# Corps finis

Tout sous-groupe fini du groupe multiplicatif d'un corps est cyclique.

$K^\times$ $\quad m$ entier $\geq 1$ $\quad \Phi_m(X) \in K[X]$

défini par récurrence sur $m$

$\Phi_1(X) = X - 1 \qquad X^m - 1 = \prod_{d|m} \Phi_d(X)$

degré $\Phi_d = \varphi(d) \qquad m = \sum_{d|m} \varphi(d)$



Si la caractéristique de $K$ est nulle $X^m - 1$ n'a pas de racine multiple

Si $K$ est de caractéristique finie $p$ on écrit $\quad m = p^r \cdot n \qquad p \nmid n$. $\quad r \geq 0$

$X^m - 1 = (X^n - 1)^{p^r}$ dans $K[X]$.

Comme $n \nmid p$, $X^n - 1$ n'a pas de racine multiple dans $K$

Sa dérivée $nX^{n-1}$ n'a pas de racine commune avec $X^n - 1$.



$n$ entier $\geq 1$ non divisible par la caractérisque de $K$ si cette caract. est $\neq 0$.

$X^n - 1 = \prod_{d|n} \Phi_d(X)$

Si $\alpha \in K$ vérifie $\alpha^n = 1$, alors $\alpha$ est racine d'un unique $\Phi_d(X)$, $d | n$.

Alors $\alpha^d - 1 = 0$ car $\Phi_d | X^d - 1$

$\alpha^{d'} - 1 \neq 0$ si $d' | d$, $d' \neq d$.

Donc $\alpha$ est d'ordre $d$ dans $K^\times$.



racines $n$-ièmes de l'unité dans $K$ : les $\alpha \in K$ tels que $\alpha^n = 1$

racines primitives $n$-ièmes de $1$ = les éléments d'ordre $n$ dans $K^\times$

$\alpha^n = 1$ et $\alpha^d \neq 1 \quad \forall d | n, \ d \neq n$

= les racines de $\Phi_n$ dans $K$.

$K$ corps $G$ sous-groupe de $K^\times$ d'ordre $m$. Tout $\alpha \in G$ vérifie $\alpha^m = 1$

$\alpha$ est racine de $X^m - 1$ dans $K[X]$.

$X^m - 1 = \prod_{d|m} \Phi_d(X) \qquad$ degré $\Phi_d = \varphi(d)$.

Pour $d / m$, $k_d$ le nombre de racines de $\Phi_d$ dans $K$. On a $k_d \le \varphi(d)$.

$$m = |G| \le \sum_{d/m} k_d \le \sum_{d/m} \varphi(d) = m$$

Donc $k_d = \varphi(d)$ pour tout $d/m$.

$\alpha_m \ge 1$. Donc $G$ contient un élément d'ordre $m$. $\Rightarrow$ $G$ est cyclique

De plus si $K$ est de caractéristique $p$ alors $p \nmid m$. Unique $G$ avec $|G|$ = racines de $X^m - 1$.



$K$ corps fini, $q = |K|$.

$p$ caractéristique. $\mathbb{Z} \longrightarrow K$

$n \mapsto \underbrace{1 + \dots + 1}_{n \text{ fois}}$, $n > 0$

$0 \longmapsto 0$

$-|n| \longmapsto \underbrace{-1-1\dots-1}_{|n| \text{ fois}}$

homomorphisme de groupes additifs

noyau idéal premier de $\mathbb{Z}$, $p\mathbb{Z}$.

$\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z} \hookrightarrow K$ $\quad r = [K : \mathbb{F}_p] < \infty$.

$\Rightarrow q = p^r$. $\quad K^\times$ groupe avec $q-1$ éléments

Tout $x \in K^\times$ vérifie $x^{q-1} = 1$



$K^\times$ est l'ensemble des racines du polynôme $X^{q-1} - 1$

cyclique. $\Phi_{q-1}(\alpha) = 0 \Rightarrow$

$K^\times = \{1, \alpha, \dots, \alpha^{q-2}\}$

$K$ est l'ensemble des racines de $X^q - X$

$F_p : K \longrightarrow K$ Frobenius. $\quad F_p(xy) = F_p(x) F_p(y)$

$x \longmapsto x^p$ $\quad F_p(x+y) = F_p(x) + F_p(y)$

homomorphisme injectif

$K$ fini $\Rightarrow$ bijection. Automorphisme de $K$.



$F_p(x) = x^p$ $\quad x \in K$.

$F_p \circ F_p(x) = F_p^2(x) = (x^p)^p = x^{p^2}$

$F_p^s(x) = x^{p^s}$. $\quad s \ge 1$.

$s < r$ $\exists \alpha \in K$

$F_p^s(\alpha) \ne \alpha$

$\alpha^{p^s} - \alpha \ne 0$

$X^{p^s} - X$

a $p^s$ racines

$q = p^r$ $\quad F_p^r(x) = x^{p^r} = x$ $\quad \forall x \in K$.

