Anneaux et corps

1) Polynômes cyclotomiques

Définition. Soit $n \geq 1$.

On pose $\Phi_n(X) = \prod_{\substack{k=1 \\ k \wedge n}}^{n} \left(X - e^{\frac{2ik\pi}{n}}\right)$

ex $\Phi_1(X) = (X-1)$, $\Phi_2(X) = (X+1)$ $\Phi_3(X) = (X-j)(X-j^2)$ où $j = e^{\frac{2i\pi}{3}}$
$= X^2+X+1$

$\Phi_4(X) = (X-i)(X+i) = X^2+1$

Proposition 1) $\forall n \geq 1$, $\Phi_n(X) \in \mathbb{Z}[X]$, unitaire, de degré $\varphi(n)$

2) $\forall n \geq 1$, $\Phi_n(X)$ irréductible sur $\mathbb{Q}$.

démo 1) Comme $\left\{\frac{k}{n} : 1 \leq k \leq n\right\} = \bigsqcup_{d \mid n} \left\{\frac{k}{d} : 1 \leq k \leq d, k \wedge d = 1\right\}$

$$\prod_{k=1}^{n}\left(X - e^{\frac{2ik\pi}{n}}\right) = \boxed{X^n - 1 = \prod_{d \mid n} \Phi_d(X)} \quad (*)$$

[Rappel si $f : \mathbb{N} \to (G,+)$ (groupe abélien) alors $\forall n \geq 1$, $f(n) = \sum_{d \mid n} \mu\left(\frac{n}{d}\right) F(d)$

où $F(d) = \sum_{k \mid d} f(k)$ et $\mu(\ell) = \begin{cases} 1 & \text{si } \ell = 1 \\ (-1)^r & \text{si } \ell = p_1 \cdots p_r \text{ } p_i \text{ premiers distincts} \\ 0 & \text{sinon} \end{cases}$]

$(*) \Rightarrow \Phi_n(X) = \prod_{d \mid n} (X^d - 1)^{\mu\left(\frac{n}{d}\right)}$

or $\Phi_n(X) \in \mathbb{C}[X]$ et $\forall d$ $(X^d-1)^{\pm 1} \in \mathbb{Z}[[X]]$

$$\frac{1}{X^d - 1} = -\sum_{k=0}^{\infty} X^{kd}$$

donc $\Phi_n(X) \in \mathbb{C}[X] \cap \mathbb{Z}[[X]] = \mathbb{Z}[X]$.

ex! $\Phi_6(X) = \dfrac{(X^6-1)(X-1)}{(X^2-1)(X^3-1)} = X^3 - X^2 - 1$

2) $n = p$ premier $\Phi_p(X) = \dfrac{X^p - 1}{X-1} \Rightarrow \Phi_p(X+1) = \dfrac{(X+1)^p - 1}{X}$

$$= \frac{\sum_{k=0}^{p} \binom{p}{k} X^k - 1}{X} \quad (\text{et } p^2 \nmid p)$$

$$= \sum_{k=1}^{p} \binom{p}{k} X^{k-1}$$

← irréductible par Eisenstein ($\forall 1 \leq k \leq p-1$, $p \mid \binom{p}{k}$)

de même $\Phi_{p^\alpha}(X) = \Phi_p(X^{p^{\alpha-1}})$ irréductible sur $\mathbb{Q}$
(p premier)

Plus généralement (plus difficile), $\Phi_n(X)$ irréductible ($\forall n \geq 1$)

2) Corps finis

Théorème : 1) Si K corps fini, alors $|K| = p^\alpha$ pour un p premier et un $\alpha \in \mathbb{N}_{\geq 1}$. De plus $(K,+) \simeq \left((\mathbb{Z}/p\mathbb{Z})^\alpha, +\right)$

2) (existence et unicité) $\forall p$ premier, $\forall \alpha \geq 1$, il existe un corps fini de cardinal p^α. De plus si K_1, K_2 corps fini, si $|K_1| = |K_2|$, alors $K_1 \simeq K_2$ (isomorphisme de corps)

démo 1) car $(K|$ fini donc $\exists p$ premier, $p = \mathrm{car}(K)$.

