Introduction aux corps finis

Serge Haddad, LMF, ENS Paris-Saclay & CNRS

Groupes

G, un ensemble doté d'une loi interne $\oplus$ est un groupe si :

- $\oplus$ est associative : $\forall a, b, c\ (a \oplus b) \oplus c = a \oplus (b \oplus c)$;
- Il existe un élément neutre : $\exists 0\ \forall a\ a \oplus 0 = 0 \oplus a = a$;
- Tout élément a un inverse : $\forall a\ \exists -a\ a \oplus -a = -a \oplus a = 0$.

Illustration. Soit $\mathbb{Z}_n = \{0, 1, \ldots, n-1\}$ muni de l'addition modulo n.
$\mathbb{Z}_n$ est un groupe avec pour tout $i \neq 0$, $-i = n - i$.

Soit $|G| = n$. n est dit *l'ordre* du groupe.

G est *commutatif* si $\oplus$ est commutative : $\forall a, b\ a \oplus b = b \oplus a$.

Notation. Soit $k \in \mathbb{N}$ et $g \in G$. On définit inductivement $k \cdot g \in G$ par :

$$0 \cdot g = 0 \text{ et } (k+1) \cdot g = k \cdot g \oplus g.$$

Sous-groupes

Soit $\emptyset \neq S \subseteq G$. S est un *sous-groupe* de G si $\forall a, b \in S \ \{-a, a \oplus b\} \subseteq S$.
Par conséquent S est aussi un groupe.

Soit $g \in G$, $S \oplus g = \{a \oplus g \mid a \in S\}$ est la *classe* de g (par S).

Propriétés. Soit $n = |G|$ et $m = |S|$

- $\forall g \in G$, $|S \oplus g| = m$;
- L'ensemble des classes forme une partition de G ;
- Par conséquent $m|n$.

Illustration. Soit $\mathbb{Z}_n$ avec n pair.

Alors l'ensemble $\{0, 2, 4, \ldots, n-2\}$ est un sous-groupe de $\mathbb{Z}_n$

isomorphe à $\mathbb{Z}_{\frac{n}{2}}$ par $i \mapsto \frac{i}{2}$.

La classe de 1 est $\{1, 3, 5, \ldots, n-1\}$.

Groupe et sous-groupe cyclique

G d'ordre n est *cyclique* s'il existe $g \in G$ tel que :

$$G = \{0, 1 \cdot g, \ldots, (n-1) \cdot g\} \text{ et } n \cdot g = 0.$$

g est appelé un *générateur* de G.

$\mathbb{Z}_n$ est cyclique.

Tout groupe cyclique d'ordre n est isomorphe à $\mathbb{Z}_n$ par $i \cdot g \mapsto i$.

Soit G un groupe fini et $g \in G$.
$S(g) = \{0, g, 2 \cdot g, \ldots\}$ est un sous-groupe cyclique.

$ord(g)$, l'ordre de g, est l'ordre de $S(g)$ et vérifie $ord(g) = \min(k \mid k \cdot g = 0)$.

0 est l'unique élément d'ordre 1.

Observation. L'ordre de $m \in \mathbb{Z}_n^*$ est égal à $\frac{n}{pgcd(m,n)}$.

Le *nombre d'Euler* $\Phi(n)$ est le nombre de $m \in \mathbb{Z}_n$ t.q. l'ordre de m soit égal n :

$\Phi(n)$ est le nombre de $1 \leq m \leq n$ tels que $pgcd(m, n) = 1$.

Relation d'Euler

Soit d un diviseur de n, $g \in \mathbb{Z}_n$ est d'ordre d si

1. $dg = 0 \mod n$;
2. $\forall 0 < d' < d \; d'g \neq 0 \mod n$.

① $dg = 0 \mod n \Leftrightarrow \exists k \; dg = kn \Leftrightarrow \exists k \; g = k\frac{n}{d} \Leftrightarrow g \in S(\frac{n}{d})$

② On note $g = s\frac{n}{d}$ avec $0 \leq s < d$.

$$\begin{aligned}
&\forall 0 < d' < d \; d's\frac{n}{d} \neq 0 \mod n \\
\Leftrightarrow\; &\forall 0 < d' < d \; d's\frac{n}{d} \neq 0 \mod d\frac{n}{d} \\
\Leftrightarrow\; &\forall 0 < d' < d \; d's \neq 0 \mod d \\
\Leftrightarrow\; &s \neq 0 \wedge pgcd(s, d) = 1
\end{aligned}$$

Par conséquent $g \in \mathbb{Z}_n$ est d'ordre d ssi $g = s\frac{n}{d}$ avec $0 < s < d$ et $pgcd(s, d) = 1$.
Il y a donc $\Phi(d)$ éléments de $\mathbb{Z}_n$ d'ordre d. Puisque tout élément a un ordre :

$$\boxed{n = \sum_{d|n} \Phi(d)}$$

Action d'un groupe sur un ensemble (1)

Soit E un ensemble fini et G un groupe fini de loi $*$

et d'élément neutre 1.

