$(p=5,\ n=3)$

(exercice 3.11) $\mathbb{F}_5$

$P = X^3 + [2]_5 . X + [1]_5$

$Q = X^3 + X^2 + [1]_5$

$\mathbb{K}_1 = \mathbb{F}_5[X]/\langle P \rangle$ $\quad$ $\mathbb{K}_2 = \mathbb{F}_5[X]/\langle Q \rangle$

les corps $\mathbb{K}_1$ et $\mathbb{K}_2$ sont isomorphes $\left(\begin{matrix}\text{card}(\mathbb{K}_1) = 5^3 \\ \text{card}(\mathbb{K}_2) = 5^3\end{matrix}\right)$

$$\text{Hom}_{\text{anneaux}}(\mathbb{K}_1, \mathbb{K}_2) = \text{Hom}_{\text{anneaux}}(\mathbb{F}_5[X]/\langle P \rangle, \mathbb{K}_2)$$

$$= \left\{ \varphi \in \text{Hom}_{\text{anneaux}}(\mathbb{F}_5[X], \mathbb{K}_2),\ \text{Ker}(\varphi) \supset \langle P \rangle \right\}$$
$$\text{Ker}(\varphi) \ni P$$

Supposons avoir construit $\varphi \in \text{Hom}_{\text{anneaux}}(\mathbb{F}_5[X]/\langle P \rangle, \mathbb{K}_2)$

Alors φ est un isomorphisme (!)

($\text{Ker}(\varphi)$ est un idéal de $\mathbb{K}_1$, qui est un corps, donc $\text{Ker}(\varphi) = \{0\}$ ou $\text{Ker}(\varphi) = \mathbb{K}_1$, mais si $\text{Ker}(\varphi) = \mathbb{K}_1$, $1_{\mathbb{K}_2} = \varphi(1_{\mathbb{K}_1}) = 0_{\mathbb{K}_2}$ donc $\mathbb{K}_2$ est l'anneau nul, contradiction car $\mathbb{K}_2$ est un corps)

Donc $\text{Ker}(\varphi) = \{0\}$ donc φ est injectif

or $\text{card}(\mathbb{K}_1) = \text{card}(\mathbb{K}_2)$ donc φ est bijectif.

On cherche un élément de

$$\left\{ \varphi \in \text{Hom}_{(\text{anneaux})}(\mathbb{F}_5[X], \mathbb{K}_2),\ \text{Ker}(\varphi) \supset \langle P \rangle \right\}$$
$\mathbb{F}_5$-algèbres $\qquad$ $\text{Ker}(\varphi) \ni P$

$$\text{Hom}_{\mathbb{F}_5\text{-algèbres}}(\mathbb{F}_5[X], \mathbb{K}_2) \text{ « = » } \mathbb{K}_2$$
$$\varphi \qquad\qquad \varphi(X)$$
$$R \in \mathbb{F}_5[X] \mapsto R(\beta) \longleftarrow \beta$$

Soit $\varphi \in \text{Hom}_{\mathbb{F}_5\text{-algèbres}}(\mathbb{F}_5[X], \mathbb{K}_2)$. Soit $\beta := \varphi(X)$

$P \in \text{Ker}(\varphi) \iff P(\beta) = 0$

$\varphi(P) = P(\beta)$

Il suffit de trouver $\beta \in \mathbb{K}_2$ tel que $P(\beta) = 0$

On cherche un élément de

$$\{ \varphi \in \mathrm{Hom}_{\text{(anneaux)}\ \mathbb{F}_5\text{-algèbres}}(\mathbb{F}_5[X], \mathbb{K}_2),\ \ker(\varphi) \supset \langle P \rangle \}$$

$\ker(\varphi) \ni P$

$\mathrm{Hom}_{\mathbb{F}_5\text{-algèbres}}(\mathbb{F}_5[X], \mathbb{K}_2)$ « = » $\mathbb{K}_2$

$\varphi \quad \psi$

$\varphi(X)$

$(R \in \mathbb{F}_5[X] \mapsto R(\beta)) \longleftarrow \beta$

Soit $\varphi \in \mathrm{Hom}_{\mathbb{F}_5\text{-algèbres}}(\mathbb{F}_5[X], \mathbb{K}_2)$. Soit $\beta := \varphi(X)$