$F_p$ est un élément d'ordre $r$ dans

$\mathrm{Aut}(K) = \mathrm{Gal}(K/\mathbb{F}_p)$

$= \{1, F_p, F_p^2, \dots, F_p^{r-1}\}$

$K$

$| r$

$\mathbb{F}_p$

$K/\mathbb{F}_p$ est séparable.

Bijection diviseurs de $n = [K : \mathbb{F}_p]$
et les sous-corps de $K$

$n = d\delta$.

$$n\left(\begin{array}{l} K \\ \ \big| \Big) d \\ L \\ \ \big| \Big) \delta \\ \mathbb{F}_p \end{array}\right. \longrightarrow$$

sous-groupe d'ordre $d$
de $\{1, F_p, \dots, F_p^{n-1}\}$
$=$ s/g engendré par $F_p^\delta$
$= \{1, F_p^\delta, F_p^{2\delta}, \dots, F_p^{(d-1)\delta}\}$

$K/L$ Galoisienne

$|L| = p^\delta$ $\quad$ $\mathrm{Gal}(K/L)$ cyclique engendré par
$F_p^\delta : x \longmapsto x^{p^\delta}$.



Toute extension finie de corps finis est monogène. (fin de la démonstration du Théorème de l'élément primitif).

$$\begin{array}{c} K \\ | \\ L \\ | \\ \mathbb{F}_p \end{array}$$

$\alpha \in K^\times$ un générateur du groupe cyclique $K^\times$

$K = \mathbb{F}_p(\alpha) = L(\alpha)$

Étant donné $p$ premier $n \geq 1$
il existe un corps ayant $p^n$ éléments
unique à isomorphisme (non unique si $n \geq 2$) près.



$n \geq 1$

$\mathbb{F}_p[X] \ni X^{p^n} - X$

$K$ un corps de décomposition

$\{\alpha \in K, \alpha^{p^n} = \alpha\}$ est un corps
$\Rightarrow$ c'est $K$.

$K$ a $p^n$ éléments.

Dans une clôture algébrique $\overline{\mathbb{F}_p}$
pour tout $n \geq 1$ il y a un unique sous-corps
ayant $p^n$ éléments. $\mathbb{F}_{p^n}$.

$\mathrm{Aut}\,\mathbb{F}_{p^r} = \mathrm{Gal}(\mathbb{F}_{p^r}/\mathbb{F}_p) \neq (1)$

pour $r \geq 2$.

**Théorème.** $E$ corps à $q$ éléments. $K$ extension de $E$, $\alpha \in K$ algébrique sur $E$. Soit $r \geq 1$ le plus petit entier tel que $\alpha^{q^r} = \alpha$.

$$\begin{array}{l} K \ni \alpha \\ | \\ E \end{array}$$

Alors $\alpha$ est de degré $r$ sur $E$ et le polynôme irréductible de $\alpha$ sur $E$ est

$$(X-\alpha)(X-\alpha^q)(X-\alpha^{q^2})\cdots(X-\alpha^{q^{r-1}})$$



**Démonstrations.**

① Les conjugués de $\alpha$ sur $E$ sont les racines du polynôme irréductible de $\alpha$ sur $E$. Ce sont aussi les images de $\alpha$ par les isomorphismes de $E(\alpha)$ dans une extension normale.

Ce sont $\alpha, \alpha^q, \alpha^{q^2}, \dots, \alpha^{q^{r-1}}$.

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

② $[E(\alpha):E] = s$ $\qquad |E(\alpha)| = q^s$.

$m$ l'ordre de $\alpha$ dans $E(\alpha)^\times$ qui est d'ordre $q^s-1$. $\quad m \mid q^s-1$.



$|E(\alpha)^\times| = q^s - 1$.

$\alpha$ ordre $m$.

$\alpha^{q^s-1} = 1$.

$\alpha^{q^s} = \alpha$.

$\exists s \geq 1, \alpha^{q^s} = \alpha$.

$r$ est le plus petit.

$$\begin{array}{l} E(\alpha) \\ |\ s \\ E \end{array}$$

$f \in E[X]$ le polynôme irréductible de $\alpha$ sur $E$. degré $s$.

$f$ nul en $\alpha$, aussi en $\alpha^q$.

$f \in E[X]$ $\qquad f(X)^q = f(X^q)$

$|E| = q$

$f$ nul en $\alpha^{q^j}$ $\forall j \geq 0$

$$g(X) = \prod_{j=0}^{r-1} (X - \alpha^{q^j}) \in E[X].$$



$g(X)^q = g(X^q) \implies g(X) \in E[X]$.

$f \mid g \implies s = r,\ f = g$.

$s \geq r$

**Proposition.** Soit $E$ un corps fini à $q$ éléments. $r \geq 1$. Le polynôme $X^{q^r} - X$ est le produit de tous les polynômes irréductibles unitaires dont le degré divise $r$.

Exercice. $m, n$ entiers $> 0$  $K$ corps

$a$ entier $\geq 2$.