$\otimes$ de $G \times E$ dans E est une *action* de G sur E si :

$$(g * g') \otimes e = g \otimes (g' \otimes e) \text{ et } 1 \otimes e = e.$$

O_e, *l'orbite* de e sous l'action de G est définie par $O_e = \{g \otimes e \mid g \in G\}$.

L'ensemble des orbites forme une partition de E.

Preuve.

Pour tout e puisque $1 \otimes e = e$, $E = \bigcup_{e \in E} O_e$.

Soit e et e' tels que $\exists e'' \in O_e \cap O_{e'}$.

$e'' = g \otimes e = g' \otimes e'$. Donc $e = (g^{-1} * g') \otimes e'$

ce qui implique $O_e \subseteq O_{e'}$.

Par symétrie, $O_e = O_{e'}$.

Action d'un groupe sur un ensemble (2)

St_e, le *stabilisateur* de e, un sous-ensemble de G est défini par :

$$St_e = \{g \in G \mid g \otimes e = e\}.$$

St_e est un sous-groupe :

- $1 \in St_e$ car $1 \otimes e = e$
- Soit $g, g' \in St_e$, $(g * g') \otimes e = g \otimes (g' \otimes e) = g \otimes e = e$. Donc $g * g' \in St_e$.
  $e = (g^{-1} * g) \otimes e = g^{-1} \otimes (g \otimes e) = g^{-1} \otimes e$. Donc $g^{-1} \in St_e$.

$$\boxed{|O_e| = \frac{|G|}{|St_e|}}$$

Preuve.

Définissons $g \sim g'$ si $\exists h \in St_e \; g' = h * g$

$g \sim g$ avec $h = 1$; $g = h^{-1} * g'$ donc $\sim$ est symétrique.

$g'' = h' * g'$ implique $g'' = (h' * h) * g$ donc $\sim$ est transitive et une équivalence.

La classe de g est $\{g' * g \mid g' \in St_e\}$ et $g' * g = g'' * g$ implique :

$$g'' = g'' * g * g^{-1} = g' * g * g^{-1} = g'.$$

Donc les classes ont même cardinal $|St_e|$ et le nombre de classes est $\frac{|G|}{|St_e|}$.

Soit H un ensemble de représentants de classe.

Alors $h \mapsto h \otimes e$ est une bijection de H dans O_e.

Corps gauche

Un ensemble $\mathbb{F}$ contenant 0 et $1 \neq 0$, muni des lois $\oplus$ et $*$ est un *corps gauche* si :

- $\mathbb{F}$ muni de $\oplus$ est un groupe commutatif dont 0 est l'élément neutre ;
- $\mathbb{F}^* = \mathbb{F} \setminus \{0\}$ muni de $*$ est un groupe dont 1 est l'élément neutre ;
- $*$ est distributive par rapport à $\oplus$:

  $\forall a, b, c \; a * (b \oplus c) = (a * b) \oplus (a * c) \wedge (b \oplus c) * a = (b * a) \oplus (c * a)$

Si $*$ est commutative, $\mathbb{F}$ est un *corps commutatif*.

Illustration. Soit p un nombre premier.

$\mathbb{F}_p = \{0, 1, \ldots, p-1\}$ muni de $+$ et de $\times$ modulo p est un corps commutatif.

Preuve.

Soit $a \neq 0$ et $f_a(b) = ab \mod p$. $f_a(\mathbb{F}_p^*) \subseteq \mathbb{F}_p^*$ car $b \neq 0 \Rightarrow ab \mod p \neq 0$.

f_a est injective donc bijective car $b \neq b' \Rightarrow a(b - b') \mod p \neq 0$.

Donc $\exists b \; f_a(b) = ab \mod p = 1$.

Observation. Si p n'est pas premier alors $\mathbb{F}_p$ n'est pas un corps.

Sous-corps

Soit $\mathbb{F}$ un corps. $\mathbb{F}' \subseteq \mathbb{F}$ est un *sous-corps* si :

- $\mathbb{F}'$ muni de $\oplus$ est un sous-groupe de $\mathbb{F}$;
- $\mathbb{F}'^*$ muni de $*$ est un sous-groupe de $\mathbb{F}^*$.

Dans la suite, $\mathbb{F}$ est un corps gauche fini.

Soit $a \in \mathbb{F}$. $\mathbb{G}_a = \{x \in \mathbb{F} \mid \in \mathbb{F}\ x * a = a * x\}$.

$\mathbb{G}_0 = \mathbb{G}_1 = \mathbb{F}$. Soit $a \notin \{0, 1\}$, $\{0, 1\} \subseteq \mathbb{G}_a$.

Soit $b, c \in \mathbb{G}_a^*$.

- $0 = (b \oplus -b) * a = b * a \oplus -b * a = a * b \oplus -b * a$ donc $-b * a = a * -b$;
- $(b \oplus c) * a = b * a \oplus c * a = a * b \oplus a * c = a * (b \oplus c)$;
- $a^{-1} * b * a * b^{-1} = a^{-1} * a * b * b^{-1} = 1$ d'où $a * b^{-1} = (a^{-1} * b)^{-1} = b^{-1} * a$;
- $a * b * c = b * a * c = b * c * a$.

