123 Corps finis. Applications.

I/ Généralités sur les corps finis

1) Caractéristique et sous corps premier [Per]

Déf 1 : Soit A anneau unitaire intègre. Alors $\varphi : \mathbb{Z} \to A$, $n \mapsto n.1_A$ est un morphisme d'anneaux et son noyau $\ker \varphi$ est soit (0) soit (p) avec p nombre premier. Cet entier est appelé la caractéristique de A notée $\operatorname{car} A$.

Déf 2 : Soit K un corps. On appelle sous corps premier de K le plus petit sous corps de K contenant 1.

Prop 3 : Deux cas se présentent
- Si $\operatorname{car} K = 0$ alors le sous corps premier $\simeq \mathbb{Q}$
- Si $\operatorname{car} K = p$ alors $\simeq \mathbb{Z}/p\mathbb{Z}$

Rque 4 • Si $\operatorname{car} K = 0$ alors K est infini
• Si K est fini alors $\operatorname{car} K = p > 0$ et de plus K peut être muni d'une structure de $\mathbb{F}_p := \mathbb{Z}/p\mathbb{Z}$ ev de dim finie n et ainsi $\# K = p^n$.

Prop 5 : Soit K un corps de caractéristique $p > 0$. $F : K \to K$, $x \mapsto x^p$ est un morphisme de corps appelé morphisme de Frobenius.
Si $\# K < +\infty$, c'est un automorphisme
Si $K = \mathbb{F}_p$, c'est l'identité.

2) Existence et unicité des corps finis [Per]

Th 6 : p nbre premier et $n \in \mathbb{N}^*$, on pose $q = p^n$.
i) Il existe un corps K à q éléments, c'est le corps de décomposition du polynôme $X^q - X$ sur $\mathbb{F}_p$
ii) K est unique, à isomorphisme près (non unique). On le note $\mathbb{F}_q$

ex 7 : $\mathbb{F}_4$ est le corps de décomposition de $X^4 - X$ sur $\mathbb{F}_2$ c'est à dire $\mathbb{F}_2(j)$.

c-ex 8 : Il n'existe pas de corps à 6 éléments.

3) Sous corps de $\mathbb{F}_q$ [FG]

Lemme 9 : $a \geq 2$, $a^d - 1 \mid a^n - 1$ ssi $d \mid n$

Prop 10 : $\mathbb{F}_{p^n}$ admet un sous corps de cardinal p^d ssi $d \mid n$

ex 11 : Les sous corps de $\mathbb{F}_{16}$ sont $\mathbb{F}_2$, $\mathbb{F}_4$, $\mathbb{F}_{16}$ mais pas $\mathbb{F}_8$ car $3 \nmid 4$.

4) Étude du groupe multiplicatif $\mathbb{F}_q^*$ (Per)

Lemme 12 : $n \in \mathbb{N}^*$, $n = \sum_{d \mid n} \Phi(d)$ (Φ indicatrice d'Euler)

Th 13 : Tout sous groupe fini du groupe multiplicatif d'un corps est cyclique. En particulier, $\mathbb{F}_q^*$ est cyclique.

Corollaire 14 : (th. de l'élément primitif version corps finis) Soit $\mathbb{F}_q / \mathbb{F}_p$ une extension de corps. Alors il existe $\alpha \in \mathbb{F}_q$ tq $\mathbb{F}_q = \mathbb{F}_p(\alpha)$

ex 15 : $\mathbb{F}_9 = \mathbb{F}_3(e^{2i\pi/8})$

Rque 16 : ⚠ $\mathbb{F}_q = \mathbb{F}_p(\alpha) \not\Rightarrow \alpha$ générateur de $\mathbb{F}_q^*$.

5) Les carrés de $\mathbb{F}_q$ (Per) (GG)

Déf 17 : • $\mathbb{F}_q^2 = \{x \in \mathbb{F}_q ; \exists y \in \mathbb{F}_q, x = y^2\}$
• $\mathbb{F}_q^{*2} = \mathbb{F}_q^2 \cap \mathbb{F}_q^*$

Prop 18 : • Pour $p = 2$, on a $\mathbb{F}_q^2 = \mathbb{F}_q$
• pour $p > 2$, on a $|\mathbb{F}_q^2| = \frac{q+1}{2}$ et $|\mathbb{F}_q^{*2}| = \frac{q-1}{2}$

Prop 19 ($p > 2$) (caractérisation des carrés)
$x \in \mathbb{F}_q^{*2} \iff x^{\frac{q-1}{2}} = 1$

ex 20 : Si $q = 7$, $\mathbb{F}_7 = \mathbb{Z}/7\mathbb{Z}$, on a $\frac{q-1}{2} = 3$ et donc $2^3 = 8 = 1 \mod 7$ donc 2 est un carré de $\mathbb{F}_7$.