$P \in \ker(\varphi) \iff P(\beta) = 0$

$\varphi(P) = P(\beta)$

Il suffit de trouver $\beta \in \mathbb{K}_2$ tel que $P(\beta) = 0$

$$\mathbb{K}_2 = \mathbb{F}_5[X]/\langle Q \rangle \leftarrow \mathbb{F}_5[X] : \pi_Q \qquad \alpha_Q := \pi_Q(X)$$

ψ

$$\beta = \pi_Q\Big(\underbrace{\sum_{i=0}^{2} a_i \cdot X^i}_{R_\beta \in \mathbb{F}_5[X]}\Big) \qquad a_0, a_1, a_2 \in \mathbb{F}_5$$

$P(R_\beta) \in \mathbb{F}_5[X]$

on substitue R_β à X dans l'écriture de $P = X^3 + [2]_5 \cdot X + [4]_5$

$P(R_\beta) = R_\beta^3 + [2]_5 \cdot R_\beta + [4]_5$

On a $\pi_Q(P(R_\beta)) = P(\beta)$

Donc $P(\beta) = 0 \iff P(R_\beta) \in \ker(\pi_Q) \iff Q$ divise $P(R_\beta)$

SAGE montre que $\beta := [3]_5 \times \alpha_Q + [1]_5$ vérifie $P(\beta) = 0$

$\pi_P : \mathbb{F}_5[X] \longrightarrow \mathbb{F}_5[X]/\langle P \rangle \qquad \alpha_P := \pi_P(X)$

$\varphi : R \longmapsto R(\beta) = R([3]_5 \times \alpha_Q + [1]_5)$

$$\mathbb{F}_5[X] \xrightarrow{\pi_P} \mathbb{F}_5[X]/\langle P \rangle \longrightarrow \mathbb{F}_5[X]/\langle Q \rangle$$

$$\sum_{i=0}^{2} a_i \cdot \alpha_P^i \longmapsto \sum_{i=0}^{2} a_i \cdot ([3]_5 \alpha_Q + [1]_5)^i$$

$a_0, a_1, a_2 \in \mathbb{F}_5$

générateur de $\mathbb{K}_1^\times = \left(\mathbb{F}_5[X]/\langle P\rangle\right)^\times$?

$\mathrm{card}\,(\mathbb{K}_1^\times) = 5^3 - 1 = 124 = 4 \times 31$

Ordre de $\alpha_P = \pi_P(X)$? $\quad \pi_P(\alpha_P) = 0$

$\alpha_P^3 = [3]_5 X + [1]_5$

$\alpha_P^5 = \alpha_P^2 + [4]_5 \alpha_P + [3]_5$

$P = X^3 + [2]_5 \times X + [4]_5$

donc $0 = \alpha_P^3 + [2]_5 \times \alpha_P + [4]_5$

donc $\alpha_P^3 = -[2]_5 \alpha_P - [4]_5$

$= [3]_5 \alpha_P + [1]_5$

$\alpha_P^{4\times 31} = \alpha_P^{5^3-1} = 1$ (Lagrange)

$\forall \beta \in \mathbb{K}_1^\times, \ \beta^{5^3-1} = 1$

$\left(a_0, a_1, a_2 \in \mathbb{F}_5 \ / \ a_0 + a_1 \cdot \alpha_P + a_2 \cdot \alpha_P^2 = 1_{\mathbb{K}_1}\right.$

$\left. \Leftrightarrow \begin{cases} a_0 = [1]_5 \\ a_1 = a_2 = [0]_5 \end{cases}\right)$

$\alpha_P^{31} = 1$ donc l'ordre de α_P divise 31

donc l'ordre de α_P est égal à 31

(31 est premier et $\alpha_P \neq 1_{\mathbb{K}_1}$ donc l'ordre de α_P n'est pas 1)

Rq Si on trouve un élément d'ordre 4, on aura trouvé un élément d'ordre 4×31 (donc un générateur de $\mathbb{K}_1^\times$)

(Soit G un groupe ; $g_1 \in G$ d'ordre fini n_1

$g_2 \in G$ d'ordre fini n_2

tels que 1) $g_1 \times g_2 = g_2 \times g_1$ 2) $\mathrm{pgcd}(n_1, n_2) = 1$

alors $g_1 \times g_2$ est d'ordre $n_1 \times n_2$)