$\mathbb{G}_a$ est donc un sous-corps de $\mathbb{F}$.

$\mathbb{G} = \bigcap_{a \in \mathbb{F}} \mathbb{G}_a$ est un corps commutatif appelé le *centre* de $\mathbb{F}$.

Espaces vectoriels à gauche

Soit $(E, +)$ un groupe commutatif, $\mathbb{F}$ un corps gauche

et $\cdot$ une application de $\mathbb{F} \times E$ dans E.

E est un $\mathbb{F}$-espace vectoriel à gauche si $\lambda, \mu \in \mathbb{F}$ et $e, f \in E$:

- $1 \cdot e = e$;
- $\lambda \cdot (e + f) = \lambda \cdot e + \lambda \cdot f$;
- $(\lambda + \mu) \cdot e = \lambda \cdot e + \mu \cdot e$;
- $(\lambda * \mu) \cdot e = \lambda \cdot (\mu \cdot e)$.

Soit $\mathcal{F} = \{e_i\}_{i \in I}$ une famille de E, $Gen(\mathcal{F}) = \{e \mid \exists \{\lambda_i\}_{i \in I}\ e = \sum_{i \in I} \lambda_i \cdot e_i\}$.

$\mathcal{F}$ est *libre* si pour toute famille $\{\lambda_i\}_{i \in I}$ de $\mathbb{F}$,

$$\sum_{i \in I} \lambda_i \cdot e_i = 0 \Rightarrow \forall i \in I\ \lambda_i = 0$$

$\mathcal{F}$ est *génératrice* si $E = Gen(\mathcal{F})$.

$\mathcal{F}$ est une *base* si elle est libre et génératrice.

Dimension d'un espace vectoriel (1)

Soit une famille libre maximale $\mathcal{F} = \{e_i\}_{1 \leq i \leq d}$. Alors :

- $\mathcal{F}$ est une base ;
- Toute famille libre maximale $\mathcal{F}' = \{e'_j\}_{1 \leq j \leq d'}$ vérifie $d' = d$.

Si une telle famille existe alors d est la dimension finie de E.

Preuve.

Supposons que $\mathcal{F}$ ne soit pas une base : soit $f \notin Gen(\mathcal{F})$.

Montrons que $\mathcal{F} \cup \{f\}$ est libre. Soit $\sum_{i \in I} \lambda_i \cdot e_i + \lambda \cdot f = 0$.

Si $\lambda \neq 0$ alors $f = \sum_{i \in I} (\lambda^{-1} * -\lambda_i) \cdot e_i \in Gen(\mathcal{F})$.

D'où $\lambda = 0$ ce qui implique pour tout i, $\lambda_i = 0$.

Dimension d'un espace vectoriel (2)

Preuve (suite). On note $I = \{1, \ldots, d'\}$.

Montrons que pour tout $0 \leq k \leq d$,

il existe une base $\mathcal{F}_k = \{e'_j\}_{j \in I_k} \cup \{e_i\}_{i \leq k}$ tel que $|I \setminus I_k| = k$.

$\mathcal{F}_0 = \mathcal{F}'$ vérifie le cas de base.

Supposons l'existence prouvée pour $k < d$. $e_{k+1} = \sum_{j \in I_k} \mu_j \cdot e'_j + \sum_{i \leq k} \nu_i \cdot e_i$.

Puisque $\mathcal{F}$ est libre, $\exists j_{k+1}\ \mu_{j_{k+1}} \neq 0$. Soit $I_{k+1} = I_k \setminus \{j_{k+1}\}$.

Donc $e'_{j_{k+1}} = \mu^{-1}_{j_{k+1}} \cdot e_{k+1} - \sum_{j \in I_{k+1}} \mu^{-1}_{j_{k+1}} * \mu_j \cdot e'_j - \sum_{i \leq k} \mu^{-1}_{j_{k+1}} * \nu_i \cdot e_i$.

Donc $\mathcal{F}_{k+1}$ est génératrice.

Soit $\sum_{j \in I_{k+1}} \theta'_j \cdot e'_j + \sum_{i \leq k+1} \theta_i \cdot e_i = 0$. D'où :

$\theta'_{k+1} * \mu_{j_{k+1}} \cdot e'_{j_{k+1}} + \sum_{j \in I_{k+1}} (\theta'_j + \theta'_{k+1} * \mu_j) \cdot e'_j + \sum_{i \leq k} (\theta_i + \theta'_{k+1} * \nu_i) \cdot e_i = 0$

Puisque $\mathcal{F}_k$ est libre,

$\theta'_{k+1} = 0$ ce qui implique pour tout $j \in I_{k+1}$, $\theta'_j = 0$ et tout $i \leq k$, $\theta_i = 0$.

Donc $\mathcal{F}_{k+1}$ est libre.

$\mathcal{F}_d = \{e'_j\}_{j \in I_d} \cup \mathcal{F}$ avec $|I_d| = d' - d$. D'où $d' \geq d$.

Puisque $\mathcal{F}$ est maximale, $I_d = \emptyset$ et $d' = d$.