Cor 21 : ($p > 2$). On pose $q = p^n$, $n \in \mathbb{N}^*$. Alors -1 est un carré dans $\mathbb{F}_q$ ssi q est congru à 1 modulo 4.

App 22 : Il existe une infinité de nombres premiers de la forme $4m+1$.

Déf 23 : ($p > 2$). Soit $a \in \mathbb{F}_p$. On définit le symbole de Legendre de a par $\left(\frac{a}{p}\right) := \begin{cases} 1 & \text{si } a \in \mathbb{F}_p^{*2} \\ -1 & \text{si } a \notin \mathbb{F}_p^{*2} \\ 0 & \text{si } a = 0 \end{cases}$ $\left(= a^{\frac{p-1}{2}}\right)$

Thm 24 (loi de réciprocité quadratique). Soient p et q deux nbres premiers impairs distincts. Alors $\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2} \cdot \frac{q-1}{2}}$

ex 25 : Est-ce que 5 est un carré dans $\mathbb{F}_{19}$?
$\left(\frac{5}{19}\right) \underset{5 \equiv 1 \bmod 4}{=} \left(\frac{19}{5}\right) \underset{19 \equiv -1 \bmod 5}{=} \left(\frac{-1}{5}\right) \underset{5 \equiv 1 \bmod 4 \oplus \text{Cor } 21}{=} 1$
La réponse est oui.

Th. IV

[OA]

II/ Polynômes sur les corps finis

1) Clôture algébrique d'un corps fini [FG]

Fait 26 : un corps fini n'est jamais algébriquement clos.

Thm 27 : p premier, $q = p^n$ $(n \geq 1)$.
$K = \bigcup_{n \geq 0} \mathbb{F}_{p^{n!}}$ est une clôture algébrique de $\mathbb{F}_q$.

Rque 28 : ⚠ au sens de l'union ci-dessus, il faut la comprendre modulo les injections $\mathbb{F}_{p^{n!}} \hookrightarrow \mathbb{F}_{p^{(n+1)!}}$ grâce à la prop 10.

2) Polynômes irréductibles sur les corps finis (Dem)

On pose $q = p^m$ avec $m \geq 1$ et p premier.

Déf 29 : $I(d,q)$ désigne l'ensemble des polynômes irréductibles unitaires de degré d sur $\mathbb{F}_q[X]$.

Lemme 30 : $P \in I(d,q)$. $(P \mid X^{q^n} - X) \Leftrightarrow (d \mid n)$

Prop 31 : Soit $P \in I(n,q)$. Alors le corps de rupture et le corps de décomposition de P sur $\mathbb{F}_q$ coïncident.

ex 32 : $q = 5$ $(m=1)$. $P = X^2+X+1 \in I(2,q)$ donc $\mathbb{F}_5[X]/(P) = \mathbb{F}_{25}$ est (par définition) le corps de rupture de P sur $\mathbb{F}_5$ mais aussi le corps de décomposition de P sur $\mathbb{F}_5$. En effet, on peut vérifier que $\mathbb{F}_{25} = D_{\mathbb{F}_5}(X^{25} - X)$ contient j et j^2.

Thm 33 : n entier ≥ 1. On a (sur $\mathbb{F}_q[X]$)
$$X^{q^n} - X = \prod_{d \mid n} \prod_{P \in I(d,q)} P$$

ex 34 : $X^{2^3} - X = X(X^7 - 1) = X(X-1)(X^6+X^5+X^4+X^3+X^2+X+1)$
$= X(X-1)(X^3+X+1)(X^3+X^2+1)$ sur $\mathbb{F}_2[X]$

cor 35 : $q^n = \sum_{d \mid n} d \times \# I(d,q)$

En particulier, $0 < \dfrac{q^n - q^{\lfloor n/2 \rfloor + 1}}{n} \leq \# I(n,q) \leq \dfrac{q^n}{n}$

App 36 : Sans utiliser le théorème de l'élément primitif, ceci redémontre qu'on peut toujours construire $\mathbb{F}_q = \mathbb{F}_{p^m}$ comme le corps de rupture d'un certain polynôme $P \in I(m,p)$ sur $\mathbb{F}_p$

ex 37 $\mathbb{F}_4 \simeq \mathbb{F}_2[X]/(X^2+X+1)$

3) Factorisation de polynômes – Algorithme de Berlekamp

$q = p^s$ (p premier). On considère $P \in \mathbb{F}_q[X]$ sans facteurs carrés : $P = \prod_{i=1}^{r} P_i$ où les P_i sont irréductibles premiers entre eux deux à deux. L'algorithme de Berlekamp calcule le nombre r de facteurs irréductibles de P et lorsque $r \geq 2$, il donne explicitement les P_i.

