Corps finis (suite).

Théorème (rappel).

F corps fini à q éléments. K/F extension. $\alpha \in K$ algébrique sur F. Il existe des $s \in \mathbb{Z}_{>0}$ tels que $\alpha^{q^s} = \alpha$. Soit r le plus petit. Le polynôme irréductible de α sur F est $\prod_{j=0}^{r-1} (X - \alpha^{q^j})$

$[F(\alpha) : F] = r$

$\mathrm{Frob}_p : K \longrightarrow K$ $\quad p = \text{caract. } K$.

$x \longmapsto x^p$

automorphisme de K

Si $K/\mathbb{F}_p$ est finie, $\mathrm{Gal}(K/\mathbb{F}_p)$ est cyclique engendré par Frob_p.

Notations: $\mathrm{Frob}_p^2 = \mathrm{Frob}_p \circ \mathrm{Frob}_p$

$\mathrm{Frob}_p^s = \mathrm{Frob}_p^{s-1} \circ \mathrm{Frob}_p : x \longmapsto x^{p^s}$

$\mathrm{Frob}_p^s = \mathrm{Frob}_{p^s}$

F corps fini à q éléments

K extension finie de F, alors

K/F est galoisienne cyclique

$\mathrm{Gal}(K/F)$ est engendré par Frob_q.

Démonstration du théorème

$F(\alpha)$ $\quad q^s$ $\quad \mathrm{Frob}_{q^s}(\alpha) = \alpha$ $\quad s \geq 1$

F $\quad q$ $\quad \mathrm{Frob}_{q^s}(\alpha) = \alpha^{q^s}$

r le plus petit tel que $\mathrm{Frob}_{q^r}(\alpha) = \alpha$

Si i, j vérifient $\mathrm{Frob}_q^i(\alpha) = \mathrm{Frob}_q^j(\alpha)$ alors

$i, j \in \mathbb{Z}$ $\quad \mathrm{Frob}_q^{i-j}(\alpha) = \alpha$

donc $\mathrm{Frob}_q^i(\alpha) = \mathrm{Frob}_q^k(\alpha)$ quand k est le reste de la division euclidienne de i par r. Donc $\alpha, \mathrm{Frob}_q \alpha, \mathrm{Frob}_q^2 \alpha, \dots, \mathrm{Frob}_q^{r-1}(\alpha)$ sont les conjugués de α sur F.

Donc $[F(\alpha) : F] = r$

irred. de α sur F est

$$\prod_{j=0}^{r-1} \left(X - \mathrm{Frob}_q^j(\alpha)\right).$$

Corollaire. Décomposition des polynômes cyclotomiques en facteurs irréductibles sur un corps fini. F fini q éléments n entier $\mathrm{pgcd}(n,q)=1$. Alors $\Phi_n(X)$ est produit de facteurs irréductibles de $F[X]$, degré d, d = ordre de q modulo n.

Dém. α racine de Φ_n α est d'ordre n

degré de α = le plus petit entier $r > 0$

$\alpha^{q^r - 1} = 1$

= le plus petit entier tel que

$n \mid q^r - 1$

= ordre de q dans $(\mathbb{Z}/n\mathbb{Z})^\times$.

Exemples.

$d = 1$ Φ_n complètement décomposé dans F

$\iff q \equiv 1 \bmod n. \iff n \mid q-1.$

2. $d = \varphi(n)$ $\iff q$ est d'ordre $\varphi(n)$ dans $(\mathbb{Z}/n\mathbb{Z})^\times$

$\iff (\mathbb{Z}/n\mathbb{Z})^\times$ est cyclique et l'image de q est un générateur.

3. F fini à q éléments ; $m \geq 1$

$\Phi_{q^m - 1}$ est produit de facteurs irréductibles tous de degré m. $n = q^m - 1$

Résidus quadratiques.

Extensions quadratiques de $\mathbb{F}_p$, p premier.

$p = 2$ $\mathbb{F}_2$ polyn. degré 2 :

X^2, $X^2 + X$, $X^2 + X + 1$, $X^2 + 1$

$X^2 + X + 1$ est irréductible $/\mathbb{F}_2$.