Sous-corps et espaces vectoriels

Soit $\mathbb{F}'$ un sous-corps de $\mathbb{F}$, un corps gauche fini.

En considérant $*$ comme une opération de $\mathbb{F}' \times \mathbb{F}$ dans $\mathbb{F}$,

on vérifie que $\mathbb{F}$ est un $\mathbb{F}'$-espace vectoriel.

Puisque $\mathbb{F}$ est fini sa dimension d est finie.

On note $q = |\mathbb{G}|$.

Soit $\mathbb{F}'$ un corps tel que $\mathbb{G} \subseteq \mathbb{F}' \subseteq \mathbb{F}$.

$\mathbb{F}'$ est un $\mathbb{G}$-espace vectoriel de dimension d'. D'où $|\mathbb{F}'| = q^{d'}$.

$\mathbb{F}$ est un $\mathbb{F}'$-espace vectoriel à gauche de dimension d''.

D'où $|\mathbb{F}| = (q^{d'})^{d''} = q^{d'd''}$ et $d = d'd''$.

Polynômes

Soit $P = \sum_{i \leq d} p_i X^i$, un polynôme de degré $deg(P) = d$ (i.e., $p_d \neq 0$)
à coefficients dans un corps commutatif $\mathbb{F}$,

- P est *unitaire* si $p_d = 1$;
- Q est un *diviseur* de P s'il existe R tel que $P = QR$.
  Q est un *facteur* de P s'il est unitaire et $1 \leq deg(Q) < d$;
- P tel que $deg(P) > 0$ est *irréductible* s'il n'a pas de facteurs ;
- P est *premier* s'il est irréductible et unitaire.

Tout polynôme unitaire de degré non nul admet une unique factorisation (à l'ordre près) en polynômes premiers $P = \prod_{i \in I} P_i$.

Illustration.

$X^2 + X \in \mathbb{F}_2[X]$ se factorise en $X(X+1)$.

$X^2 + X + 1 \in \mathbb{F}_2[X]$ est irréductible.

$X^2 + 1 \in \mathbb{F}_2[X]$ se factorise en $(X+1)^2$.

Racines n^{iemes} de l'unité

Soit $n > 0$. On note $\omega_k = e^{2ik\pi/n} \in \mathbb{C}$ et $U_n = \{\omega_k \mid 0 \leq k < n\}$.

$(U_n, \times)$ est un groupe isomorphe à $(\mathbb{Z}_n, \oplus)$.

Le polynôme $X^n - 1 \in \mathbb{C}[X]$ a pour racines les éléments de U_n. D'où :

$$X^n - 1 = \prod_{0 \leq k < n} X - \omega_k$$

$\mathrm{Pr}_n = \{\omega_k \mid ord(\omega_k) = n\}$ est l'ensemble des racines *primitives*.

Le polynôme *cyclotomique* d'ordre n est défini par $\Phi_n = \prod_{\omega_k \in Pr_n} X - \omega_k$.

D'où : $X^n - 1 = \prod_{d|n} \Phi_d$.

$\boxed{\Phi_d \text{ est à coefficients entiers.}}$

Preuve. Par récurrence : $\Phi_1 = X - 1$.

Φ_n est le résultat de la division de $X^n - 1$ par

$\prod_{d|n, d<n} \Phi_d$, un polynôme unitaire.

Une action de $\mathbb{F}^*$ sur lui-même

On définit l'opération $\circ$ de $(\mathbb{F}^*, *)$ sur lui-même par : $g \circ h = g * h * g^{-1}$

$\circ$ est une action car :

$$(g * g') \circ h = g * g' * h * g'^{-1} * g^{-1} = g * (g' \circ h) * g'^{-1} = g \circ (g' \circ h)$$

Par définition, $St_h = \mathbb{G}_h^*$ et pour tout $g \in \mathbb{G}^*$, $O_g = \{g\}$

Soit $\{g_1, \ldots, g_K\}$, un ensemble de représentants par orbite

non réduite à un singleton.

En appliquant le résultat sur les orbites :

$$|\mathbb{F}^*| = |\mathbb{G}^*| + \sum_{i \leq K} \frac{|\mathbb{F}^*|}{|\mathbb{G}_{g_i}^*|}$$

Puisque $\mathbb{G}_{g_i}$ est un $\mathbb{G}$-espace vectoriel,

il existe $1 \leq d_i < d$ tel que $|\mathbb{G}_{g_i}| = q^{d_i}$. D'où :

$$q^d - 1 = q - 1 + \sum_{i \leq K} \frac{q^d - 1}{q^{d_i} - 1}$$

Théorème de Wedderburn

$\mathbb{F}$ est un $\mathbb{G}_{g_i}$-espace vectoriel, donc $d_i | d$.

Soit le polynôme $F = X^d - 1 - \sum_{i \leq K} \frac{X^d - 1}{X^{d_i} - 1}$ ($F(q) = q - 1$ voir plus haut).