Déf-Prop 38 : L'application $S_P : \begin{cases} \mathbb{F}_q[X]/(P) \longrightarrow \mathbb{F}_q[X]/(P) \\ \overline{Q(X)} \longmapsto \overline{Q(X^q)} \end{cases}$

est bien définie et coïncide avec l'élévation à la puissance q dans $\mathbb{F}_q[X]/(P)$.

Notons x la classe de P dans $\mathbb{F}_q[X]/(P)$ et $\mathcal{B} = \{1, x, \dots, x^{\deg P - 1}\}$ base de $\mathbb{F}_q[X]/(P)$

(1) On calcule la matrice $S_P - Id$ dans $\mathcal{B}$ puis on passe au (2)

(2) Le nombre de facteurs irréductibles de P est $r = \dim(\ker(S_P - Id)) = \deg P - rg(S_P - Id)$

Si $r = 1$, P est irréductible et on arrête l'algorithme, sinon on passe au (3)

(3) On calcule un polynôme V non congru modulo P à un polynôme constant de $\mathbb{F}_q[X]$ et tel que $V \bmod P \in \ker(S_P - Id)$. Avec l'algo d'Euclide, on calcule ensuite les $\mathrm{pgcd}(P, V - \alpha)$ $(\alpha \in \mathbb{F}_q)$

On a alors $P = \prod_{\alpha \in \mathbb{F}_q} \mathrm{pgcd}(P, V - \alpha)$

Retour au (1) avec chacun des facteurs non triviaux du produit.

ex 39 : On considère $P = X^4 + X^2 + 1$ sur $\mathbb{F}_3[X]$.

On trouve $S_P = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 2 & 2 \\ 0 & 1 & 2 & 1 \end{pmatrix}$ donc $S_P - Id = \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & -1 & 0 & 1 \\ 0 & 0 & 1 & 2 \\ 0 & 1 & 2 & 0 \end{pmatrix}$

D'où : $r = 2 > 1$ et considérant $V = X^3 + X^2 + X \in \ker(S_P - Id)$

↳ on trouve $\mathrm{pgcd}(P, V) = X - 1$ (irréductible)
$\mathrm{pgcd}(P, V-1) = X^3 + X^2 + X - 1$ (réappliquer Berlekamp)
$\mathrm{pgcd}(P, V-2) = 1$

Finalement, la décomposition en facteurs irréductibles de P est : $(X-1)(X^3+X^2+X-1)$.

4) Equations polynomiales

DVPT 2

Thm (Chevalley-Warning) : $q = p^r$ avec $r \geq 1$. Soit A un ens. fini, $(f_\alpha)_{\alpha \in A} \in \mathbb{F}_q[X_1, \dots X_n]^A$ tels que $\sum_{\alpha \in A} \deg(f_\alpha) < n$. On pose $V := \{ x \in \mathbb{F}_q^n ;\ \forall \alpha \in A\ f_\alpha(x) = 0 \}$

Alors : $\# V \equiv 0 \bmod p$.

App : une forme quadratique sur un corps fini $\mathbb{F}_q$ en au moins trois variables admet un zéro non trivial.

III/ Algèbre linéaire sur les corps finis (C-G)

1) Dénombrement sur les corps finis

Déf 40 : L'espace projectif (de dim n) $\mathbb{P}^n(\mathbb{F}_q)$ est l'ensemble des droites vectorielles de $\mathbb{F}_q^{n+1}$.

Déf-prop 41 : Le groupe $PGL_n(\mathbb{F}_q) = GL_n(\mathbb{F}_q)/\mathbb{F}_q^*$ agit de manière fidèle sur $\mathbb{P}^{n-1}(\mathbb{F}_q)$.

prop 42 : (i) $\# \mathbb{F}_q^n = q^n$

(ii) $\# \mathbb{P}^n(\mathbb{F}_q) = 1 + q + \dots + q^n$

$\#PSL(n, \mathbb{F}_q) = \frac{\#SL(n,\mathbb{F}_q)}{pgcd(n,q-1)}$

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

$= q^{n(n-1)/2} (q^n - 1)(q^{n-1} - 1)(\dots)(q-1)$

(iv) $\# PGL_n(\mathbb{F}_q) = q^{n(n-1)/2} (q^n - 1)(q^{n-1} - 1) \dots (q^2 - 1)$

