Leçon 103 : Corps finis. Applications.

Dans cette leçon on suppose connu les définitions et résultats classique de théorie des corps. Tous les corps sont supposés commutatifs.
Nous rappelerons quand même les résultats de clôture algébrique et de corps de décomposition, notions fondamentales pour la construction des corps finis.

I Rappels, définitions, propriétés

1 Def (i) Soit $f \in K[X]$, un corps de décomposition de f sur K est un corps E contenant K tel que
- f est scindé sur $E[X]$
- $E = K(x_1, \dots, x_n)$, x_i racines de f.

(ii) Une clôture algébrique d'un corps K, noté $\overline{K}$ est un corps algébriquement clos tel que $K \subset \overline{K}$ soit algébrique

2 Thm Il existe toujours, à isomorphisme près, un unique corps de décomposition et une unique clôture algébrique

3 Prop $\mathbb{Z}/n\mathbb{Z}$ est un corps $\Leftrightarrow$ n est premier, on le note $\mathbb{F}_n$.

4 Prop $\varphi : \mathbb{Z} \to K$, $m \mapsto 1 + \dots + 1$ est un morphisme d'anneau et $\ker \varphi = p\mathbb{Z}$, p premier ou $\ker \varphi = \{0\}$

5 Def Si $\ker \varphi = p\mathbb{Z}$, on appel caractéristique de K le nombre p. Sinon la caractéristique est nulle

6 Exemples (i) $\mathbb{F}_p$ est de caractéristique p
(ii) $\mathbb{R}$ est de caractéristique nulle
(iii) Tout corps fini est de caractéristique > 0
(iv) $\mathbb{F}_p(X)$ est de caractéristique p, mais infini.

7 Def On appel corps premier (il existe toujours), d'un corps K, le plus petit corps L tel que $L \subset K$ et L n'a aucun sous corps.

8 Prop (i) Soit K de caractéristique p, le sous corps premier de K est isomorphe à $\mathbb{F}_p$
(ii) Soit K de caractéristique nul, alors le sous corps premier de K est isomorphe à $\mathbb{Q}$.

9 Prop Soit K corps de caractéristique $p > 0$
$\Phi : K \to K$, $x \mapsto x^p$ est un morphisme de corps, appelé morphisme de Frobenius.
En particulier $(x+y)^p = x^p + y^p$ $\forall (x, y) \in K^2$.

II Construction, existence

10 Prop Soit K un corps fini. Alors $\exists!$ p premier (la caractéristique) et $r \in \mathbb{N}^*$ tel que $|K| = p^r$

11 Thm Réciproquement si p est premier et $r \in \mathbb{N}^*$ $\exists!$ (à isomorphisme près) K corps tel que $|K| = p^r$

on note $\mathbb{F}_{p^r}$ le corps.

12 Remarque Il existe plusieurs construction de $\mathbb{F}_{p^r}$

(i) $\mathbb{F}_{p^r}$ est le corps de décomposition de $X^{p^r}-X \in \mathbb{F}_p[X]$

(ii) $X^{p^r}-X$ ayant p^r racines dans $\mathbb{F}_{p^r}$, $\mathbb{F}_{p^r}$ est aussi l'ensemble des racines de $X^{p^r}-X$.

13 Propᵗ Le groupe $(\mathbb{F}_{p^r}^*, \times)$ est cyclique

(ii) Sur $\mathbb{F}_{p^r}$, le morphisme de Frobenius est un automorphisme

iii) $\exists \alpha \in \mathbb{F}_{p^r}$, algébrique, telque $\mathbb{F}_{p^r} = \mathbb{F}_p[\alpha]$ et $\deg \mu_\alpha = r$, μ_α polynôme minimal.

iv) $\mathbb{F}_{p^r} \simeq \mathbb{F}_p[X]/(P)$ $\forall$ P polynôme irréductible de degré r sur $\mathbb{F}_p[X]$.

(v) $\exists$ des polynômes irréductibles de tout les degré sur $\mathbb{F}_p$.