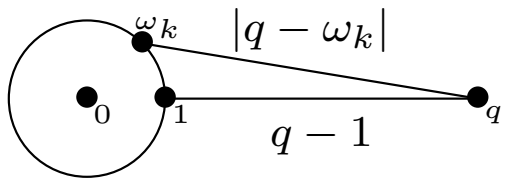
$$\frac{X^d - 1}{X^{d_i} - 1} = \prod_{d' \neq d_i, d' | d} \Phi_{d'}$$

Par conséquent Φ_d divise F.

On note $F = \Phi_d Q$ avec $Q \in \mathbb{Z}[X]$ puisque Φ_d est unitaire.

$0 < q - 1 = \Phi_d(q) Q(q) \Rightarrow Q(q) \neq 0 \Rightarrow |Q(q)| \geq 1 \Rightarrow |\Phi_d(q)| \leq q - 1$

Pour tout $n \geq 1$, $|\Phi_n(q)| = \prod_{\omega_k \in \mathrm{Pr}_n} |q - \omega_k|$.



Or pour tout k, $|q - \omega_k| \geq 1$ et $|q - \omega_k| = 1$ ssi $k = 0$. D'où $d = 1$ et $\mathbb{F} = \mathbb{G}$.

Tout corps gauche fini est commutatif.

Caractéristique d'un corps

Soit le sous-groupe $(S(1), \oplus)$ de $\mathbb{F}$. Alors :

$p = |S(1)|$ est premier et $(S(1), \oplus, *)$ est un sous-corps de $\mathbb{F}$ isomorphe à $\mathbb{F}_p$.

Preuve. $(S(1), \oplus)$ est isomorphe à $(\mathbb{Z}_p, +)$.
Pour tout $a \cdot 1, b \cdot 1 \in S(1)^*$, $a \cdot 1 * b \cdot 1 = (ab \mod p) \cdot 1 \in S(1)^*$
car $(\mathbb{F}^*, *)$ est un groupe. Donc $ab \mod p \neq 0$, ce qui implique que p est premier.

Soit $f_a(b \cdot 1) = a \cdot 1 * b \cdot 1 = (ab \mod p) \cdot 1$. $f_a(S(1)^*) \subseteq S(1)^*$.
Soit $c \cdot 1 \in S(1)^*$ tel que $f_a(b \cdot 1) = f_a(c \cdot 1)$. Donc $(a(b-c) \mod p) \cdot 1 = 0$.
Puisque $f_a(S(1)^*) \subseteq S(1)^*$ et p premier, $b = c$. Donc f_a est injective puis bijective.
D'où $\exists a^{-1} \cdot 1 \in S(1)^*$ $a \cdot 1 * a^{-1} \cdot 1 = 1$. $(S(1), \oplus, *)$ est donc un sous-corps de $\mathbb{F}$.

Puisque $a \cdot 1 * b \cdot 1 = (ab \mod p) \cdot 1$, $(S(1)^*, *)$ est isomorphe à $(\mathbb{Z}_p^*, \times)$.

p est appelée la *caractéristique* de $\mathbb{F}$.

Corollaire. Tout corps $\mathbb{F}$ tel que $p = |\mathbb{F}|$ est premier est isomorphe à $\mathbb{F}_p$.

$(\mathbb{F}_q^*, *)$ est cyclique

Soit $\mathbb{F}_q$ un corps à q éléments et d un diviseur de $q-1$.

Il y a au plus un sous-groupe cyclique multiplicatif $\mathbb{F}_q^*$ d'ordre d car :

- Les d éléments d'un tel sous-groupe sont des racines de $X^d - 1$;
- Il y a au plus d racines de $X^d - 1$.

Dans cet éventuel sous-groupe il y a exactement $\Phi(d)$ éléments d'ordre multiplicatif d. Donc le nombre d'éléments de $\mathbb{F}_q^*$ est inférieur ou égal à

$$\sum_{d|q-1} \Phi(d)$$

Puisque $q - 1 = \sum_{d|q-1} \Phi(d)$ cela implique que :

- Pour tout diviseur de $q-1$
  il y a un unique sous-groupe multiplicatif cyclique d'ordre d ;
- et donc il y a $\Phi(q-1) > 0$ éléments d'ordre $q-1$;
- et le sous-groupe multiplicatif $\mathbb{F}_q^*$ est cyclique.

Factorisation de $X^q - X$

Soit $\mathbb{F}_q$ un corps fini de cardinal q et $\beta \in \mathbb{F}_q^*$.

L'ordre du groupe multiplicatif $S(\beta) = \{1, \beta, \beta^2, \ldots\}$ vérifie

- $\beta^{|S(\beta)|} = 1$;
- $|S(\beta)|$ divise $q-1$ qui implique $\beta^{q-1} = 1$.

D'où les factorisations dans $\mathbb{F}_q[X]$:

$$X^{q-1} - 1 = \prod_{\beta \neq 0} X - \beta \text{ et } X^q - X = \prod_{\beta \in \mathbb{F}_q} X - \beta$$

Soit p la caractéristique de $\mathbb{F}_q$, $\mathbb{F}_p \subseteq \mathbb{F}_q$
et $\prod_{i \leq k} Q_i$ la factorisation de $X^q - X$ dans $\mathbb{F}_p[X]$.

