Anneaux & corps

1) Critère d'Eisenstein

Théorème

Soit A un anneau factoriel de corps des fractions K

(Par ex: $A=\mathbb{Z}$, $K=\mathbb{Q}$, $A=\mathbb{C}[X]$, $K=\mathbb{C}(X)$)

Soit $P(X)=a_nX^n+\dots+a_0 \in A[X]$, soit $p\in A$ irréductible tq

i) $p \nmid a_n$

ii) $\forall 0\le i\le n-1$, $p \mid a_i$

iii) $p^2 \nmid a_0$

ALORS $P(X)$ est irréductible sur K (dans $K[X]$)

démo. si $P(X)=Q(X)R(X)$ avec $Q(X), R(X) \in K[X]$, $\deg Q, \deg R>0$

soient $\alpha,\beta \in A\setminus\{0\}$ tq αQ , $\beta R \in A[X]$

Alors $\alpha\beta P = \alpha Q\, \beta R$ dans $A[X]$

(où $c(\lambda_0+\dots+\lambda_dX^d)=\text{pgcd}(\lambda_0,\dots,\lambda_d)$ si $\lambda_0,\dots,\lambda_d\in A$)

$\Rightarrow \alpha\beta\, c(P)=c(\alpha Q)\,c(\beta R)$

$\Rightarrow P=c(P)\underbrace{\frac{\alpha Q}{c(\alpha Q)}}_{Q_1}\underbrace{\frac{\beta R}{c(\beta R)}}_{R_1}$

$\Rightarrow P=Q_1R_1$ avec $Q_1, R_1\in A[X]$, $\deg Q_1=\deg Q>0$, $\deg R_1=\deg R>0$

$\Rightarrow \overline{P}=\overline{Q_1}\,\overline{R_1}$ dans $A/(p)[X]$ ($A/(p)$ intègre)

or $p\nmid a_n$, $\deg\overline{P}=\deg P$

de même $\deg\overline{Q_1}=\deg Q_1>0$, $\deg\overline{R_1}=\deg R_1>0$

or $\overline{P}=\overline{a_n}X^n$ dans $A/p[X]$

donc $\overline{a_n}X^n=\overline{Q_1}\,\overline{R_1} \Rightarrow \overline{Q_1}=\overline{b}X^d$, $\overline{R_1}=\overline{c}X^e$ où $d,e>0$

donc $Q_1=bX^d \bmod p$, $R_1=cX^e \bmod p$

$\Rightarrow p\mid Q_1(0)$, $p\mid R_1(0)$ dans A

$\Rightarrow p^2\mid Q_1(0)R_1(0)=P(0)=a_0$ absurde.

Donc P irréductible sur K.

Ex: a) $\forall n\ge 1$, X^n+2 est irréductible sur $\mathbb{Q}$. (Eisenstein avec $A=\mathbb{Z}$, $K=\mathbb{Q}$, $p=2$ $p\nmid 1$, $p\mid 2$ et $p^2=4\nmid 2$.)

b) $P(X,Y) = X^3 - Y^2 + 1 \in \mathbb{C}[X,Y] = \mathbb{C}[Y][X]$

$A = \mathbb{C}[Y]$, $p = Y-1$, $K = \mathbb{C}(Y)$.

Les coefficients de $P(X,Y)$ vu comme $P \in \mathbb{C}[Y][X]$ sont :

$a_3 = 1$, $a_2 = 0$, $a_1 = 0$, $a_0 = 1 - Y^2$

$p \mid a_0, a_1, a_2$, $p \nmid a_3$, $p^2 = (Y-1)^2 \nmid a_0$.

Eisenstein $\Rightarrow$ $P(X,Y)$ irréductible sur $\mathbb{C}(Y)$

$\Leftrightarrow$ irréductible sur $\mathbb{C}[Y]$ donc dans $\mathbb{C}[X,Y]$.

c) $\Phi_p(X) = X^{p-1} + X^{p-2} + \cdots + 1 = \dfrac{X^p - 1}{X-1} \in \mathbb{Z}[X]$, p premier

$$\Phi_p(X+1) = \frac{(X+1)^p - 1}{X} = \sum_{k=1}^{p} \binom{p}{k} X^{k-1} = p + \binom{p}{2} X + \cdots + \binom{p}{p-1} X^{p-2} + X^{p-1}$$

Or $\forall\, 1 \le k \le p-1$, $p \mid \binom{p}{k}$ $\Rightarrow$ (Eisenstein avec p) $\Phi_p(X+1)$ irréductible sur $\mathbb{Q}$.

$\Rightarrow$ $\Phi_p(X)$ irréductible sur $\mathbb{Q}$

(car $\mathbb{Q}[X] \to \mathbb{Q}[X]$, $f(X) \mapsto f(X+1)$ est un automorphisme d'anneaux)

exo : De même $\Phi_{p^k}(X) = \Phi_p(X^{p^{k-1}}) = 1 + X^{p^{k-1}} + \cdots + X^{p^{k-1}(p-1)}$ irréductible sur $\mathbb{Q}$.