14 Exemples (i) $\mathbb{F}_{2^2} = \{0, 1, \alpha, \alpha^2\}$ avec

+	0	1	α	α^2
0	0	1	α	α^2
1	1	0	α^2	α
α	α	α^2	0	1
α^2	α^2	α	1	0

×	0	1	α	α^2
0	0	0	0	0
1	0	1	α	α^2
α	0	α	α^2	1
α^2	0	α^2	1	α

α et α^2 sont générateurs de $(\mathbb{F}_4^*, \times) \simeq (\mathbb{Z}/3\mathbb{Z}, +)$

et X^2+X+1 est irréductible de degré 2 sur $\mathbb{F}_2[X]$

(ii) X^2+2X+1 est réductible sur $\mathbb{F}_3$

15 Thm Soit $\mathbb{F}_{p^r}$ corps fini

(i) Si L est un sous corps on a $L = \mathbb{F}_{p^n}$, $n \mid r$

(ii) Soit $n \mid r$, $\exists!$ sous corps L de $\mathbb{F}_{p^r}$, avec $|L| = p^n$

(iii) En particulier si $\mathbb{F}_{p^n} \subset \mathbb{F}_{p^r} \subset \mathbb{F}_{p^m}$ alors

$$[\mathbb{F}_{p^m} : \mathbb{F}_{p^n}] = \frac{m}{n} = \frac{m}{r}\frac{r}{n} = [\mathbb{F}_{p^m} : \mathbb{F}_{p^r}][\mathbb{F}_{p^r} : \mathbb{F}_{p^n}].$$

III Polynômes cyclotomique

16 Def Soit $n \in \mathbb{N}$, on pose $P_{n,K}(X) = X^n - 1 \in K[X]$.

L'ensemble des racines de $P_{n,K}$, noté $U_{n,K}$, est appelé racines n-ièmes de l'unité, c'est un sous groupe cyclique de K^*, d'ordre au plus n.

17 Rmq Sans perte de généralité, lorsque $K = \mathbb{F}_{p^r}$, on peut supposer $P_{n,K}$ avec $p \nmid n$

18 Prop On note $U_{n,K}^\times$ les éléments générateurs de $U_{n,K}$, appelé racines primitive, on a $|U_{n,K}^\times| \leq \varphi(n)$ où φ est l'indicatrice d'Euler.

19 Def On note $D_{n,K}$ le corps de décomposition de $P_{n,K}$

Le n-ième polynôme cyclotomique $\Phi_{n,K} \in D_{n,K}[X]$ est défini par $\Phi_{n,K}(X) = \prod_{\zeta \in U_{n,K}^\times} (X - \zeta)$

deg $\Phi_{n,q} \leq \varphi(n)$

2) Prop On a

(i) $\Phi_{n,q} \in \mathbb{Z}[X]$, de degré $\varphi(n)$

(ii) $\Phi_{n,q}$ est irréductible sur $\mathbb{Q}$ $\forall n \in \mathbb{N}$

Ce résultat est crucial pour démontrer ce qui suit

21 Thm (Wedderburn : Tout corps fini est commutatif

22 Contre exemple $\mathcal{H}_2(\mathbb{F}_3)$ est un anneau fini non commutatif

IV Applications

23 Soit $R \in \mathbb{Z}[X]$ unitaire si, il existe p premier tel que $\overline{R}$ soit irréductible sur $\mathbb{F}_p[X]$, alors R est irréductible sur $\mathbb{Q}$.

24 Eisenstein Soit $P = \sum_{i=0}^{n} a_i X^i \in \mathbb{Z}[X]$, si $\exists p$ premier tel que (1) $p \mid a_0, \dots, a_{n-1}$ (2) $p \nmid a_n$ (3) $p^2 \nmid a_0$

Alors P est irréductible sur $\mathbb{Q}[X]$.