Alors $Q_i = \prod_{j \leq k_i} X - \beta_{i,j}$ tel que pour tout $\beta \in \mathbb{F}_q$,
il existe un unique (i,j) tel que $\beta_{i,j} = \beta$.

Q_i est appelé *le polynôme minimal* de β (aussi noté Q_β)

Propriétés d'un polynôme minimal

Q_β le polynôme minimal de β vérifie :

- Pour tout $Q \neq Q_\beta$, polynôme unitaire t.q. $Q(\beta) = 0$, $deg(Q_\beta) < deg(Q)$;
- Pour tout Q t.q. $Q(\beta) = 0$, Q_β divise Q.

Preuve. Le cas $\beta = 0$ est évident car $Q_0 = X$. Soit $\beta \neq 0$.

• Soit $Q \neq Q_\beta$, polynôme unitaire tel que $Q(\beta) = 0$ et $deg(Q)$ soit minimal.
Soit $Q_\beta = Q \cdot D + R$ la division euclidienne de Q_β par Q,
Puisque $deg(R) < deg(Q)$ et $R(\beta) = 0$, $R = 0$. Donc Q divise Q_β.
Puisque Q_β est irréductible et Q est unitaire, $Q = Q_\beta$.

• Soit Q tel que $Q(\beta) = 0$,
Soit $Q = Q_\beta \cdot D + R$ la division euclidienne de Q par Q_β,
Puisque $deg(R) < deg(Q_\beta)$ et $R(\beta) = 0$, $R = 0$. Donc Q_β divise Q.

$\mathbb{F}_p[Q]$

Soit $Q \in \mathbb{F}_p[X]$, polynôme premier avec $d = deg(Q)$.

$\mathbb{F}_p[Q]$ est l'ensemble des polynômes de degré inférieur à d
muni de l'addition notée $\oplus$ et de la multiplication modulo Q notée $*$.

$\boxed{\mathbb{F}_p[Q] \text{ est un corps.}}$

Preuve.

• Soit $R \in \mathbb{F}_p[Q]^*$ et pour tout $S \in \mathbb{F}_p[Q]^*$, $f_R(S) = R * S$.
$f_R(\mathbb{F}_p[Q]^*) \subseteq \mathbb{F}_p[Q]^*$ car $R * S = 0$ implique $\exists S'\ R \cdot S = Q \cdot S'$.

Puisque Q est irréductible
et que la factorisation de $R \cdot S$ est le produit de la factorisation de R et de S,
Q divise R ou S ce qui implique que R ou S est nul.

• f_R est injective donc bijective car $R * S = R * S'$
implique $R * (S - S') = 0$ implique $S - S' = 0$.

• Donc pour tout $R \in \mathbb{F}_p[Q]^*$, il existe $R^{-1} \in \mathbb{F}_p[Q]^*$ tel que $R * R^{-1} = 1$.

$\mathbb{F}_p[\beta]$

Soit $\beta \in \mathbb{F}_q^*$ avec $d = deg(Q_\beta)$.

$\mathbb{F}_p[\beta] = \{P(\beta) \mid P \in \mathbb{F}_p[X]\}$.

$\boxed{\mathbb{F}_p[\beta] \text{ est un corps d'ordre } p^d \text{ isomorphe à } \mathbb{F}_p[Q_\beta].}$

Preuve.

• Soit $P \in \mathbb{F}_p[X]$ et $P = DQ_\beta + R$ la division euclidienne de P par Q_β.
Alors $P(\beta) = R(\beta)$. D'où $\mathbb{F}_p[\beta] = \{P(\beta) \mid P \in \mathbb{F}_p[X] \wedge deg(P) < d\}$.

• Soit R et S de degré inférieur à d avec $R(\beta) = S(\beta) \Leftrightarrow (R - S)(\beta) = 0$.
Puisque $P \neq 0 \wedge P(\beta) = 0 \Rightarrow deg(P) \geq d$, $R - S = 0$.

• Soit f de $\mathbb{F}_p[Q_\beta]$ dans $\mathbb{F}_p[\beta]$ définie par $f(P) = P(\beta)$.
f est un isomorphisme car :

- f est bijective ;
- $(P \oplus Q)(\beta) = P(\beta) + Q(\beta)$;
- Soit $P, Q \in \mathbb{F}_p[Q_\beta]$. $PQ = P * Q + DQ_\beta$ pour un certain D.
  Donc $(P * Q)(\beta) = P(\beta) * Q(\beta) + D(\beta) * Q_\beta(\beta) = P(\beta) * Q(\beta)$.

Vers une caractérisation des corps finis

Soit $\mathbb{F}_q$ un corps d'ordre q et p sa caractéristique.

Si β est un générateur de $\mathbb{F}_q^*$ alors $\mathbb{F}_p[\beta] = \mathbb{F}_q$. D'où :

Pour tout corps $\mathbb{F}$, il existe d tel que $\lvert\mathbb{F}\rvert = p^d$ avec p caractéristique de $\mathbb{F}$

Questions.

Deux corps $\mathbb{F}$ et $\mathbb{F}'$ tels que $\lvert\mathbb{F}\rvert = \lvert\mathbb{F}'\rvert$ sont-ils isomorphes ?

