A anneau

$P \in A[X]$

$P \neq 0$

Comprendre $A[X]/\langle P\rangle$?

Division euclidienne (par P)

Si A n'est pas un corps, on a besoin que le coefficient dominant de P soit inversible dans A

Si A est un corps, c'est toujours vrai et on comprend très bien ($A = \mathbb{K}$) $\mathbb{K}[X]/\langle P\rangle$

(exemple $\mathbb{K} = \mathbb{Z}/p\mathbb{Z}$ p premier
$P \in \mathbb{K}[X]$ est irréductible)

Rappel Si A est un corps, tout idéal de $A[X]$ est de la forme $P.A[X]$ où $P \in A[X]$

Si A n'est pas un corps et P a son coefficient dominant inversible, la situation est similaire

Ex : $A[X]/\langle X-a\rangle \simeq A$
$a \in A$

$$\varphi : \begin{array}{ccc} A[X] & \longrightarrow & A \\ P & \longmapsto & P(a) \end{array}$$

$\mathrm{Ker}(\varphi) = (X-a).A[X]$

Ex : $\mathbb{Z}[X]/\langle 2X-1\rangle \not\simeq \mathbb{Z}$

Si A n'est pas un corps, il existe des idéaux de $A[X]$ qui ne sont pas engendrés par un seul élément

Ex (3.13) $\mathbb{Z}[X]/\langle n, X\rangle \xrightarrow{\sim} \mathbb{Z}/n\mathbb{Z}$

$n \in \mathbb{Z} \setminus \{0\}$

$$\varphi : \begin{array}{ccc} \mathbb{Z}[X] & \longrightarrow & \mathbb{Z}/n\mathbb{Z} \\ P & \longmapsto & [P(0)]_n \end{array}$$

$\mathrm{Ker}(\varphi) = \langle n, X\rangle$

Ex (3.13) $\quad \mathbb{Z}[X]/\langle m, X\rangle \xrightarrow{\sim} \mathbb{Z}/m\mathbb{Z}$

$m \in \mathbb{N}\setminus\{0,1\}$

$\langle m, X\rangle$ → n'est pas engendré par un seul élément sauf si $\begin{cases} m=0 \\ \text{ou} \\ m=1 \end{cases}$

$$\varphi : \mathbb{Z}[X] \longrightarrow \mathbb{Z}/m\mathbb{Z}$$
$$P \longmapsto [P(0)]_m$$

$\mathrm{Ker}(\varphi) = \langle m, X\rangle$

$\supset$ "facile" $\quad m \in \mathrm{Ker}(\varphi)$, $X \in \mathrm{Ker}(\varphi)$ donc $\underbrace{\langle m, X\rangle}_{\text{idéal engendré par } m \text{ et } X} \subset \underbrace{\mathrm{Ker}(\varphi)}_{\text{en particulier idéal}}$

$\subset$ "difficile"

Soit $P \in \mathbb{Z}[X]$ $\quad P = X.Q(X) + R(X)$ $\quad$ division euclidienne par X, $\deg(R(X)) \leq \deg(X) - 1 = 0$ donc $R(X) \in \mathbb{Z}$

$= \boxed{X.Q(X) + d}$ avec $d \in \mathbb{Z}$

en fait $d = P(0)$

$P = \sum_{i=0}^{D} a_i X^i \quad D \in \mathbb{N}, \ a_i \in \mathbb{Z}$

$= a_0 + \sum_{i=1}^{D} a_i X^i$

$= P(0) + X \underbrace{\sum_{i=0}^{D-1} a_{i+1} X^i}_{Q(X)}$

$= X.Q(X) + q\underbrace{m + n}_{\text{division euclidienne de } d = P(0) \text{ par } m}$ $\quad q, n \in \mathbb{Z}$ $\quad 0 \leq n \leq m-1$

$X.Q(X) + qm \in \langle X, m\rangle$

$[n]_m = [d]_m = [P(0)]_m$

$= (\text{un élément de } \langle X, m\rangle) + n$

$\boxed{\text{Si en outre } P \in \mathrm{Ker}(\varphi), \text{ on a } \underset{m \mid P(0)}{[P(0)]_m} = [0]_m}$ donc $[n]_m = [0]_m$ donc $n = 0$

donc $P \in \langle X, m\rangle$

$\mathbb{Z}[X,Y]/\langle X, Y\rangle \simeq \mathbb{Z}$ $\quad \varphi : \mathbb{Z}[X,Y] \longrightarrow \mathbb{Z}$
$$P(X,Y) \longmapsto P(0,0)$$
$$\mathrm{Ker}(\varphi) = \langle X, Y\rangle$$