2) Relations coefficients - racines.

Proposition : si $P(X) = a_n X^n + \cdots + a_0 = a_n (X - r_1) \cdots (X - r_n) \in K[X]$

(K corps, $a_i, r_i \in K$, $a_n \neq 0$)

Alors $\forall\, 0 \le k \le n$

$$\boxed{\frac{a_{n-k}}{a_n} = (-1)^k \sum_{1 \le i_1 < \cdots < i_k \le n} r_{i_1} \cdots r_{i_k}}$$

Ex : a) si $X^2 + pX + q = (X - r_1)(X - r_2)$ $\Rightarrow$ $(r_1 - r_2)^2 = (r_1 + r_2)^2 - 4 r_1 r_2$

$= p^2 - 4q$

b) (exo) $X^3 + pX + q = (X - r_1)(X - r_2)(X - r_3)$

$\Rightarrow (r_1 - r_2)^2 (r_2 - r_3)^2 (r_1 - r_3)^2 = -4p^3 - 27q^2$.

3) Corps de rupture, Corps de décomposition.

Définitions. a) Soit K corps. Soit $P(X) \in K[X]$ irréductible,

on dit que $K[X]/(P(X))$ est le corps de rupture de P

si $L = K(\alpha)$ avec $\alpha \in L$ et $P(\alpha) = 0$, on dit que L est un corps de rupture de P.

b) Soit K corps. Soit $P(X) \in K[X]$

On dit que $L \supset K$ est un corps de décomposition de P sur K si $P(X) = c(X-\alpha_1)\cdots(X-\alpha_m)$ avec $c \in K^*$, $\alpha_1, \dots, \alpha_m \in L$ et $L = K(\alpha_1, \dots, \alpha_m)$.

Proposition : a) Si $L = K(\alpha)$ corps de rupture de P sur K avec $P(X)$ irréductible sur K.

alors $K[X]/(P(X)) \simeq K(\alpha)$ isomorphisme de corps

$$r(X) \longmapsto r(\alpha)$$

b) Si $L = K(\alpha_1, \dots, \alpha_n)$ et $L' = K(\alpha'_1, \dots, \alpha'_n)$

sont des corps de décomposition de $P \in K[X]$ sur K.

alors $\exists\, \varphi : L \xrightarrow{\sim} L'$ isomorphisme K-linéaire de corps.

(admis)

ex : 1) $\mathbb{Q}(\sqrt[3]{2})$ est un corps de rupture de $X^3 - 2$ sur $\mathbb{Q}$.

2) $\mathbb{Q}(\sqrt[3]{2}, j\sqrt[3]{2}, j^2\sqrt[3]{2}) = \mathbb{Q}(j, \sqrt[3]{2})$ est un corps de décomposition de $X^3 - 2$ sur $\mathbb{Q}$. ($j = e^{2i\pi/3}$)

3) $\mathbb{Q}(e^{2i\pi/5})$ est un corps de décomposition de $X^5 - 1$ sur $\mathbb{Q}$

$\mathbb{Q}(1, e^{2i\pi/5}, e^{4i\pi/5}, e^{6i\pi/5}, e^{8i\pi/5})$.

4) Sous-groupes finis de K^*

Théorème : Soit K corps, Soit $G \leq K^*$ sous-groupe fini

alors G cyclique.

En particulier si K fini, alors K^* est cyclique.

ex : $(\mathbb{Z}/17\mathbb{Z})^* = \{\pm\bar{1}, \pm\bar{2}, \pm\bar{3}, \pm\bar{4}, \pm\bar{5}, \pm\bar{6}, \pm\bar{7}, \pm\bar{8}\}$

$= \langle \bar{3} \rangle$

(en effet :

$\bar{3}^2 = 9 = -8\ [17]$

$\bar{3}^4 = 64 = -4\ [17]$, $\bar{3}^8 = 16 = -1\ [17] \Rightarrow \bar{3}^{16} = 1\ [17]$

$\Rightarrow \bar{3}$ d'ordre 16 dans $(\mathbb{Z}/17\mathbb{Z})^*$ or $|(\mathbb{Z}/17\mathbb{Z})^*| = 16$ donc $\langle \bar{3} \rangle = (\mathbb{Z}/17\mathbb{Z})^*$.

Démo : Cas facile : si $K = \mathbb{C}$.

si $G \leq \mathbb{C}^*$ fini d'ordre n, alors $\forall g \in G$, $g^n = 1 \Rightarrow G \subseteq \mu_n = \{z \in \mathbb{C}^* : z^n = 1\}$

$\Rightarrow G \subseteq \langle e^{2i\pi/n} \rangle$

$\Rightarrow G = \langle e^{2i\pi/n} \rangle$ cyclique

cas général.

Soit $G \leq K^*$ sous-groupe fini d'ordre n

$\forall d|n$, soit N_d le nombre d'éléments d'ordre d dans G.

$\forall d|n$, si $N_d \neq 0$, il existe $x \in G$ d'ordre d.

