constant alors ces polynômes admettent un zéro non trivial.

III/ Corps finis et arithmétique.

1) Critères de primalité

prop 35 Critère de Fermat et de Miller-Rabin.

Soit $n \in \mathbb{N}$. Si $\exists\, a \in [\![1, n[\![$ tel que $a^{n-1} \neq 1 \ (n)$ alors n n'est pas premier. (critère de Fermat).

Plus précisément, si $\exists\, a \in [\![1, n[\![$ et $\exists k \geq 0$ tels que $2^{k+1} | n-1$ et $a^{n-1} \equiv a^{\frac{n-1}{2}} \equiv \dots \equiv a^{\frac{n-1}{2^k}} \equiv 1 \ (n)$ et $a^{\frac{n-1}{2^{k+1}}} \not\equiv \pm 1 \ (n)$ alors n n'est pas premier.

[DEM] 76 prop 36 Soit $n \in \mathbb{N}^*$ impair. On suppose qu'on connaît les facteurs premiers de $n-1$. Alors n est premier $\Leftrightarrow \exists\, a \in \mathbb{N}$ tel que $a^{n-1} \equiv 1 \ (n)$ et $a^{\frac{n-1}{q}} \not\equiv 1 \ (n)$ pour tout q facteurs premiers de $n-1$

2) Carrés dans $\mathbb{F}_p$ pour p premier

Pq 37. Tout élément de $\mathbb{F}_{2^n}$ est un carré car le Frobenius sur $\mathbb{F}_{2^n}$ est un automorphisme (car l'élévation au carré est le Frobenius)

Dans la suite, p est un premier impair

def 38 Symbole de Legendre.

Soit $a \in \mathbb{Z}$. $\left(\frac{a}{p}\right) = \begin{cases} 0 \text{ si } a \equiv 0 \ (p) \\ 1 \text{ si } a \text{ est un carré non nul modulo } p \\ -1 \text{ sinon.} \end{cases}$

prop 39 $\forall a \in \mathbb{Z}$, $\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \ (p)$

prop 40 pour tous $a, b \in \mathbb{Z}$, on a :

$a \equiv b \ (p) \Rightarrow \left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$ et $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$

cor 41 (découle de la prop 39) -1 est un carré mod $p \Leftrightarrow p \equiv 1 \ (4)$

appli 42 Il y a une infinité de nombres premiers congrus à 1 mod 4 [PER] p76

prop 43 $\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$. Autrement dit, 2 est un carré modulo p $\Leftrightarrow p \equiv \pm 1 \ (8)$

Th 44 Réciprocité quadratique.

Soit p, q premiers et impairs. Alors $\left(\frac{q}{p}\right) = \left(\frac{p}{q}\right)(-1)^{\frac{p-1}{2} \times \frac{q-1}{2}}$

Donc $\left(\frac{p}{q}\right) = \left(\frac{q}{p}\right)$ sauf si p et q sont congrus à -1 modulo 4; auquel cas, $\left(\frac{p}{q}\right) = -\left(\frac{q}{p}\right)$

Ex 45 $\left(\frac{3}{7}\right) = -1$ donc 3 n'est pas un carré modulo 7

Prop 46 Soit p premier tq $p \equiv 3 \ (4)$. Si $\left(\frac{a}{p}\right) = 1$ alors $a^{\frac{p+1}{4}}$ est une racine carrée de a

3) Ouverture cryptographique.

prop 47 Idée du protocole d'identification de Fiat-Shamir [ECS] p457

Soit $n = pq$ le produit de 2 grands entiers premiers. Alice est seule détentrice des identifiants $s_1, \dots, s_k$. Pour s'identifier à Bob, Alice lui envoie $\forall i, v_i = s_i^2 \bmod n$ et $t = x^2 \bmod n$. Bob envoie alors $a_1, \dots a_k \in \{0,1\}^k$ à Alice. Alice calcule alors $y = x s_1^{a_1} \dots s_k^{a_k} \bmod n$ Puis Bob vérifie que $y^2 \equiv t\, v_1^{a_1} \dots v_k^{a_k} \ (n)$. Il est difficile pour quelqu'un d'autre qu'Alice de s'authentifier car il faut pour cela connaître les racines carrées des v_i modulo n (difficile)

prop 48 Idée du cryptosystème de Elgamal [IHC] p 68

Soit G un groupe cyclique et g un générateur d'ordre q connu de tous. Alice choisit $x \in [\![1, q-1]\!]$ et calcule $h = g^x$ qu'elle diffuse. Pour lui envoyer un message, Bob choisit k au hasard dans $[\![1, q-1]\!]$ calcule $c_1 = g^k$ et $c_2 = h^k m$ où m est son message. Alice retrouve m en calculant $(c_1^x)^{-1} c_2$. Pour un autre qu'Alice ce problème est difficile dès lors que le problème du logarithme discret dans G est dur. C'est le cas dans certains $(\mathbb{F}_p^*)^x$