25 Berlekamp Soit $P \in \mathbb{F}_q[X]$, polynôme sans racine double. On peut calculer le nombre de facteurs irréductible et si il y en a plusieurs, on peut trouver un polynôme $V \in \mathbb{F}_q[X]$ tel que V soit non constant modulo P et

$$P = \prod_{a \in \mathbb{F}_q} P \wedge (V - a)$$ Dev 1

26 Fermat Soit q premier, n un entier et $d = n \wedge (q-1)$. Tel que $q > d^4 + 4$. Alors $x^n + y^n = z^n$ admet des solutions non triviales dans $\mathbb{F}_q$. Dev 2

27 Dénombrement

(i) $|\mathbb{F}_q^2| = \frac{q-1}{2}$

(ii) $|\mathbb{P}^n(\mathbb{F}_q)| = |\{\text{droite } D \text{ sur } \mathbb{F}_q^{n+1}\}| = \frac{|\mathbb{F}_q^{n+1} \setminus \{0\}|}{|\mathbb{F}_q^*|} = 1 + q + \dots + q^n$

(iii) $|GL_n(\mathbb{F}_q)| = (q^n - 1)(q^n - q) \dots (q^n - q^{n-1})$

28 Sylow Soit G groupe fini et p diviseur premier de $|G|$. Soit $\alpha \in \mathbb{N}$ tel que $p^\alpha \mid |G|$ et $p^{\alpha+1} \nmid |G|$. Alors $\exists$ un sous groupe H de G de cardinal p^α.

29 Chevalley-Warning Soit $(f_i)_{1 \leq i \leq r}$ famille de polynômes non nuls de $\mathbb{F}_{p^n}[X_1, \dots, X_n]$. On suppose que les degrés des $(f_i)_{1 \leq i \leq r}$ vérifient l'inégalité $\sum_{i=1}^{r} \deg(f_i) < n$. Posons $V = \{x \in \mathbb{F}_{p^n}^n \mid \forall 1 \leq i \leq r \ f_i(x) = 0\}$

Alors $\#V \equiv 0 [p]$.

Corollaire Erdos-Ginzburg-Ziv Soit p nombre premier et soit $a_1, \dots, a_{2p-1} \in \mathbb{Z}$. Parmis ces $(2p-1)$ nombres entiers, on peut en trouver p dont la somme est divisible par p

Équation de Fermat dans un corps fini

Notations : G un groupe commutatif fini, ϕ une fonction de G dans $\mathbb{C}$, χ un caractère de $|G|$, sa transformée de Fourier est

$$\hat{\phi}(\chi) = \sum_{x \in G} \phi(x)\chi(x)$$

Si H est un sous-groupe de G, on note $H^{\perp}$ les caractères dont la restriction à H est triviale. C'est un sous-groupe d'indice $|H|$.
Si χ est un caractère de $\mathbb{F}_q^{\times}$, ψ de $\mathbb{F}_q$, on prend la convention $\chi(0) = 0$ et on note

$$G(\chi, \psi) = \sum_{x \in \mathbb{F}_q} \chi(x)\psi(x) = \mathcal{F}_{add}(\chi)(\psi) = \mathcal{F}_{mul}(\psi)(\chi)$$

Où $\mathcal{F}_{add}$ est la transformée de Fourier dans $\mathbb{F}_q$ et $\mathcal{F}_{mul}$ celle dans $\mathbb{F}_q^{\times}$.

Lemme. *$A_1, A_2..A_r$ des parties de G, $S = \{(a_1, .., a_r) \in A_1 \times .. \times A_r \ t.q. \ a_1 + .. + a_r = 0\}$. On a :*

$$|S| = \frac{|A_1 \times .. \times A_r|}{|G|} + R$$
$$où \ R = \frac{1}{|G|} \sum_{\chi \in \hat{G}, \ \chi \neq \chi_0} \prod_{i=1}^{r} \widehat{1_{A_i}}(\chi)$$