(v) $\# SL_n(\mathbb{F}_q) = q^{n(n-1)/2} (q^n - 1) \ - - - \ (q^2 - 1)$

ex 43 : $\mathbb{P}_1(\mathbb{F}_3) = 4$ (cf annexe - dessin 1 pour une représentation graphique)

2) Théorèmes de Sylow et variétés de drapeaux sur les corps finis

Thm 44 : • Le groupe TSU_n des matrices triangulaires supérieures avec des 1 sur la diagonale est un p-Sylow de $GL_n(\mathbb{F}_q)$

• L'ensemble de ces p-Sylow est en bijection avec les drapeaux complets de $\mathbb{F}_q^n$ ie avec

$\mathcal{F}_n(\mathbb{F}_q) = \{ (F_0, \dots F_n) ;\ \dim F_i = i,\ \{0\} = F_0 \subset F_1 \subset \dots \subset F_n = \mathbb{F}_q^n \}$

3) Isomorphismes exceptionnels de groupes finis

Thm 45 (adms)

• Les groupes alternés $\mathcal{A}_n$, $n \geq 5$, sont simples non abéliens.

• Les groupes $PSL_n(\mathbb{F}_q)$, $(n,q) \neq (2,2), (2,3)$ sont simples non abéliens.

question : Est-ce que ces deux séries de groupe peuvent accidentellement être isomorphes ?

Réponse : En général non, mais exceptionnellement oui.

Prop 46 :

(i) $GL_2(\mathbb{F}_2) \simeq SL_2(\mathbb{F}_2) \simeq PSL_2(\mathbb{F}_2) \simeq PGL_2(\mathbb{F}_2) \simeq \mathfrak{S}_3$

(ii) $PSL_2(\mathbb{F}_3) \simeq \mathcal{A}_4$, $PGL_2(\mathbb{F}_3) \simeq \mathfrak{S}_4$

(iii) $PGL_2(\mathbb{F}_4) \simeq PSL_2(\mathbb{F}_4) \simeq \mathcal{A}_5$

(iv) $PSL_2(\mathbb{F}_5) \simeq \mathcal{A}_5$, $PGL_2(\mathbb{F}_5) \simeq \mathfrak{S}_5$.

Prop 47 (un non isomorphisme exceptionnel)

Les groupes $PSL(4, \mathbb{F}_2)$ et $PSL(3, \mathbb{F}_4)$ sont deux groupes simples non isomorphes de même ordre 20160

Rque 48 : Pour trouver un autre non isomorphisme de groupes finis simples de petit cardinal, il faut aller chercher à l'ordre 4585351680.

4) Formes quadratiques sur un corps fini

q : puissance d'un nombre premier $p > 2$.

Thm 49 (Classification) : Il y a exactement deux classes d'équivalence de formes quadratiques non dégénérées sur $\mathbb{F}_q^n$. Deux représentants respectifs de ces classes sont donnés par les matrices

$\begin{pmatrix} 1 & & 0 \\ & \ddots & \\ 0 & & 1 \end{pmatrix}$ et $\begin{pmatrix} 1 & & & 0 \\ & \ddots & & \\ & & 1 & \\ 0 & & & \alpha \end{pmatrix}$ avec $\alpha \notin (\mathbb{F}_q^*)^2$.

Résoudre $y^2 = 41x+3$.

On a, si (x,y) solution :

$y^2 \equiv 3\ [41]$

$\left(\frac{3}{41}\right) = \left(\frac{41}{3}\right) = \left(\frac{2}{3}\right) = \left(\frac{-1}{3}\right) = -1$.

Contradiction.

Montrer que $\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$

Déjà si p impair, $p = 2k+1$

$p^2-1 = (p-1)(p+1) = 2k(2k+2) = 4\underbrace{k(k+1)}_{\text{pair}}$

donc $8 \mid (p^2-1)$

$\Phi : \begin{array}{|l} \mathbb{F}_p \longrightarrow \mathbb{F}_p \\ x \longmapsto ax \end{array}$; $a \in \mathbb{F}_p^\times$, $a = g^k$ où $\langle g \rangle = \mathbb{F}_p^*$.

Donc $\varepsilon(\Phi) = (-1)^k = \left(\frac{a}{p}\right)$.

$\mathbb{F}_8 \simeq \mathbb{F}_2[X]/(X^3+X+1)$

$\alpha = P(X)$.