$\hookrightarrow \mathbb{F}_4$ extension de degré 2 de $\mathbb{F}_2$.

p impair.

$$X^2 + aX + b = \left(X + \frac{a}{2}\right)^2 + b - \frac{a^2}{4}.$$

$\alpha \in \mathbb{F}_p$. $\quad X^2 - \alpha \in \mathbb{F}_p[X]$.

Définition. Un élément de $\mathbb{F}_p^\times$ est un résidu quadratique si c'est un carré dans $\mathbb{F}_p$. C'est un non-résidu sinon.

Un entier $a \in \mathbb{Z}$ tel que $\operatorname{pgcd}(a,p)=1$ est un résidu quadratique modulo p si sa classe dans $\mathbb{Z}/p\mathbb{Z}$ est un carré, c'est un non-résidu sinon.

Symbole de Legendre.

$$\left(\frac{a}{p}\right) = \left(\frac{\alpha}{p}\right) = \begin{cases} 0 & \text{si } p \mid a \ (\alpha = 0) \\ 1 & \text{si } \begin{Bmatrix} \alpha \\ a \end{Bmatrix} \text{ résidu quadratique} \\ -1 & \text{si } \begin{Bmatrix} \alpha \\ \text{ou} \\ a \end{Bmatrix} \text{ non résidu.} \end{cases}$$

$a \in \mathbb{Z} \qquad \alpha \in \mathbb{F}_p$

$$\begin{array}{ccc} \mathbb{F}_p^\times & \longrightarrow & \mathbb{F}_p^\times \\ \rotatebox{90}{$\in$} & & \rotatebox{90}{$\in$} \\ x & \longmapsto & x^2 \end{array}$$

homomorphisme de groupes, image = résidus quadratiques.

noyau $\{\pm 1\}$

sous-groupe d'ordre $\frac{p-1}{2}$.

$$\sum_{\alpha \in \mathbb{F}_p} \left(\frac{\alpha}{p}\right) = 0$$

$$\boxed{\text{Pour } \alpha \in \mathbb{F}_p^\times \quad \left(\frac{\alpha}{p}\right) = \alpha^{\frac{p-1}{2}}}$$

Tout $\alpha \in \mathbb{F}_p^\times$ vérifie $\alpha^{p-1} = 1$.

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

$\alpha^{\frac{p-1}{2}} = 1 \qquad$ Si $\alpha = \beta^2$, $\beta \in \mathbb{F}_p^\times$, $\alpha^{\frac{p-1}{2}} = \beta^{p-1} = 1$

$\alpha^{\frac{p-1}{2}} = -1$

Exemple. $\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}} = \begin{cases} 1 & p \equiv 1 \bmod 4 \\ -1 & p \equiv 3 \bmod 4 \end{cases}$

$\left(\frac{\alpha}{p}\right) = \alpha^{\frac{p-1}{2}} \qquad \alpha \in \mathbb{F}_p^\times$

$\Rightarrow \left(\frac{\alpha}{p}\right)\left(\frac{\beta}{p}\right) = \left(\frac{\alpha\beta}{p}\right)$

$$\begin{array}{ccc} \mathbb{F}_p^\times & \longrightarrow & \{\pm 1\} \\ \alpha & \longmapsto & \left(\frac{\alpha}{p}\right) \end{array}$$

Caractère multiplicatif.

$\mathbb{F}_p^\times$ cyclique.

ζ un générateur.

(racine primitive $p-1$ ième de 1)

$\left(\frac{\zeta}{p}\right) = -1$ $\qquad$ $\left(\frac{\zeta^k}{p}\right) = \left(\frac{\zeta}{p}\right)^k = \begin{cases} 1 & k \text{ pair} \\ -1 & k \text{ impair} \end{cases}$

Théorème de Wilson : $(p-1)! \equiv -1 \mod p$.

$$(p-1)! = \prod_{k=1}^{p-1} \zeta^k = \zeta^{\sum_{k=1}^{p-1} k} = \zeta^{p\frac{p-1}{2}} = \zeta^{\frac{p-1}{2}}$$

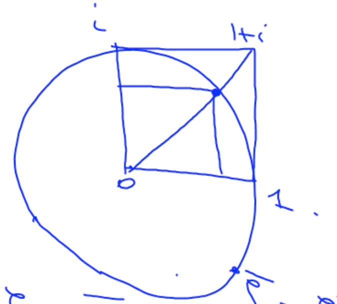
$$= \left(\frac{\zeta}{p}\right) = -1 \text{ dans } \mathbb{F}_p.$$

Calcul de $\left(\frac{2}{p}\right)$

X^2-2 irréductible sur $\mathbb{F}_p$?