A anneau $\quad$ Comprendre $A[X_1, \dots, X_m]/\langle P_1, \dots, P_n\rangle$ $\quad m, n \in \mathbb{N}\setminus\{0\}$

Même si A est un corps, c'est difficile

⚠ Si $P \in \mathbb{K}[X,Y]\setminus\{0\}$, la division euclidienne par P n'a pas de sens
($\mathbb{K}$ est un corps)

(bases de Gröbner)

On peut raisonner "variables par variables"

$P \in \mathbb{Z}[X,Y]$

$$P = \sum_{(i,j)\in\mathbb{N}^2} a_{i,j} X^i Y^j \qquad \{(i,j)\in\mathbb{N}^2,\ a_{i,j}\neq 0\} \text{ fini}$$

$$= \underset{\substack{\shortparallel \\ P(0,0)}}{a_{0,0}} + \underbrace{X \sum_{\substack{(i,j)\in\mathbb{N}^2 \\ i\geq 1}} a_{i,j} X^{i-1} Y^j + Y \sum_{\substack{(i,j)\in\mathbb{N}^2 \\ j\geq 1 \\ i=0}} a_{i,j} X^i Y^{j-1}}_{\in \langle X,Y\rangle}$$

$P = 1 + XY$

Donc si $P(0,0) = 0$ alors $P \in \langle X, Y\rangle$

Soit $P \in \mathbb{Z}[X,Y] = A[X]$ avec $A = \mathbb{Z}[Y]$

L'élément X, vu comme élément de $A[X]$, a pour coefficient dominant $1 \in A^\times$

$$A^\times = \mathbb{Z}[Y]^\times = \mathbb{Z}^\times$$

On écrit la division euclidienne de P par X dans $A[X]$

$P = X . Q_1 + R_1$ $\qquad Q_1, R_1 \in A[X] = \mathbb{Z}[X,Y]$

$\deg_X(R_1) < \deg_X(X) = 1$

donc $\deg_X(R_1) \leq 0$ c'est-à-dire $R_1 \in \mathbb{Z}[Y]$

soit $P = X . Q_1(X,Y) + R_1(Y)$ $\qquad Y \in \mathbb{Z}[Y]$ a un coefficient dominant inversible

$= X . Q_1(X,Y) + Y . Q_2(Y) + R_2(Y)$ avec $\deg_Y(R_2) \leq 0$

$Q_2(Y), R_2(Y) \in \mathbb{Z}[Y]$ c'est-à-dire $R_2 \in \mathbb{Z}$

soit $P = \underbrace{X . Q_1(X,Y) + Y . Q_2(Y)}_{\in\langle X,Y\rangle} + r$ $\qquad Q_1(X,Y) \in \mathbb{Z}[X,Y]$, $Q_2(Y) \in \mathbb{Z}[Y]$, $r \in \mathbb{Z}$

$P(0,0) = 0 . Q_1(0,0) + 0 . Q_2(0) + r$

donc $r = P(0,0)$

$$\begin{array}{ccc} \alpha & \mathbb{K}[X]/\langle P\rangle =: A \\ \uparrow & \uparrow \pi \\ X & \mathbb{K}[X] \end{array}$$

$\mathbb{K}$ corps

$P \in \mathbb{K}[X]$ de degré $d \in \mathbb{N}$

$\boxed{\{1, \alpha, \dots, \alpha^{d-1}\} \text{ base du } \mathbb{K}\text{-espace vectoriel } A}$

$\Updownarrow$ bijection (isomorphisme de $\mathbb{K}$-espaces vectoriels)

$$\boxed{\begin{array}{l} \mathbb{K}^d \longrightarrow A \\ (\beta_0, \dots, \beta_{d-1}) \longmapsto \sum_{i=0}^{d-1} \beta_i \cdot \alpha^i \\ \text{isomorphisme de } \mathbb{K}\text{-espaces vectoriels} \end{array}}$$

$\mathbb{K} = \mathbb{Z}/p\mathbb{Z}$ $\quad P \in \mathbb{K}[X]$ irréductible $\quad A = \mathbb{K}[X]/\langle P\rangle$ est un corps

$p = 3 \quad P = X^3 - X - 1$

$y \in A\setminus\{0\}$ ordre de y dans $A\setminus\{0\} = A^\times$?