Propriétés équivalentes

(1) $m \mid n$

(2) $X^m - 1 \mid X^n - 1$ dans $K[X]$

(3) $a^m - 1 \mid a^n - 1$ dans $\mathbb{Z}$.

(1) $\Rightarrow$ (2)  $X^m = T$  $n = md$.

$T - 1 \mid T^d - 1$

(2) $\Rightarrow$ (3)

(3) $\Rightarrow$ (1)  $n = mq + r$

le reste de la division de $a^n - 1$ par $a^m - 1$ est $a^r - 1$.



$$X^{q^r} - X = X\left(X^{q^r - 1} - 1\right)$$

$f \in E[X]$ unitaire irréductible de degré $d$

$d / r$.

$$\begin{array}{c} E(\alpha) \\ \mid \\ E \end{array} \Big) \, d.$$

$E(\alpha)$ a $q^d$ éléments.

$$\alpha^{q^d} - \alpha = 0$$

$X^{q^r} - X$ est multiple de $f$.

$g \in E[X]$ un diviseur irréductible de $X^{q^r} - X \overset{?}{\Rightarrow} r \mid d$.  $\alpha$ racine de $g$ dans une extension $\bar{E}$

$\alpha^{q^r} = \alpha$  $\alpha \in$ s/corps de $\bar{E}$ ayant $q^r$ élts.



$$\begin{array}{c} \bar{E} \\ \mid \\ \mathbb{F}_{q^r} \\ \mid \\ E(\alpha) \\ \mid \\ E \end{array}$$

$d$.

$$X^{q^r} - X = \prod_{d/r} \prod_{P \in A_d} P$$

$A_d = \{$ polyn. irr. unit. deg. $d$, coeff. ds $E \}$

$\Rightarrow d / r$.

$|E(\alpha)| = q^d$.

Soit $\psi_q(d)$ = le nombre de polynômes irréductibles sur $\mathbb{F}_q$ unitaires degré $d$.

$$q^r = \sum_{d/r} d \, \psi_q(d).$$

Exercice

$$\frac{q^r}{2r} \leq \psi_q(r) \leq \frac{q^r}{r}.$$



$$\begin{array}{c} E \\ \mid \\ \mathbb{F}_p \end{array}$$

corps fini, au moins la moitié des éléments $\alpha$ de $E$ vérifient

$E = \mathbb{F}_p(\alpha)$

Théorie de Galois infinie.

Extension galoisienne = normale et séparable.

$\bar{\mathbb{F}}_p$ clôture algébrique

$$\begin{array}{c} \bar{\mathbb{F}}_p \\ \mid \\ \mathbb{F}_p \end{array} \Big)$$

infinie.  $\mathrm{Aut}(\bar{\mathbb{F}}_p) = \mathrm{Gal}(\bar{\mathbb{F}}_p / \mathbb{F}_p)$

isomorphe à

$$\hat{\mathbb{Z}} = \varprojlim_{n \to \infty} \mathbb{Z}/n\mathbb{Z}.$$

$\mathbb{Z}/m\mathbb{Z} \xrightarrow{s_{m,n}} \mathbb{Z}/n\mathbb{Z}$

$\cup$

$a_m$  $n / m$

$p$ premier $\quad \mathbb{Z}/p^m\mathbb{Z} \twoheadrightarrow \mathbb{Z}/p^n\mathbb{Z}$.

$\qquad\qquad \gamma_m \in \qquad n < m. \quad \ni \gamma_n.$

$$\mathbb{Z}_p = \varprojlim_{m\to\infty} \mathbb{Z}/p^m\mathbb{Z} \qquad \hat{\mathbb{Z}} = \prod_p \mathbb{Z}_p.$$

? $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$

Décomposition des polynômes cyclotomiques sur un corps fini.



Théorème. $K$ fini à $q$ éléments.
$n$ entier $\geq 1$ premier avec $q$.
Le polynôme cyclotomique $\Phi_n(X)$ se décompose dans $K[X]$ en facteurs irréductibles ayant tous le même degré $d$ qui est l'ordre de $q$ modulo $n$.

Dans un corps de décomposition soit $\alpha$ une racine d'un facteur irréductible $g$ de $\Phi_n$.
$\deg g = [K(\alpha):K] =$ le plus petit entier $r$ tel que $\alpha^{q^r} = \alpha$. $\quad \alpha^{q^r-1} = 1$



$\deg g =$ le plus petit entier $r$ tel que $\alpha^{q^r-1} = 1$

$\Phi_m(\alpha) = 0 \iff \alpha$ est d'ordre $m$ dans $K(\alpha)^\times$

$\alpha^{q^r-1} = 1 \iff m \mid q^r - 1$
$\iff q^r \equiv 1 \bmod m$.

Donc $\deg g =$ le + plus petit entier $r$ t.q. $q^r \equiv 1 \bmod m$
$=$ ordre de $q$ dans $(\mathbb{Z}/m\mathbb{Z})^\times$.