Exprimer $\sqrt{2}$ avec des racines de l'unité dans $\mathbb{C}$

$\Phi_8(X) = X^4+1$



$\zeta_8 = e^{2i\pi/8} = (1+i)\frac{\sqrt{2}}{2}$

$\zeta_8^2 = i$

$\zeta_8^4 = -1$

$\zeta_8 + \overline{\zeta}_8 = \sqrt{2}$ $\qquad$ $\overline{\zeta}_8 = \zeta_8^{-1} = \zeta_8^7$

$\mathbb{F}_p \subset \mathbb{F}_{p^2} \ni \alpha$ $\qquad$ X^4+1

$|\mathbb{F}_{p^2}^\times| = p^2-1$ éléments $= (p-1)(p+1)$ multiple de 8.

α racine primitive 8ème de 1.

$\alpha^4 = -1$ $\qquad$ $\beta = \alpha + \alpha^{-1}$

$\alpha^8 = 1$. $\qquad$ $\beta^2 = \alpha^2 + \alpha^{-2} + 2 = 2$.

$\left.\begin{matrix}\alpha^2 \\ \alpha^{-2}\end{matrix}\right\}$ racines de X^2+1. $\qquad$ $\alpha^2 + \alpha^{-2} = 0$

Question : $\beta \in \mathbb{F}_p$?

Calculer β^p. $\qquad$ $\beta^p = \beta \iff \beta \in \mathbb{F}_p \iff \left(\frac{2}{p}\right) = 1$

$\beta = \alpha + \alpha^{-1}$

$\beta^p = \alpha^p + \alpha^{-p}$ $\qquad$ $\beta^p = -\beta \iff \beta \notin \mathbb{F}_p \iff \left(\frac{2}{p}\right) = -1$

α^p ne dépend que de la classe de p modulo 8.

$\alpha^8 = 1$

$\beta^p = \beta \Longleftarrow \begin{cases} p \equiv 1 \mod 8 & \alpha^p = \alpha,\ \alpha^{-p} = \alpha^{-1} \\ p \equiv 7 \mod 8 & \alpha^p = \alpha^{-1},\ \alpha^{-p} = \alpha \end{cases}$

$\alpha^3 = -\alpha^{-1}$

$\alpha^5 = -\alpha$

$\beta^p = -\beta \Longleftarrow \begin{cases} p \equiv 3 \mod 8 & \alpha^p = -\alpha^{-1},\ \alpha^{-p} = -\alpha \\ p \equiv 5 \mod 8 & \alpha^p = -\alpha,\ \alpha^{-p} = -\alpha^{-1}. \end{cases}$

Conclusion : $\left(\frac{2}{p}\right) = \begin{cases} 1 & p \equiv \pm 1 \bmod 8 \\ -1 & p \equiv \pm 3 \bmod 8 \end{cases}$.

$$= (-1)^{\frac{p^2-1}{8}}$$

$p \equiv 1 \bmod 8$ $\quad \frac{p-1}{4}$ pair. $\quad \frac{p+1}{2}$ impair.

$\cdot\ 3$ $\quad \frac{p-1}{2}$ impair $\quad \frac{p+1}{4}$ pair.

Loi de réciprocité quadratique.

ℓ, p premiers impairs distincts

$$\left(\frac{\ell}{p}\right) = (-1)^{\frac{\ell-1}{2}\cdot\frac{p-1}{2}} \cdot \left(\frac{p}{\ell}\right)$$

Signe $+$ si $p \equiv 1 \bmod 4$

$+$ si $\ell \equiv 1 \bmod 4$

$-$ si $p \equiv 3 \bmod 4$ et $\ell \equiv 3 \bmod 4$

Gauss.

Caractère multiplicatif : $\mathbb{F}_p^\times \longrightarrow \{\pm 1\}$

$\alpha \longmapsto \left(\frac{\alpha}{p}\right)$.

Caractère additif. $\mathbb{F}_p \longrightarrow K$.

$\alpha \longmapsto \zeta^\alpha$

K contenant une racine primitive p-ième de 1.