$A = \{\beta_0 + \beta_1\alpha + \beta_2\alpha^2\}_{\beta_0, \beta_1, \beta_2 \in \mathbb{Z}/3\mathbb{Z}}$

$A\setminus\{0\} = \{\beta_0 + \beta_1\alpha + \beta_2\alpha^2\}_{\substack{\beta_0, \beta_1, \beta_2 \in \mathbb{Z}/3\mathbb{Z} \\ (\beta_0, \beta_1, \beta_2) \neq (0,0,0)}}$

$y_1 = 1 + \alpha + \alpha^2 \in A\setminus\{0\}$

$y_2 = \alpha^6 + 2\alpha^5 + \alpha^2 \in A \qquad y \in A\setminus\{0\}$?

$\pi : \mathbb{K}[X] \longrightarrow A = \mathbb{K}[X]/\langle P\rangle \qquad \alpha = \pi(X) \qquad P \in \mathrm{Ker}(\pi)$

donc $P(\alpha) = 0$

$$\begin{array}{ccc} Q & \longmapsto & Q(\alpha) \\ \| & & \| \\ \sum_{i=0}^{D} a_i \cdot X^i & & \sum_{i=0}^{D} a_i \cdot \alpha^i \end{array}$$

$a_i \in \mathbb{Z}$

$D \in \mathbb{N}$

structure de $\mathbb{K}$-algèbres sur A

$$P = X^3 - X - 1$$

$$0 = P(\alpha) = \alpha^3 - \alpha - 1$$

donc $\alpha^3 = \alpha + 1$

donc $\alpha^4 = \alpha \times \alpha^3 = \alpha(\alpha+1)$
$= \alpha^2 + \alpha$

donc $\alpha^5 = \alpha \times \alpha^4 = \alpha \times (\alpha^2 + \alpha)$
$= \alpha^3 + \alpha^2$
$= \alpha + 1 + \alpha^2$

donc $\alpha^6 = \alpha \times \alpha^5 = \alpha^2 + \alpha + \alpha^3$
$= \alpha^2 + \alpha + \alpha + 1$
$= \alpha^2 + 2\alpha + 1$

$$y_2 = \alpha^6 + 2\alpha^5 + \alpha^2$$
$$= (\alpha^2 + 2\alpha + 1) + (2 + 2\alpha + 2\alpha^2) + \alpha^2$$
$$= \alpha^2 + \alpha$$

donc $y_2 \neq 0$

$$y_2 = \pi(X^6 + 2X^5 + X^2)$$

$$X^6 + 2X^5 + X^2 = P.Q + R \qquad \deg(R) \leq \deg(P) - 1 = 2$$

$Q, R \in \mathbb{F}_3[X]$

Donc $y_2 = \pi(X^6 + 2X^5 + X^2) = \underbrace{\pi(P)}_{0} . \pi(Q) + \pi(R)$

$= \pi(R) \qquad R = \beta_0 + \beta_1 X + \beta_2 X^2 \quad \beta_0, \beta_1, \beta_2 \in \mathbb{F}_3$

$= \beta_0 + \beta_1 \alpha + \beta_2 \alpha^2 \qquad = X^2 + X$

$= \alpha^2 + \alpha \qquad$ donc $y_2 \neq 0$

Inverse de $y_2 = \alpha^2 + \alpha = \pi(X^2 + X)$

$$\text{pgcd}(X^2 + X, \underbrace{X^3 - X - 1}_{\text{irréductible}}) = 1$$

D'après Bézout (qui est effectif) il existe $Q_1, Q_2 \in \mathbb{F}_3[X]$
tels que $Q_1 . (X^2 + X) + Q_2 \times (X^3 - X - 1) = 1$

donc $\pi(\qquad) = \pi(1) = 1$

donc $\pi(Q_1) . \pi(X^2 + X) + \underbrace{\pi(Q_2) \times \underbrace{\pi(X^3 - X - 1)}_{=0}}_{=0} = 1$

donc $\underbrace{\pi(Q_1)}_{\text{inverse de } y \text{ dans } A} \times y = 1$