Alors $\mathbb{Z}/p\mathbb{Z} \hookrightarrow K$ morphisme injectif de corps

$n \longmapsto \underbrace{1+\cdots+1}_{n \text{ fois}}$

donc K est un $\mathbb{Z}/p\mathbb{Z}$ – espace vectoriel de dimension finie

donc comme groupe $(K,+) \simeq \left((\mathbb{Z}/p\mathbb{Z})^\alpha, +\right)$ (choisir une base)

$\Rightarrow |K| = p^\alpha$.

$\mathbb{F}_2 = \mathbb{Z}/2\mathbb{Z}$

2) ex $K_1 = \mathbb{F}_2[X]/(X^3+X+1)$ corps de cardinal 8

$K_2 = \mathbb{F}_2[X]/(X^3+X^2+1)$ corps de cardinal 8

$K_1 \simeq K_2$ isomorphisme

$\overline{X} \longmapsto \overline{X+1}$

démo de l'existence

Lemme : Soit $\mathbb{F}_q$ corps de cardinal q

Dans $\mathbb{F}_q[X]$: $X^{q^n} - X = \prod_{d/n} \prod_{P \in I_d(q)} P$ (*)

($\forall n \geq 1$)

où $I_d(q) = \{$Polynômes unitaires de degré d sur $\mathbb{F}_q$ irréductibles$\}$

Admettons ce lemme :

$q = p$, $\mathbb{F}_q = \mathbb{Z}/p\mathbb{Z}$

$(*) \xrightarrow[\text{degrés}]{} q^n = \sum_{d|n} d\,|I_d(q)|$

$\Rightarrow n|I_n(q)| = \sum_{d|n} \mu\left(\frac{n}{d}\right) q^d$

$\Rightarrow |I_n(q)| = \frac{1}{n} \sum_{d|n} \mu\left(\frac{n}{d}\right) q^d$

$\Rightarrow |I_n(q)| \geq \frac{1}{n}\left(q^n - \sum_{1 \leq d < n} q^d\right) > \frac{1}{n}\left(q^n - \sum_{d=0}^{n-1} q^d\right)$

$= \frac{1}{n}\left(q^n - \frac{q^n - 1}{q-1}\right) \geq \frac{1}{n}\left(q^n - (q^n - 1)\right)$

$\geq \frac{1}{n} > 0$

$\Rightarrow |I_n(q)| > 0 \Rightarrow \exists P \in I_n(p)$

Alors $K = \mathbb{F}_p[X]/(P)$ est un corps de cardinal p^n.

démo du lemme : $X^{q^n} - X = \prod_{d|n} \prod_{P \in I_d(q)} P$

Soit $d|n$, soit $P \in I_d(q)$ alors $K = \mathbb{F}_q[X]/(P)$ corps de cardinal q^d

donc $\forall x \in K^*, x^{q^d - 1} = 1$

$\forall x \in K, x^{q^d} - x = 0$

En particulier si $x = X \bmod (P) = \overline{X}$, $\overline{X}^{q^d} = \overline{X}$ dans K

c-à-d : $X^{q^d} = X \bmod P$

c-à-d : $P \mid X^{q^d} - X$.

donc $P \mid X^{q^d} - X$

or $d|n \Rightarrow q^d - 1 \mid q^n - 1 = \left(q^d\right)^{\frac{n}{d}} - 1 = (q^d - 1)\left(1 + \cdots + q^{d\left(\frac{n}{d} - 1\right)}\right)$

$\Rightarrow X^{q^d - 1} - 1 \mid X^{q^n - 1} - 1$

$\Rightarrow X^{q^d} - X \mid X^{q^n} - X$

$\Rightarrow P \mid X^{q^n} - X$.

Réciproquement : Soit P irréductible sur $\mathbb{F}_q$ tq $P \mid X^{q^n} - X$.

soit $d = \deg P$. ALORS $|\mathbb{F}_q[X]/(P)| = q^d$

$\Rightarrow P \mid X^{q^d} - X$

si $d > 1$, $P \neq X \Rightarrow P \mid X^{q^d-1} - 1$

$\Rightarrow P \mid X^{q^d-1} - 1 \wedge X^{q^n-1} - 1$

On : si $a, b \geq 1$, $X^a - 1 \wedge X^b - 1 = X^{a \wedge b} - 1$

[en effet : si $a = bq + r$ division euclidienne

alors $X^a - 1 = X^{bq+r} - 1 = X^{bq+r} - X^r + X^r - 1$

$= X^r(X^{bq} - 1) + X^r - 1$

$= X^r(1 + X^b + \dots + X^{b(q-1)})(X^b - 1) + X^r - 1$

$\Rightarrow X^a - 1 \wedge X^b - 1 = X^b - 1 \wedge X^r - 1$

$= X^{b \wedge r} - 1 = X^{a \wedge b} - 1$]