Démonstration. On a

$$\begin{aligned} |S| &= \sum_{a_1 + .. + a_r = 0} \prod_{i=1}^{r} 1_{A_i}(a_i) \\ &= 1_{A_1}(a_1) * .. 1_{A_r}(a_r)(0) \\ &= \frac{1}{|G|} \sum_{\chi \in \hat{G}} \prod_{i=1}^{r} \widehat{1_{A_i}}(\chi) \end{aligned}$$

On a utilisé la transformée de Fourier inverse, et le fait que la transformée de Fourier transforme convolution en produits. Il suffit d'isoler le terme $\chi = \chi_0$. □

Corollaire. *Dans le cas $r = 3$, S est non vide dès que*

$$\frac{\Lambda(A_3)}{A_3} < \frac{\sqrt{|A_1 \times A_2|}}{|G|} \tag{1}$$

Où $\Lambda(A) := \max_{\chi \in \hat{G}, \ \chi \neq \chi_0} |\widehat{1_A}(\chi)|$.

Démonstration. Il suffit de montrer que sous cette condition, on a $R < \frac{|A_1 \times A_2 \times A_3|}{|G|}$. Avec une inégalité de Cauchy-Schwarz, on a :

$$\begin{aligned} R &\leq \frac{\Lambda(A_3)}{|G|} \left(\sum_{\chi \in \widehat{G}} |\widehat{1_{A_1}}(\chi)|^2 \right)^{1/2} \left(\sum_{\chi \in \widehat{G}} |\widehat{1_{A_2}}(\chi)|^2 \right)^{1/2} \\ &= \Lambda(A_3) \left(\sum_{x \in G} |1_{A_1}(x)|^2 \right)^{1/2} \left(\sum_{x \in G} |1_{A_2}(x)|^2|^2 \right)^{1/2} \\ &= \Lambda(A_3) \sqrt{|A_1 \times A_2|} \end{aligned}$$

Ce qui conclut. □

Théorème. *Soit q un nombre premier, k un entier et $d = k \wedge (q-1)$ tel que $q > d^4 + 4$. Alors $x^k + y^k = z^k$ admet des solutions non triviales dans $\mathbb{F}_q$.*

Démonstration. Notons $H = \{x^k,\ x \in \mathbb{F}_q^\times\} = \{x^d,\ x \in \mathbb{F}_q^\times\}$ (on a égalité par une relation de Bézout entre $k, q-1, d$). C'est un sous-groupe multiplicatif d'indice d.
On va appliquer le corollaire avec $A_1, A_2, A_3 = -H, H, H$ dans G le groupe (additif!) $\mathbb{F}_q$. Le terme de droite dans (??) vaut $\frac{q-1}{qd}$, il suffit donc de montrer :

$$\Lambda(H) < \frac{(q-1)^2}{qd^2}$$

Soit ψ un caractère non trivial de $\mathbb{F}_q$, on a :

$$\begin{aligned} \widehat{1_H}(\psi) &= \sum_{x \in H} \psi(x) \\ &= \frac{1}{q-1} \sum_{x \in H} \sum_{\chi \in \widehat{\mathbb{F}_q^\times}} G(\chi, \psi) \bar{\chi}(x) \\ &= \frac{1}{q-1} \sum_{\chi \in \widehat{\mathbb{F}_q^\times}} G(\chi, \psi) \sum_{x \in H} \bar{\chi}(x) \\ &= \frac{1}{d} \sum_{\chi \in H^\perp} G(\chi, \psi) \end{aligned}$$

Pour tout caractère non trivial χ, $|G(\chi, \psi)| = \sqrt{q}$ et $G(1, \psi) = -1$, d'où $\widehat{1_H}(\psi) \leq \frac{1 + (d-1)\sqrt{q}}{d} < \sqrt{q}$.
Il suffit alors de vérifier $\sqrt{q} \leq \frac{(q-1)^2}{qd^2}$, c'est-à-dire $d^4 < \frac{(q-1)^4}{q^3}$; $q > d^4 + 4$ convient. En effet, $(q-1)^4 = (q^2 - 2q + 1)^2 > (q^2 - 2q)^2 = q^4 - 4q^3 + 4q^2 > (q-4)q^3$. □