Si y est un autre élément d'ordre d, alors

$$y^d = 1$$

Or $\forall z \in \langle x \rangle$, $z^d = 1$ donc l'équation $t^d = 1$ a pour solutions les éléments de $\langle x \rangle$. (au plus d solutions or $|\langle x \rangle| = d$)

donc si y d'ordre d, $y \in \langle x \rangle \Rightarrow y = x^k$, $1 \leq k \leq d$.

Or l'ordre de x^k est $\frac{d}{k \wedge d} = d \Rightarrow k \wedge d = 1$

Donc $N_d = |\{1 \leq k \leq d : k \wedge d = 1\}| = \varphi(d)$

Donc $\forall d|n$, $N_d = 0$ ou $\varphi(d)$.

Or $|G| = n \Rightarrow \sum_{d|n} N_d = n$

Or $\sum_{d|n} \varphi(d) = n$, $\forall d|n$, $N_d \leq \varphi(d)$

$\Rightarrow \forall d|n \quad N_d = \varphi(d)$.

$\Rightarrow N_n = \varphi(n) > 0 \Rightarrow \exists g \in G$ d'ordre n c-à-d $\langle g \rangle = G$.

□

5) Caractéristique d'un corps

~~$(\mathbb{Z},+) \longrightarrow (K,+)$~~

Soit K corps. L'application $\mathbb{Z} \longrightarrow K$ est un morphisme de ~~groupes~~ d'anneaux

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

de noyau $p\mathbb{Z}$ tq $\mathbb{Z}/p\mathbb{Z} \hookrightarrow K$ sous-anneau de K

donc $\mathbb{Z}/p\mathbb{Z}$ intègre donc p = premier ou 0

définition: Le nombre p est la caractéristique de K.

c-à-d : si $\forall n>0$, $\underbrace{1+\cdots+1}_{n \text{ fois}} \neq 0$, K est de caractéristique nulle

sinon K est de caractéristique p, p premier

et $p = \min\{\ell>0,\ \underbrace{1+\cdots+1}_{\ell \text{ fois}} = 0\}$.

ex : $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, $\mathbb{R}(X)$, etc sont de caractéristique nulle

$\mathbb{Z}/p\mathbb{Z}$, $\mathbb{Z}/p\mathbb{Z}(X)$ sont de caractéristique p (p premier)

$\mathbb{Z}[\sqrt{2}]/(3)$ est de caractéristique 3

6) Corps finis

Théorème : a) si K corps fini alors il existe p premier, $n \geq 1$ tq $|K| = p^n$

de plus $(K,+) \simeq \left((\mathbb{Z}/p\mathbb{Z})^n, +\right)$

b) $\forall p$ premier, $\forall n \geq 1$, $\exists$ K corps fini de cardinal p^n

de plus K unique à isomorphisme près

démo : a) K de caractéristique p premier car $\mathbb{Z} \xrightarrow{\varphi} K$ non injectif.

$1 \longmapsto 1$

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

donc $K > \varphi(\mathbb{Z}) \simeq \mathbb{Z}/p\mathbb{Z}$

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

Si on choisit $(e_1, \ldots, e_n)$ base de K comme $\mathbb{Z}/p\mathbb{Z}$-espace vectoriel,

alors $(\mathbb{Z}/p\mathbb{Z})^n \to K$ isomorphisme de groupes pour $+$

$(x_1, \ldots, x_n) \longmapsto x_1 e_1 + \cdots + x_n e_n$

⚠ à retenir, comme groupe, $(K,+) \simeq \left((\mathbb{Z}/p\mathbb{Z})^n, +\right) \neq \left(\mathbb{Z}/p^n\mathbb{Z}, +\right)$

ex : $\mathbb{F}_2[X]/(X^3+X+1) = K_1$ } sont des corps car X^3+X+1, X^3+X^2+1

$\mathbb{F}_2[X]/(X^3+X^2+1) = K_2$ } irréductibles sur $\mathbb{F}_2 = \mathbb{Z}/2\mathbb{Z}$

$|K_1| = |K_2| = 2^3 = 8$ (K_1 est un $\mathbb{F}_2$-ev de dimension 3)

$K_1 \longrightarrow K_2$

$x \longmapsto x+1$

c-à-d : $\mathbb{F}_2[X] \xrightarrow{\varphi} \mathbb{F}_2[X]/(X^3+X^2+1)$ morphisme d'anneaux surjectif

$r(X) \longmapsto r(X+1) \bmod X^3+X^2+1$

et de noyau ?

$\ker \phi = (X^3+X+1)$ car $\phi(X^3+X+1)$

$= (X+1)^3 + (X+1) + 1$

$= X^3 + 3X^2 + 3X + 1 + X + 1 + 1$

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

$= 0 \mod X^3 + X^2 + 1$.

donc $(X^3+X+1) \subset \ker \phi \Rightarrow (X^3+X+1) = \ker \phi$

donc ϕ induit $\overline{\phi} : K_1 = \mathbb{F}_2[X]/(X^3+X+1) \xrightarrow{\simeq} \mathbb{F}_2[X]/(X^3+X^2+1) = K_2$.

Pause = 5'