(récurrence sur b)

$\deg P = d$, $P \mid \underbrace{X^{q^d-1} - 1 \wedge X^{q^n-1} - 1}$

$\Rightarrow P \mid X^{q^{d \wedge n}-1} - 1 = X^{q^{d \wedge n}} - 1$

donc $P \mid X^{q^{d \wedge n}} - X \Rightarrow$ dans $K = \mathbb{F}_q[X]/(P)$, $\overline{X}^{q^{d \wedge n}} = \overline{X}$

On $q = p^\alpha$ p premier, donc $\begin{array}{ccc} K & \longrightarrow & K \\ x & \longmapsto & x^q \end{array}$ automorphisme $\mathbb{F}_q$-linéaire de corps

donc $\{x \in K : x^{q^{d \wedge n}} = x\}$ sous-corps de K

qui contient $\mathbb{F}_q$ et $\overline{X}$ donc c'est K.

donc $\forall x \in K$, $x^{q^{d \wedge n}} = x \Rightarrow |K| \leq q^{d \wedge n} \Leftrightarrow q^d \leq q^{d \wedge n} \Rightarrow d = d \wedge n$

$\Rightarrow \underline{d \mid n}$.

Conclusion $X^{q^n} - X = \prod_{d \mid n} \prod_{P \in I_d(q)} P$ car dans $X^{q^n} - X$ pas de facteur carré.

(si $P^2 \mid X^{q^n} - X$ alors $P \mid (X^{q^n} - X)' = q^n X^{q^n-1} - 1$

$= -1$ absurde)

Remarque : $\boxed{|I_n(q)| = \frac{1}{n} \sum_{d \mid n} \mu\left(\frac{n}{d}\right) q^d}$

$\Rightarrow |I_3(2)| = \frac{1}{3}(2^3 - 2) = 2$

On a bien $I_3(2) = \{X^3+X+1 \ , \ X^3+X^2+1\}$

$|I_4(2)| = \frac{1}{4}(2^4 - 2^2) = 3$

on a bien $I_4(2) = \{X^4+X+1, X^4+X^3+1, X^4+X^3+X^2+X+1\}$

$(X^4+X^2+1) = (X^2+X+1)^2$.

Unicité Soit P_0 irréductible de degré n sur $\mathbb{F}_p$ $(I_n(p) \neq \emptyset)$
Soit K corps de cardinal p^n. ALORS $\mathbb{F}_p[X]/(P_0) \simeq K$.

En effet $\forall x \in K, \ x^{p^n} - x = 0$

donc $X^{p^n} - X = \prod_{x \in K} (X-x)$

On $P_0 \mid X^{p^n} - X$ donc P_0 est scindé sur K

donc $\exists x_0 \in K, \ P_0(x_0) = 0$

Donc $\mathbb{F}_p[X] \longrightarrow K$ morphisme d'anneaux
$R(X) \longmapsto R(x_0)$

Comme $P_0(x_0) = 0$ on obtient un morphisme d'anneaux :

$$\mathbb{F}_p[X]/(P_0) \xrightarrow{\varphi} K$$
$$R(X) \bmod P_0 \longmapsto R(x_0)$$

or $\mathbb{F}_p[X]/(P_0)$ corps donc φ injectif.

donc φ bijectif car $|\mathbb{F}_p[X]/(P_0)| = p^n = |K|$. □

Exercice : Soit $n \geq 1$, Soit $N = p^n - 1$.
Soit $P \in \mathbb{F}_p[X]$ facteur irréductible de $\Phi_N(X)$ (dans $\mathbb{F}_p[X]$)
alors $\deg P = n$ □

(Ex : $p=2, n=3$ $N = 2^3 - 1 = 7$, $\Phi_7(X) = \frac{X^7-1}{X-1} = X^6+X^5+X^4+X^3+X^2+X+1$

$\Phi_7(X)$ irréductible sur $\mathbb{Q}$ mais pas sur $\mathbb{F}_2$:

$\Phi_7(X) = (X^3+X+1)(X^3+X^2+1)$ dans $\mathbb{F}_2[X]$. □

Pause 5'