Algorithme de Berlekamp (Beck, Objectif Agrégation)

Théorème : Soit $P \in \mathbb{F}_q[X]$, un polynôme sans facteur carré. On peut calculer le nombre de facteurs irréductibles et si il y en a plusieurs on peut trouver un polynôme $V \in \mathbb{F}_q[X]$ tel que V soit non constant modulo P et $P = \prod_{\alpha \in \mathbb{F}_q} pgcd(P, V-\alpha)$

Lemme : Soit $R \in \mathbb{F}_q[X]$, l'application $S_R : \left| \begin{array}{ccc} \mathbb{F}_q[X]/(R) & \longrightarrow & \mathbb{F}_q[X]/(R) \\ \overline{Q(X)} & \longmapsto & \overline{Q(X^q)} \end{array} \right.$ est bien définie et coincide avec l'élévation à la puissance q dans $\mathbb{F}_q[X]/(R)$

Démo du lemme : On pose $S_1 : \left| \begin{array}{ccc} \mathbb{F}_q[X] & \to & \mathbb{F}_q[X] \\ Q(X) & \mapsto & Q(X^q) \end{array} \right.$, qui est un morphisme d'anneaux et correspond à l'élévation à la puissance q.
On note $\pi_R : \mathbb{F}_q[X] \to \mathbb{F}_q[X]/(R)$ la projection canonique et on pose $S = \pi_R \circ S_1 : \mathbb{F}_q[X] \to \mathbb{F}_q[X]/(R)$. Le morphisme d'anneaux S passe au quotient par (R) et donne S_R, qui est donc bien défini.
Soit $Q \in \mathbb{F}_q[X]$, on a $S_R(Q \bmod (R)) = S_R(\pi_R(Q)) = \pi_R(Q(X^q)) = \pi_R(Q)^q$

Algorithme : On note $\mathcal{B} = \{1, x, \dots, x^{\deg(P)-1}\}$, une base de $\mathbb{F}_q[X]/(P)$

① On calcule la matrice de $S_p - Id$ dans la base $\mathcal{B}$

② Le nb de facteurs irréductibles de P est
$r = \dim(\ker(S_p - Id)) = \deg(P) - rg(S_p - Id)$
Si $r = 1$, on arrête l'algorithme, sinon on passe à l'étape ③

③ On calcule un polynôme V non congru modulo P à un polynôme constant de $\mathbb{F}_q[X]$ et tel que $V \bmod (P) \in \ker(S_p - Id)$
On a alors $P = \prod_{\alpha \in \mathbb{F}_q} pgcd(P, V-\alpha)$ et on retourne à l'étape ① avec chaque facteur non trivial.

Démo : Soit $P = P_1 \dots P_r$ la décomposition en produit d'irréductibles de P deux à deux distincts, mq $r = \dim(\ker(S_p - Id))$
On pose : $\forall i \in [\![1, r]\!]$, $K_i = \mathbb{F}_q[X]/(P_i)$

On a alors l'isomorphisme $\varphi : \left| \begin{array}{l} \mathbb{F}_q[X]/(P) \to K_1 \times \dots \times K_r \\ Q \bmod(P) \mapsto (Q \bmod(P_1), \dots, Q \bmod(P_r)) \end{array} \right.$

par le lemme Chinois.

On pose $\widehat{S_p} = \varphi \circ S_p \circ \varphi^{-1}$ qui est l'élévation à la puissance q dans l'anneau $K_1 \times \dots \times K_r$.

Alors $(x_1, \dots, x_r) \in \operatorname{Ker}(\widehat{S_p} - Id) \Leftrightarrow (x_1^q, \dots, x_r^q) = (x_1, \dots, x_r)$

$\Leftrightarrow \forall i \in [\![1, r]\!], x_i^q = x_i$ dans K_i

Soit K une extension de corps de $\mathbb{F}_q$, alors l'image de $\mathbb{F}_q$ dans K est l'ensemble des éléments de K tels que $x^q = x$.