$\mathbb{F}_8 = \{0, 1, \alpha, \alpha^2, 1+\alpha, 1+\alpha^2, 1+\alpha+\alpha^2, \alpha+\alpha^2\}$

$\mathbb{F}_8^* \simeq \mathbb{Z}/7\mathbb{Z}$

$\begin{cases} u_{n+3} = u_{n+1} + u_n \\ u_0 = 3 \\ u_1 = 0 \\ u_2 = 2 \end{cases}$ Montrer $\forall p$ premier, $p \mid u_p$.

$\begin{pmatrix} u_{n+1} \\ u_{n+2} \\ u_{n+3} \end{pmatrix} = \underbrace{\begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 1 & 0 \end{pmatrix}}^{\Pi} \begin{pmatrix} u_n \\ u_{n+1} \\ u_{n+2} \end{pmatrix}$ $\quad \chi_\Pi = \underline{-X^3+X+1}$.

$k = \mathcal{D}_{\mathbb{F}_p}(X^3-X-1)$

$X^3-X-1 = (X-a)(X-b)(X-c)$.

$u_n = \lambda a^n + \mu b^n + \gamma c^n$, $\lambda, \mu, \gamma \in k$.

$u_n = a^n + b^n + c^n$

$u_0 = 3$, $u_1 = a+b+c = 0$, $u_2 = (a+b+c)^2 - 2(ab+ac+bc) = 2$

$u_p = a^p + b^p + c^p = (a+b+c)^p = 0$ dans k. donc $p \mid u_p$.

$\mathbb{F}_2[X]/(X^3+X^2+1) \simeq \mathbb{F}_2(\beta)$.

$\beta^3 = -\beta^2 - 1$

$(1+\beta^2)^3 = (1+\beta^2)+1$.

$\mathbb{F}_2[X]/(X^3+X+1) \simeq \mathbb{F}_2(\alpha)$.

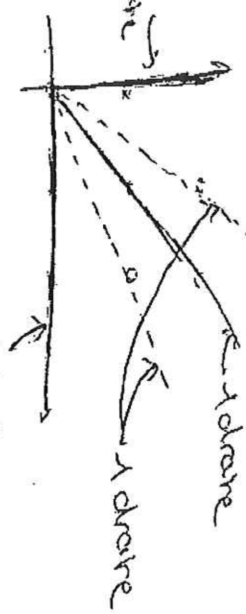
$\alpha \overset{\Phi}{\mapsto} 1+\beta^2$ est un isom. de corps entre $\mathbb{F}_2(\alpha)$ et $\mathbb{F}_2(\beta)$

$\varphi : x \mapsto x^2$ dans $\mathbb{F}_2[X]/(X^3+X^2+1)$

$\varphi \circ \Phi$ et $\varphi^2 \circ \Phi$ isom.

Annexe :

Dessin 1 ($\mathbb{P}_1(\mathbb{F}_3)$)



Les 4 droites de $\mathbb{P}_2(\mathbb{F}_7)$.

Références

- Daniel PERRIN, Cours d'algèbre (Per)
- S. FRANCINOU ; H. GIANELLA, Exercices de mathématiques pour l'agrégation. [FG]
- Philippe CALDERO ; Jérôme GERMONI, Histoires hédonistes de groupes et de géométries (C-G)
- Michel DEMAZURE, Cours d'algèbre (Dem)
- V. BECK ; J. MALICK ; G. PEYRÉ, Objectif Agrégation (OA)

Leçon 123 — Corps finis

Adrien Clarenne - Kévin Le Balc'h.

DEVELOPPEMENT n° 1 !
LOI DE RÉCIPROCITÉ QUADRATIQUE

Déf 1 Soit p premier.
Si $x \in (\mathbb{Z}/p\mathbb{Z})^*$, on définit le symbole de Legendre $\left(\frac{x}{p}\right)$ par :
- $\left(\frac{x}{p}\right) = 1$ si x est un carré dans $(\mathbb{Z}/p\mathbb{Z})^*$
- $\left(\frac{x}{p}\right) = -1$ sinon.

On pose $\left(\frac{0}{p}\right) = 0$ et $\left(\frac{n}{p}\right) = 0$ si $p | n$.

Th (Loi de réciprocité quadratique)
Soient p, q premiers impairs distincts.
Alors : $\left(\frac{p}{q}\right) = (-1)^{\frac{(p-1)(q-1)}{4}} \left(\frac{q}{p}\right)$.

Nous avons besoin d'établir quelques résultats pour démontrer ce théorème :

Prop 1 Soit p un nombre premier impair.
Alors pour tout entier n, $\left(\frac{n}{p}\right) \equiv n^{\frac{p-1}{2}} \; [p]$

Dém
- si $p | n$, c'est trivial
- si $p \nmid n$ on a à montrer :

si $x \in (\mathbb{Z}/p\mathbb{Z})^*$, $\left(\frac{x}{p}\right) = x^{\frac{p-1}{2}} \; [p]$ $\quad (x = \bar{n})$.