Pour tout p premier et $d \in \mathbb{N}^*$, existe-t-il un corps $\mathbb{F}$ avec $\lvert\mathbb{F}\rvert = p^d$?

Unicité de $\mathbb{F}_q$

Soit $Q \in \mathbb{F}_p[X]$, polynôme premier avec $1 < d = deg(Q)$ et $q = p^d$.

$|\mathbb{F}_p[Q]^*| = q - 1$. Donc tout élément β de $\mathbb{F}_p[Q]^*$ vérifie $\beta^{q-1} - 1 = 0$.

Soit $\beta = X$, $X^{q-1} - 1 = 0$ dans $\mathbb{F}_p[Q]$ et dans $\mathbb{F}_p[X]$: $\exists R\ X^{q-1} - 1 = QR$.

Donc Q divise $X^{q-1} - 1$.

Soit $\mathbb{F}_q$ un corps d'ordre q. D'après la factorisation de $X^{q-1} - 1$ dans $\mathbb{F}_q[X]$,

$Q = \prod_{i \leq d} X - \beta_i$ avec les $\beta_i \in \mathbb{F}_q^*$ tous distincts.

Pour tout i, $\mathbb{F}_p[\beta_i]$ est isomorphe à $\mathbb{F}_p[Q]$.

Puisque $|\mathbb{F}_p[Q]| = |\mathbb{F}_q|$, $\mathbb{F}_p[\beta_i] = \mathbb{F}_q$. D'où :

Pour tout p premier et $d \in \mathbb{N}$, il existe au plus un corps $\mathbb{F}$ avec $\lvert\mathbb{F}\rvert = p^d$

(à isomorphisme près)

De $\mathbb{F}_q[X]$ à $\mathbb{F}_p[X]$

Soit $\mathbb{F}_q$ un corps d'ordre $q = p^d$.

Soit $\alpha, \beta \in \mathbb{F}_q$.

$(\alpha + \beta)^p = \sum_{0 \leq i \leq p} \binom{p}{i} \alpha^i * \beta^{p-i} = \alpha^p + \beta^p$

$(\alpha - \beta)^p = \alpha^p + (-1)^p * \beta^p = \alpha^p - \beta^p$ car $(-1)^p = -1$ dans $\mathbb{F}_p$.

Par récurrence, pour tout n,

$$(\alpha + \beta)^{p^n} = \left((\alpha + \beta)^{p^{n-1}}\right)^p = \left(\alpha^{p^{n-1}} + \beta^{p^{n-1}}\right)^p = \alpha^{p^n} + \beta^{p^n}$$

Soit $Q = \sum_{i \leq n} q_i X^i \in \mathbb{F}_q[X]$, $Q^p = \sum_{i \leq n} q_i^p (X^p)^i$.

On rappelle que $\mathbb{F}_p = \{\beta \mid \beta \text{ racine de } X^p - X\}$.

$$\boxed{\text{Donc } Q^p = Q(X^p) \text{ ssi } Q \in \mathbb{F}_p[X]}$$

.

Racines d'un polynôme minimal

Soit $Q_\beta \in \mathbb{F}_p[X]$ un polynôme minimal de $\mathbb{F}_q$.
Alors $Q_\beta = \prod_{0 \leq i < n} X - \beta^{p^i}$ où n divise d. De plus Q_β divise $X^{p^n} - X$.

Preuve. $Q_\beta(\beta^p) = Q_\beta^p(\beta) = 0$.

Par récurrence, $\beta, \beta^p, \beta^{p^2}, \ldots, \beta^{p^d} = \beta$ sont des racines de Q_β.

Soit n le plus petit entier t.q. $\beta^{p^n} = \beta$. Si $\exists 1 \leq i < j < n$ tel que $\beta^{p^i} = \beta^{p^j}$.
Alors $\beta = \beta^{p^{n+i-j}}$ contredisant la définition de n.
Donc $|\{\beta^{p^i}\}_{0 \leq i < n}| = n$ et $deg(Q_\beta) \geq n$.
Ainsi $\beta^{p^k} = \beta$ ssi k est un multiple de n. Donc n divise d.

Soit $P = \prod_{0 \leq i < n} X - \beta^{p^i} \in \mathbb{F}_q[X]$.

$$P^p = \prod_{0 \leq i < n} (X - \beta^{p^i})^p = \prod_{0 \leq i < n} X^p - \beta^{p^{i+1}} = P(X^p)$$

Donc $P \in \mathbb{F}_p[X]$. Puisque $P(\beta) = 0$, Q_β divise P et aussi $X^{p^n} - X$.

Donc $n = deg(P) \leq deg(Q_\beta) \leq deg(P)$. D'où $deg(P) = deg(Q_\beta)$.

Puisque P est unitaire et Q_β est le polynôme minimal de P, $Q_\beta = P$.

Polynôme dérivé

Soit p premier et $P = \sum_{i \leq k} p_i X^i \in \mathbb{F}_p[X]$. $P' \equiv \sum_{i \leq k} (ip_i \mod p) X^{i-1}$.

