16/01/2025

TD2

Exercice 1

Soient $n \geq 1$, G un groupe et $f : (\mathbb{Z}/n\mathbb{Z}, +) \longrightarrow (G, *)$ un morphisme de groupe

(1) Montrons que f est complement determiné par $f(\bar{1})$

On sait que $\mathbb{Z}/n\mathbb{Z} = \langle \bar{1} \rangle$

et $f(\bar{k}) = f(k \cdot \bar{1})$
$= f(\underbrace{\bar{1} + \cdots + \bar{1}}_{k})$
$= \underbrace{f(\bar{1}) * \cdots * f(\bar{1})}_{k}$

$f(\bar{k}) = k\, f(\bar{1})$

2) Existe-t-il des elements d'ordre 3 dans $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$

* $(G, +)$ $x \in G$ $o(x)$ = le plus petit entier $n \geq 1$ tq $nx = 0$
* $(G, .)$, $x \in G$ $o(x) \neq x^n$

On a : $\mathbb{Z}/2\mathbb{Z} = \{\bar{0}, \bar{1}\}$
$\mathbb{Z}/4\mathbb{Z} = \{\hat{0}, \hat{1}, \hat{2}, \hat{3}\}$

$(\bar{x}, \hat{y})$	$(\bar{0}, \hat{0})$	$(\bar{0}, \hat{1})$	$(\bar{0}, \hat{2})$	$(\bar{0}, \hat{3})$	$(\bar{1}, \hat{0})$
$o(\bar{x}, \hat{y})$	1	4	2	4	2

$(\bar{1}, \hat{1})$	$(\bar{1}, \hat{2})$	$(\bar{1}, \hat{3})$
4	2	4

$(G, .)$, $(H, *)$
$(G \times H, \circ)$
$(x, y) \circ (a, b) = (x.a, y * b)$

$(\bar{1}, \hat{1}) + (\bar{1}, \hat{3}) = (\bar{1} + \bar{1}, \hat{1} + \hat{3})$
$= (\bar{2}, \hat{4})$
$= (\bar{0}, \hat{0})$

Supposons qu'il existe $(\bar{x}, \hat{y}) \in \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$ tq

$o((\bar{x}, \hat{y})) = 3$
$\Rightarrow |\langle (\bar{x}, \hat{y}) \rangle| \,/\, |\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}|$

$\Rightarrow 3 \,/\, 8$ impossible

donc on peut pas avoir d'élément d'ordre 3 dans $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$

Deduisons les morphisme de groupes de

$\mathbb{Z}/3\mathbb{Z} \longrightarrow \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$

Soit $\varphi : \mathbb{Z}/3\mathbb{Z} \longrightarrow \mathbb{Z}/2\mathbb{Z} / \mathbb{Z}/4\mathbb{Z}$

$\bar{a} \longmapsto (\bar{a}, \hat{a})$

on a le morphisme trivial

$f : \mathbb{Z}/3\mathbb{Z} \longrightarrow \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$

$\bar{1} \longmapsto (\bar{0}, \hat{0})$

Mq 3 pas de morphisme autre que le morphisme trivial.

Supposons qu'il existe
$\bar{1}$ tq $f(\bar{1}) = (\bar{x}, \hat{y}) \neq (\hat{0}, \hat{0})$

alors $3f(\bar{1}) = 3(\bar{x}, \hat{y})$
$\Rightarrow f(3.\bar{1}) = 3(\bar{x}, \hat{y})$
$f(\bar{0}) = 3(\bar{x}, \hat{y})$

$\Rightarrow (\bar{0}, \hat{0}) = 3(\bar{x}, \hat{y})$

$\Rightarrow o((\bar{x}, \hat{y})) \mid 3$

$\Rightarrow o((\bar{x}, \hat{y})) \in \{1, 3\}$

si $o((\bar{x}, \hat{y})) = 1 \Rightarrow (\bar{x}, \hat{y}) = (\bar{0}, \hat{0})$ absurde

si $o((\bar{x}, \hat{y})) = 3$ absurde
d'après la question precedante

3, $f : \mathbb{Z}/18\mathbb{Z} \longrightarrow \mathbb{Z}/15\mathbb{Z}$

$\bar{1} \longmapsto \hat{x}$

a, les ordres possibles de $f(\bar{1})$.

Comme $f(\bar{1}) \in \mathbb{Z}/15\mathbb{Z}$
alors
$o(f(\bar{1})) = \{1, 3, 5, 15\}$

b, reduisons les morphisme possible de f.