Comptons les carrés de $(\mathbb{Z}/p\mathbb{Z})^*$.
Soit $\varphi : (\mathbb{Z}/p\mathbb{Z})^* \longrightarrow (\mathbb{Z}/p\mathbb{Z})^*$, $x \longmapsto x^2$ morphisme

$\mathrm{Im}(\varphi)$ est l'ensemble des carrés de $(\mathbb{Z}/p\mathbb{Z})^*$

$$\mathrm{Ker}(\varphi) = \{x \in (\mathbb{Z}/p\mathbb{Z})^* \,/\, x^2 = 1\}$$
$$= \{x \in (\mathbb{Z}/p\mathbb{Z})^* \,/\, (x-1)(x+1) = 0\}$$
$$= \{\pm 1\} \text{ car } \mathbb{Z}/p\mathbb{Z} \text{ est un corps}$$

Ainsi, $\# \mathrm{Im}(\varphi) = \frac{\# (\mathbb{Z}/p\mathbb{Z})^*}{2} = \frac{p-1}{2}$.

Or, $\forall x \in (\mathbb{Z}/p\mathbb{Z})^*$, $x^{p-1} = 1$

et $X^{p-1} - 1 = (X^{\frac{p-1}{2}} - 1)(X^{\frac{p-1}{2}} + 1)$

donc $\forall x \in (\mathbb{Z}/p\mathbb{Z})^*$, $x^{\frac{p-1}{2}} = 1$ ou $x^{\frac{p-1}{2}} = -1$

Si x est un carré, $\exists a$ tq $x = a^2$

d'où $x^{\frac{p-1}{2}} = a^{p-1} = 1$

Ainsi, le polynôme $X^{\frac{p-1}{2}} - 1$ admet au plus $\frac{p-1}{2}$ racines, et les $\frac{p-1}{2}$ carrés de $(\mathbb{Z}/p\mathbb{Z})^*$ sont racines de ce polynôme on a donc :

$x \in (\mathbb{Z}/p\mathbb{Z})^*$ est un carré $\Longleftrightarrow x^{\frac{p-1}{2}} = 1$

$x \in (\mathbb{Z}/p\mathbb{Z})^*$ n'est pas un carré $\Longleftrightarrow x^{\frac{p-1}{2}} = -1$

d'où $\left(\frac{x}{p}\right) = x^{\frac{p-1}{2}}$. $\square$

Introduisons désormais les sommes de Gauss, qui étant donné q premier impair, permettent de calculer $\sqrt{\pm q}$ comme combinaison de racines $q^{\text{ème}}$ de l'unité.

Prop 2 Soit p, q deux nombres premiers impairs distincts.
Soit Ω clôture algébrique de $\mathbb{Z}/p\mathbb{Z}$ et soit $\omega \in \Omega$ une racine $q^{\text{ième}}$ de l'unité différente de 1.

On pose $\tau = \sum_{i \in \mathbb{Z}/q\mathbb{Z}} \left(\frac{i}{q}\right)\omega^i = \sum_{i=0}^{q-1}\left(\frac{i}{q}\right)\omega^i$

On a alors :

(i) $\tau^2 = (-1)^{\frac{q-1}{2}} q$ (q est la classe de q dans $\mathbb{Z}/p\mathbb{Z}$, notat°)

(ii) $\tau^{p-1} = \left(\frac{p}{q}\right)$

Dém • Déjà τ est bien défini car $\omega^q = 1$ donc ω^i ne dépend que de la classe de congruence de i dans $\mathbb{Z}/q\mathbb{Z}$.

(i) • Grâce à la prop 1, $n \in \mathbb{Z}/p\mathbb{Z} \longrightarrow \left(\frac{n}{q}\right)$ est un morphisme d'où :

$$\tau^2 = \sum_{i,j \in \mathbb{Z}/q\mathbb{Z}} \left(\frac{i}{q}\right)\left(\frac{j}{q}\right)\omega^i\omega^j = \sum_{i,j \in \mathbb{Z}/q\mathbb{Z}} \left(\frac{ij}{q}\right)\omega^{i+j}$$

$$\underset{k=i+j}{=} \sum_{k,i \in \mathbb{Z}/q\mathbb{Z}} \left(\frac{i(k-i)}{q}\right)\omega^k$$

$$\Rightarrow (-1)^{\frac{q-1}{2}}\tau^2 = \left(\frac{-1}{q}\right)\tau^2 = \sum_{k \in \mathbb{Z}/q\mathbb{Z}} S_k \omega^k$$

avec $S_k = \sum_{i \in \mathbb{Z}/q\mathbb{Z}} \left(\frac{i(i-k)}{q}\right) = \sum_{i \in (\mathbb{Z}/q\mathbb{Z})^*} \left(\frac{i(i-k)}{q}\right)$

Calculons alors S_k pour $0 \leq k \leq q-1$.