$X^p - 1 = (X-1)^p$.

en caract. p.

ζ

$\mathbb{Z} \longrightarrow K^\times$ $\quad$ homom. noyau $p\mathbb{Z}$.

$\alpha \longmapsto \zeta^\alpha$

$\mathbb{F}_p \longrightarrow K^\times$

$\alpha \longmapsto \zeta^\alpha$

Somme de Gauss :

$$S = \sum_{\alpha \in \mathbb{F}_p^\times} \left(\frac{\alpha}{p}\right) \zeta^\alpha$$

$\beta \in \mathbb{F}_p^\times$

$\alpha \longmapsto \alpha\beta$ permutation de $\mathbb{F}_p^\times$

$$S = \sum_{\alpha \in \mathbb{F}_p^\times} \left(\frac{\alpha}{p}\right) \zeta^\alpha.$$

$\beta \in \mathbb{F}_p^\times$ $\quad S = \sum_{\alpha \in \mathbb{F}_p^\times} \left(\frac{\alpha\beta}{p}\right) \zeta^{\alpha\beta}$

$$= \left(\frac{\beta}{p}\right) \sum_{\alpha \in \mathbb{F}_p^\times} \left(\frac{\alpha}{p}\right) \zeta^{\alpha\beta}.$$

$$S^2 = \sum_{\beta \in \mathbb{F}_p^\times} \left(\frac{\beta}{p}\right) \zeta^\beta \left(\frac{\beta}{p}\right) \sum_{\alpha \in \mathbb{F}_p^\times} \left(\frac{\alpha}{p}\right) \zeta^{\alpha\beta}.$$

$$= \sum_{\alpha \in \mathbb{F}_p^\times} \left(\frac{\alpha}{p}\right) \sum_{\beta \in \mathbb{F}_p^\times} \zeta^{\alpha\beta+\beta}.$$

$$S^2 = \sum_{\alpha\in\mathbb{F}_p^\times} \left(\frac{\alpha}{p}\right)\cdot \tau_\alpha$$

$$= \underbrace{\left(\frac{-1}{p}\right)(p-1)}_{\alpha=-1} - \sum_{\substack{\alpha\in\mathbb{F}_p^\times \\ \alpha\neq -1}} \left(\frac{\alpha}{p}\right)$$

$$\sum_{\alpha\in\mathbb{F}_p^\times}\left(\frac{\alpha}{p}\right)=0$$

$$\sum_{\alpha\neq -1}\left(\frac{\alpha}{p}\right)+\left(\frac{-1}{p}\right)=0$$

$$S^2 = \left(\frac{-1}{p}\right)p.$$

K corps de décomposition de X^p-1 sur $\mathbb{F}_\ell$.

$\cup$

ζ

$$S^{\ell-1} = (S^2)^{\frac{\ell-1}{2}} = \left(-\frac{1}{p}\right)^{\frac{\ell-1}{2}}\cdot p^{\frac{\ell-1}{2}}.$$

$$\left(-\frac{1}{p}\right) = (-1)^{\frac{p-1}{2}}. \qquad = (-1)^{\frac{p-1}{2}\cdot\frac{\ell-1}{2}}\cdot p^{\frac{\ell-1}{2}}.$$

D'autre part

$$S^\ell = \sum_{\alpha\in\mathbb{F}_p^\times}\left(\frac{\alpha}{p}\right)^\ell\cdot\zeta^{\ell\alpha} = \sum_{\alpha\in\mathbb{F}_p^\times}\left(\frac{\alpha}{p}\right)\zeta^{\ell\alpha}.$$

$$S^\ell = \sum_{\alpha\in\mathbb{F}_p^\times}\left(\frac{\alpha}{p}\right)\zeta^{\ell\alpha}$$

$$= \left(\frac{\ell}{p}\right)\cdot\underbrace{\sum_{\alpha\in\mathbb{F}_p^\times}\left(\frac{\ell\alpha}{p}\right)\zeta^{\ell\alpha}}_{S}.$$

$$S^{\ell-1} = \left(\frac{\ell}{p}\right)$$

$$= (-1)^{\frac{p-1}{2}\cdot\frac{\ell-1}{2}}\cdot\left(\frac{p}{\ell}\right)$$

Norme et Trace.

K
$|$) finie s
F fini $q=|F|$.