$\{\beta \in \mathbb{K}_1^\times, \ \beta^4 = 1_{\mathbb{K}_1}\} = \{a_0 + a_1 \times \alpha_P + a_2 \times \alpha_P^2, \ a_0, a_1, a_2 \in \mathbb{F}_5 \ / \ a_1 = a_2 = [0]_5, \ a_0 \neq [0]_5\}$

$= \{[1]_5, [2]_5, [3]_5, [4]_5\}$

$= \mathbb{F}_5^\times$ ($p=5$, $n=3$, $d=1$)

$\mathbb{F}_5 \subset \mathbb{K}_1 = \mathbb{F}_5[X]/\langle P\rangle$

$\boxed{\mathbb{F}_5^\times \subset \mathbb{K}_1^\times}$

($\mathbb{K}$ corps de cardinal p^n, d diviseur de n

$U := \{x \in \mathbb{K}^\times, \ x^{p^d-1} = 1\} \cup \{0\}$

est l'unique sous corps de $\mathbb{K}$ de cardinal p^d)

On prend un élément y de $\mathbb{F}_5^\times$ d'ordre 4

Alors $y \times \alpha_p$ est un élément de $K_1^\times$ d'ordre 4×31

Par exemple ($y = [4]_5 = [-1]_5$ $\quad y^2 = [1]_5$ ne marche pas)

$\mathrm{Card}(\mathbb{F}_5^\times) = 4$ $\quad y = [2]_5$ $\quad y^2 = [4]_5 \neq [1]_5$

($y \neq [1]_5$ $\quad y$ est d'ordre 2 ou 4)

Donc $[2]_5 \times \alpha_p$ est un générateur de $K_1^\times$

3.13 ① $\mathbb{Z}[X,Y]/\langle X,Y\rangle$ $\quad \langle X,Y\rangle = X\cdot\mathbb{Z}[X,Y] + Y\cdot\mathbb{Z}[X,Y]$

② $\mathbb{Z}[X]/\langle n, X\rangle$ $\quad n \in \mathbb{Z}$

① $P \in \mathbb{Z}[X,Y]$ $\quad P = \sum_{(n_1,n_2)\in\mathbb{N}^2} a_{n_1,n_2} X^{n_1} Y^{n_2}$ $\in \langle X,Y\rangle$?

oui si $\begin{cases} n_1 \geq 1 \\ \text{ou} \\ n_2 \geq 1 \end{cases}$

$a_{n_1,n_2} \in \mathbb{Z}$

$\{(n_1,n_2)\in\mathbb{N}^2,\ a_{n_1,n_2} \neq 0\}$ fini

$a_{5,3}\cdot X^5 Y^3 = X\cdot(\underbrace{a_{5,3} X^4 Y^3}_{\in\mathbb{Z}[X,Y]}) = Y\cdot(\underbrace{a_{5,3} X^5 Y^2}_{\in\mathbb{Z}[X,Y]})$ $\in \langle X,Y\rangle$

il reste ("modulo $\langle X,Y\rangle$") $\quad P$ "$=$" $a_{0,0} \in \mathbb{Z}$ $\quad P(0,0)$

$\mathbb{Z}[X,Y]/\langle X,Y\rangle \overset{?}{=} \mathbb{Z}$

On donne alors à construire $\varphi : \mathbb{Z}[X,Y] \to \mathbb{Z}$ $\begin{cases} \text{Surjectif} \\ \text{de noyau } \langle X,Y\rangle \end{cases}$

② $\mathbb{Z}[X]/\langle n,X\rangle$? $\quad P = a_0 + a_1 X + a_2 X^2 + \dots$ $\quad P \in \mathbb{Z}$

$= $ reste de la division euclidienne de a_0 par n

$\mathbb{Z}[X]/\langle n,X\rangle \overset{?}{=} \mathbb{Z}/n\mathbb{Z}$

$\varphi : \mathbb{Z}[X] \longrightarrow \mathbb{Z}/n\mathbb{Z}$, $P \longmapsto [P(0)]_n$ $\quad P(0)$

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