1er cas : $k = 0$ alors $S_0 = \sum_{i \in (\mathbb{Z}/q\mathbb{Z})^*} \left(\frac{i^2}{q}\right) = q-1$.

2nd cas : $k \neq 0$

$$S_k \underset{i \text{ inversible}}{=} \sum_{i \in (\mathbb{Z}/q\mathbb{Z})^*} \left(\frac{i^2(1-ki^{-1})}{q}\right) = \sum_{i \in (\mathbb{Z}/q\mathbb{Z})^*} \left(\frac{1-ki^{-1}}{q}\right)$$

$$\underset{\substack{j = 1-ki^{-1} \\ (k \neq 0)}}{=} \sum_{j \in (\mathbb{Z}/q\mathbb{Z}) \setminus \{1\}} \left(\frac{j}{q}\right)$$

$$= \sum_{j \in \mathbb{Z}/q\mathbb{Z}} \left(\frac{j}{q}\right) - \left(\frac{1}{q}\right)$$

$$= 0 - 1 = -1$$

car il y a autant de carrés dans $\mathbb{Z}/q\mathbb{Z}$ que de non carrés

Ainsi, $(-1)^{\frac{q-1}{2}}\tau^2 = q-1 + \sum_{k=1}^{q-1} (-1)\omega^k$

$$= q-1 - (\omega + \omega^2 + \dots + \omega^{q-1})$$

$$= q-1 - (-1)$$

$$= q$$

$\Rightarrow \tau^2 = (-1)^{\frac{q-1}{2}} q$ en multipliant à gauche par $(-1)^{\frac{q-1}{2}}$.

(ii) Ω est de caractéristique p donc $x \longmapsto x^p$ est un morphisme. On a alors :

$$\tau^p = \sum_{i=0}^{q-1} \left(\frac{i}{q}\right)^p \omega^{ip} \underset{p \text{ impair}}{=} \sum_{i=0}^{q-1} \left(\frac{i}{q}\right)\omega^{ip}$$

d'où $\left(\frac{p}{q}\right)\tau^p = \sum_{i=0}^{q-1} \left(\frac{ip}{q}\right)\omega^{ip} = \sum_{j=0}^{q-1} \left(\frac{j}{q}\right)\omega^j$

car p est inversible dans $\mathbb{Z}/q\mathbb{Z}$

$= \tau$

$\Rightarrow \tau^p = \left(\frac{p}{q}\right)\tau$ d'où $\tau^{p-1} = \left(\frac{p}{q}\right)$

(τ est non nul car $\tau^2 = (-1)^{\frac{q-1}{2}} q$ l'est)

Nous pouvons alors démontrer la loi de réciprocité quadratique :

$$\left(\frac{(-1)^{\frac{q-1}{2}}q}{p}\right) \underset{\substack{\uparrow \\ \text{Prop 1} \\ \text{et Prop 2, (i)}}}{=} \left(\tau^2\right)^{\frac{p-1}{2}} = \tau^{p-1} \underset{\substack{\uparrow \\ \text{Prop 2, (ii)}}}{=} \left(\frac{p}{q}\right)$$

Or d'après la proposition 1),

$$\left(\frac{(-1)^{\frac{q-1}{2}}q}{p}\right) = \left(\frac{(-1)^{\frac{q-1}{2}}}{p}\right)\left(\frac{q}{p}\right) = \left((-1)^{\frac{q-1}{2}}\right)^{\frac{p-1}{2}}\left(\frac{q}{p}\right)$$
$$= (-1)^{\frac{(p-1)(q-1)}{4}}\left(\frac{q}{p}\right)$$

d'où $\left(\frac{p}{q}\right) = (-1)^{\frac{(p-1)(q-1)}{4}}\left(\frac{q}{p}\right)$ $\square$

Ref : Un max de maths, p. 28

DEVELOPPEMENT n° 2 : Théorème de Chevalley-Warning

(Un max de maths, p. 33)

Soit $p \in \mathbb{P}$, $n \geq 1$ et on pose $q = p^n$.

Th (Chevalley-Warning)
Soit $(f_\alpha)_{\alpha \in A} \in \mathbb{F}_q[X_1, \dots, X_m]^A$ telles que
$$\sum_{\alpha \in A} \deg(f_\alpha) < m$$
Posons $V := \{ x \in \mathbb{F}_q^m \mid \forall \alpha \in A, f_\alpha(x) = 0 \}$
Alors $\# V \equiv 0 \ [p]$.