$\mathrm{Gal} = \langle \mathrm{Frob}_q\rangle$.

$$N_{K/F} : K\to F \qquad \alpha\mapsto\prod_{i=0}^{s-1}\mathrm{Frob}_q^i(\alpha)$$

$$\mathrm{Tr}_{K/F} : K\to F \qquad \alpha\mapsto\sum_{i=0}^{s-1}\mathrm{Frob}_q^i(\alpha)$$

$$\mathrm{Frob}_q^i(\alpha)=\alpha^{q^i}.$$

$$N_{K/F}(\alpha)=\alpha\cdot\alpha^{q}\cdot\alpha^{q^2}\cdots\alpha^{q^{s-1}} = \alpha^{\frac{q^s-1}{q-1}}\in F.$$

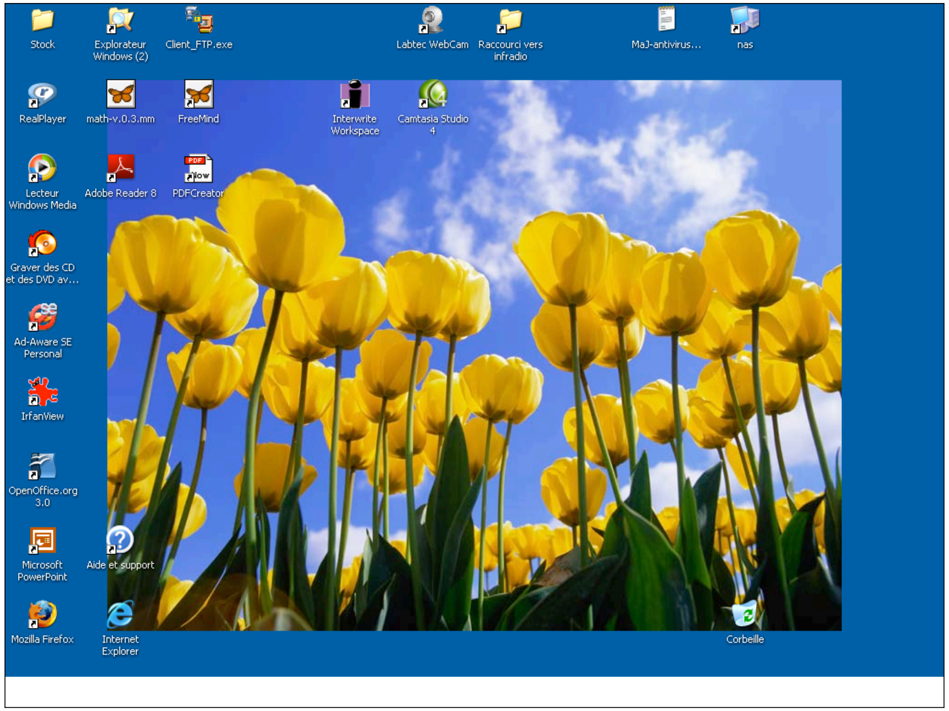
$$\alpha \in F \longrightarrow N_{K/F}(\alpha) = \alpha^s.$$

$$Tr_{K/F}(\alpha) = s\alpha.$$

$N_{K/F} : K^\times \longrightarrow F^\times$ homomorphisme de groupes.

$Tr_{K/F} : K \longrightarrow F$ forme linéaire de F-espaces vectoriels.

$Tr_{K/F}$ est surjective de noyau les racines du polynôme $X + X^q + \dots + X^{q^{s-1}}$.



$$\sum_{\beta \in \mathbb{F}_p^\times} \left(\zeta^{(\alpha+1)}\right)^\beta = \sigma = \underset{\underset{0}{\parallel}}{\Phi_p\left(\zeta^{(\alpha+1)}\right)} - 1$$

$\alpha = -1.$ $\zeta^{\alpha+1} = 1.$ $\sigma = p-1.$

$\alpha \neq -1.$ $\zeta^{\alpha+1}$ racine primitive p-ième de 1 dans K.

$$X^p - 1 = \prod_{\beta \in \mathbb{F}_p} \left(X - \zeta^{(\alpha+1)\beta}\right). \qquad \sum_{\beta \in \mathbb{F}_p} \zeta^{(\alpha+1)\beta} = 0$$

$$\Rightarrow \sigma = -1.$$