Donc $(x_1, \dots, x_r) \in \operatorname{Ker}(\widehat{S_p} - Id) \Leftrightarrow \forall i \in [\![1, r]\!], x_i \in \mathbb{F}_q$, donc $\operatorname{Ker}(\widehat{S_p} - Id) \simeq \mathbb{F}_q^r$

donc $r = \dim(\operatorname{Ker}(\widehat{S_p} - Id))$.

On suppose maintenant $r > 1$

L'ensemble des $U \bmod(P)$ avec U congru à un polynôme constant modulo P est la droite-vectorielle $\mathbb{F}_q[X]/(P)$ engendrée par 1.

Comme $\dim(\operatorname{Ker}(S_p - Id)) = r > 1$, il existe $V \in \mathbb{F}_q[X]$ non congru modulo P à un polynôme constant tel que $(V \bmod(P)) \in \operatorname{Ker}(S_p - Id)$

Ainsi $(V \bmod(P_1), \dots, V \bmod(P_r)) \in \mathbb{F}_q^r$ et on pose : $\forall i \in [\![1, r]\!], \alpha_i = V \bmod(P_i)$

Soit $\alpha \in \mathbb{F}_q$, montrons que $\operatorname{pgcd}(P, V - \alpha) = \prod_{\{i, \alpha_i = \alpha\}} P_i$

Comme $\operatorname{pgcd}(P, V - \alpha)$ divise P, on a $\operatorname{pgcd}(P, V - \alpha) = \prod_{i \in I_\alpha} P_i$, avec $I_\alpha \subset [\![1, r]\!]$

Les P_i étant deux à deux premiers entre eux, on a par le lemme de Gauss,

$I_\alpha = \{ i \in [\![1, r]\!] \mid P_i \mid (V - \alpha) \}$

Or, pour $i \in [\![1, r]\!]$, $\alpha_i = \alpha \Leftrightarrow V - \alpha = 0 \bmod(P_i) \Leftrightarrow P_i \mid V - \alpha$

Donc $I_\alpha = \{ i \in [\![1, r]\!] \mid \alpha_i = \alpha \}$, ainsi $\operatorname{pgcd}(P, V - \alpha) = \prod_{\{i, \alpha_i = \alpha\}} P_i$

Finalement $P = \prod_{i=1}^{r} P_i = \prod_{\alpha \in \mathbb{F}_q} \left(\prod_{\{i, \alpha_i = \alpha\}} P_i \right) = \prod_{\alpha \in \mathbb{F}_q} \operatorname{pgcd}(P, V - \alpha)$ #

Algorithme de factorisation :

Soit $P \in \mathbb{F}_q[X]$

① Si P est constant, on sort de l'algorithme

② On calcule $U = pgcd(P, P')$:

↳ si $U = 1$, on applique l'algorithme de Berlekamp à P

↳ si $U = P$, on calcule R tel que $R^{p^n} = P$ avec $p^n = q$ et on retourne à l'étape ① avec R

↳ sinon, on pose $V = \frac{P}{U}$ et on retourne à l'étape ① avec U et V

Preuve :

* Si P est constant, la factorisation est effectué
* Si $pgcd(P, P') = 1$, alors P est sans facteur carré ainsi l'algorithme de Berlekamp assure une factorisation de P
* Si $pgcd(P, P') = P$ alors $P \mid P'$ donc $P' = 0$, ainsi il existe $Q \in \mathbb{F}_q[X]$ tel que $P(X) = Q(X^p)$ donc, en notant R le polynome dont les coefficients sont les racines des coefficients de Q (R est bien déterminé car le Frobenius est un isomorphisme de $\mathbb{F}_q$), ainsi $P(X) = (R(X))^p$
* Sinon U est un polynome qui divise P et donc V est bien définit et $P = UV$ donc la factorisation de U et V assure celle de P