Observation. $P' = 0$ si $\exists \ell \ k = \ell p$ et $P = \sum_{i \leq \ell} p_i X^{pi}$.

Dans ce cas, $P = \left(\sum_{i \leq \ell} p_i X^i \right)^p$.

Soit la factorisation de $P = p_k \prod_{j \leq m} R_j^{\alpha_j}$ avec pour tout j, $\alpha_j \geq 1$.

Alors $P' = p_k \sum_{j \leq m} (\alpha_j \mod p) R_j' R_j^{\alpha_j - 1} \prod_{j' \neq j} R_{j'}^{\alpha_{j'}}$.

Pour tout j, $\alpha_j > 1$ ssi R_j divise P'.

Preuve.

- Pour tout $k \neq j$, R_j divise le terme $(\alpha_k \mod p) R_k' R_k^{\alpha_k - 1} \prod_{j' \neq k} R_{j'}^{\alpha_{j'}}$.
- Si $\alpha_j > 1$, R_j divise le terme $(\alpha_j \mod p) R_j' R_j^{\alpha_j - 1} \prod_{j' \neq j} R_{j'}^{\alpha_{j'}}$.
- Si $\alpha_j = 1$, R_j ne divise pas le terme $R_j' \prod_{j' \neq j} R_{j'}^{\alpha_{j'}}$
  car $deg(R_j') < deg(R_j)$ et $R_j' \neq 0$ *(d'après l'observation ci-dessus)*.

Factorisation de $X^{p^d} - X$

Soit p premier et $d \geq 1$.

Soit $Q \in \mathbb{F}_p[X]$ un polynôme premier de degré n t.q. $d = kn$.

Soit $P \in \mathbb{F}_p[X]$. $P \bmod Q \in \mathbb{F}_p[Q]$ vérifie $P^{p^n} \bmod Q = P \bmod Q$.

$P^{p^{kn}} \bmod Q = (P^{p^{(k-1)n}})^{p^n} \bmod Q = P^{p^{(k-1)n}} \bmod Q = \cdots = P \bmod Q$.

Soit $P = X$, $X^{p^d} - X = 0 \bmod Q$. D'où :

Tout polynôme premier dont le degré divise d divise $X^{p^d} - X$.

$(X^{p^d} - X)' = -1$. D'où :

$X^{p^d} - X$ est le produit sans répétition
des polynômes premiers dont le degré divise d.

Existence de polynômes premiers

Soit $N(n)$ le nombre de polynômes premiers dans $\mathbb{F}_p[X]$ de degré n.

$N(1) = |\{X - \beta \mid \beta \in \mathbb{F}_p\}| = p$.

Puisque $X^{p^d} - X$ est le produit sans répétition des polynômes premiers dont le degré divise d. Pour tout $d \geq 1$, $p^d = \sum_{n|d} nN(n)$ (1)

$$p^{d/2}(p^{d/2} - d/2) \leq dN(d) \leq p^d$$

Pour tout $d \geq 1$, $N(d) > 0$.

Preuve.

D'après (1) $p^d \geq dN(d)$ et $p^d = dN(d) + \sum_{\substack{n<d \\ n|d}} nN(n) \leq dN(d) + (d/2)p^{d/2}$.

D'où $dN(d) \geq p^d - (d/2)p^{d/2} = p^{d/2}(p^{d/2} - d/2)$.

Si $d = 2$ et $p = 2$ alors $p^{d/2} - d/2 = 2 - 1 > 0$.

Puisque $p^{d/2} - d/2$ est croissante par rapport à p et d,

pour tout $d \geq 1$, $N(d) > 0$.

Test d'irréductibilité de Rabin

Un polynôme $P \in \mathbb{F}_p[X]$ de degré n est irréductible si et seulement si :

- P divise $X^{p^n} - X$;
- Pour tout $1 \leq m < n$ tel que $m|n$, P et $X^{p^m} - X$ sont premiers entre eux.

Preuve. Sans perte de généralité, on suppose P unitaire.

• Soit P premier.

Puisque $X^{p^n} - X$ est le produit des polynômes premiers
dont le degré divise n, P divise $X^{p^n} - X$.

Puisque $X^{p^m} - X$ est le produit des polynômes premiers
dont le degré divise $m < n$, P et $X^{p^m} - X$ sont premiers entre eux.

• Soit P satisfaisant le critère de Rabin.

Puisque P divise $X^{p^n} - X$, P est soit :

- un polynôme premier de degré n ;
- un produit de polynômes premiers Q t.q. $deg(Q)|n \wedge deg(Q) < n$.

Puisque pour tout $1 \leq m < n$ tel que $m|n$,
P et $X^{p^m} - X$ sont premiers entre eux, le deuxième cas est exclus.

Caractérisation des corps finis

Pour tout $q \in \mathbb{N}$, il y a un corps d'ordre q si et seulement si

$$q = p^d \text{ pour } p \text{ premier et } d \geq 1.$$

Ce corps est unique à isomorphisme près et il est isomorphe

au corps $\mathbb{F}_p[Q]$ pour tout $Q \in \mathbb{F}_p[X]$, polynôme premier de degré d.