Pour prouver ce résultat on utilise le lemme suivant :

Lem Soit $u \in \mathbb{N}$.
On pose $S(X^u) := \sum_{x \in \mathbb{F}_q} x^u$
Alors $S(X^u) = \begin{cases} -1 & \text{si } u \geq 1 \text{ et } q-1 \mid u \\ 0 & \text{sinon} \end{cases}$

Dém
- si $u = 0$, $S(X^u) = \sum_{x \in \mathbb{F}_q} 1 = q \cdot 1 = 0$
- si $u \geq 1$ et $q-1 \mid u$.

On a $0^u = 0$ et $\forall x \in \mathbb{F}_q^*$, $x^{q-1} = 1$
donc $\forall x \in \mathbb{F}_q^*$, $x^u = 1$
$\Rightarrow S(X^u) = 0 + (q-1) \cdot 1 = q-1 = -1$

• si $u \geq 1$ et $q-1 \nmid u$

Comme $\mathbb{F}_q^*$ est cyclique de cardinal $q-1$,
il existe $y \in \mathbb{F}_q^*$ tel que $y^u \neq 1$.

En effet, dans le cas contraire on aurait
$\forall y \in \mathbb{F}_q^*$, $y^u = 1$.

Si $\mathbb{F}_q^* = \langle y_0 \rangle$, $y_0^u = 1$.

On fait la division euclidienne de u par $q-1$:
$\exists\, 0 < r < q-1$ et $a \in \mathbb{Z}$ tq $u = a(q-1) + r$.

$\Rightarrow y_0^u = 1 = (y_0^{q-1})^a y_0^r = y_0^r$

donc contradiction car y_0 est d'ordre $q-1$.

On a donc :

$$S(X^u) = \sum_{x \in \mathbb{F}_q} x^u = \sum_{x \in \mathbb{F}_q^*} x^u \underset{\substack{x \mapsto yx \\ \text{bijection}}}{=} \sum_{x \in \mathbb{F}_q^*} (yx)^u$$

$$= y^u \sum_{x \in \mathbb{F}_q^*} x^u = y^u S(X^u)$$

d'où puisque $y^u \neq 1$, $S(X^u) = 0$ □

Passons maintenant à la démonstration du théorème :

Posons $P = \prod_{\alpha \in A} (1 - f_\alpha^{q-1})$ et soit $x \in \mathbb{F}_q^n$

• si $x \in V$, $\forall \alpha \in A$, $f_\alpha(x) = 0$ donc $P(x) = 1$

• si $x \notin V$, $\exists \alpha_0 \in A$, $f_{\alpha_0}(x) \neq 0$.

Ainsi, $f_{\alpha_0}(x)^{q-1} = 1$ et $P(x) = 0$

Alors P est la fonction indicatrice de V
$P = \mathbb{1}_V$.

Pour $f \in \mathbb{F}_q[X_1, \dots X_n]$, on pose $S(f) := \sum_{x \in \mathbb{F}_q^n} f(x)$

Nous avons alors $S(P) = \sum_{x \in \mathbb{F}_q^n} \mathbb{1}_V(x) = \text{Card } V \; [p]$

On a donc $\# V = S(P) \; [p]$.

Reste à voir que $S(P) = 0$ dans $\mathbb{F}_q$.

$$\deg(P) = \sum_{\alpha \in A} \deg(1 - f_\alpha^{q-1}) = \sum_{\alpha \in A} (q-1) \deg(f_\alpha)$$
$$< n(q-1) \text{ par hypothèse}$$

donc P est combinaison linéaire de monômes
$X^u := X_1^{u_1} \dots X_n^{u_n}$, avec $\sum_{i=1}^{n} u_i < n(q-1)$

D'après le lemme des tiroirs, $\exists\, i_0 \in [\![1, n]\!]$
tel que $u_{i_0} < q-1$ et par le lemme, $S(X^{u_{i_0}}) =$

Or $S(X^u) = \sum_{x_1, \dots, x_n \in \mathbb{F}_q} x_1^{u_1} \dots x_n^{u_n} = \left(\sum_{x_1 \in \mathbb{F}_q} x_1^{u_1}\right) \dots \left(\sum_{x_n \in \mathbb{F}_q} x_n^{u_n}\right)$

$= S(X_1^{u_1}) \dots S(X_n^{u_n}) = 0$ car $S(X^{u_{i_0}}) = 0$

D'où $S(P) = 0$. □