$f(\bar{1}) = \hat{x}$
$\Rightarrow 18(f(\bar{1})) = 18\hat{x}$
$\Rightarrow f(\bar{0}) = 18\hat{x}$
$\Rightarrow \hat{0} = 18.\hat{x}$
$\Rightarrow o(\hat{x}) = o(f(\bar{1})) \mid 18$

or $\begin{cases} o(f(\bar{1})) \mid 15 \\ o(f(\bar{1})) \mid 18 \end{cases}$

$o(f(\bar{1})) \in Div(15, 18)$

$o(f(\bar{1})) \in \{1, 3\}$

* $o(f(\bar{1})) = 1 \Rightarrow$ $f(\bar{1}) = \hat{0}$ et f est trivial

* $o(f(\bar{1})) = 3 \Rightarrow f(\bar{1}) \in \{\hat{5}, \hat{10}\}$

Il y a 3 morphisme

① $\bar{1} \longrightarrow \hat{0}$
$\bar{1} \longmapsto \hat{5}$
$\bar{1} \longmapsto \hat{10}$

4, $f : \mathbb{Z}/n\mathbb{Z} \longrightarrow \mathbb{Z}/m\mathbb{Z}$

a, Mq si $f(\bar{1}) = \hat{a}$ alors $\frac{m}{m \wedge m} \mid a$

Supposons que $f(\bar{1}) = \hat{a}$

$f(\bar{1}) = \hat{a}$
$\Rightarrow n f(\bar{1}) = n\hat{a}$
$\Rightarrow f(n.\bar{1}) = n\hat{a}$
$\Rightarrow \hat{0} = n\hat{a}$

$\hat{0} = n\hat{a}$

$\Rightarrow na \equiv a[m] \Rightarrow m \mid na$

$\exists k \in \mathbb{Z}$ tq $na = km$

mais $\exists \alpha, \beta \in \mathbb{Z}$ tq $\alpha \wedge \beta = 1$

$\begin{cases} n = \alpha \cdot n \wedge m \\ m = \beta \cdot n \wedge m \end{cases}$

~~$\Rightarrow 2a =$~~

$\Rightarrow \alpha \cdot n \wedge m \cdot a = k \cdot \beta \cdot n \wedge m$

$\Rightarrow \alpha a = k\beta$

$\Rightarrow \beta \mid \alpha a \Rightarrow \beta \mid a$ car $\beta \wedge \alpha = 1$ Gauss

$\Rightarrow \frac{m}{n \wedge m} \mid a$

b, Mq $\frac{m}{n \wedge m} \mid a$ alors il existe un unique morphisme

$f_a : \mathbb{Z}/n\mathbb{Z} \longrightarrow \mathbb{Z}/m\mathbb{Z}$ tel que

$f_m(\bar{1}) = \hat{a}$

c; Condition sur m, n pour qu'il existe un seul morphisme

$\mathbb{Z}/n\mathbb{Z} \longrightarrow \mathbb{Z}/m\mathbb{Z}$

Mq $n \wedge m = 1 \Rightarrow$ il existe un seul morphisme

$f(\bar{1}) = \hat{x}$ avec $\hat{x} \neq \hat{0}$

D'après la question a)

si $f(\bar{1}) = \hat{x} \Rightarrow \frac{m}{n \wedge m} \mid x$

$\Rightarrow m \mid x$

alors $\exists ! k \in \mathbb{Z} / x = mk$

$\Rightarrow \hat{x} = \hat{mk}$

$\Rightarrow \hat{x} = \hat{0}$ absurde

~~Absurde~~

Donc il faut nécessairement que $n \wedge m = 1$ pour qu'on ait un seul morphisme

d, le nombre

Exercice 2

1, Soit $(G,\cdot)$ un groupe fini noté multiplicativement

mq $f : (\mathbb{Q},+) \longrightarrow (G,\cdot)$ est un morphisme de groupes alors f est trivial

Supposons que f est un morphisme de groupes.
soit $x \in \mathbb{Q}$, alors $\exists (p,q) \in \mathbb{Z}\times\mathbb{N}^*$ tq $x = \frac{p}{q}$

Soit $n = |G|$, on sait $\forall y \in G,\ y^n = 1_G$

$f(\frac{p}{q}) \in G$

$f(\frac{p}{q}) = f(n\frac{p}{nq}) = f(\underbrace{\frac{p}{nq} + \dots + \frac{p}{nq}}_{n \text{ fois}})$

$f(n\frac{p}{nq}) = \underbrace{f(\frac{p}{nq}) \cdot f(\frac{p}{nq}) \dots f(\frac{p}{nq})}_{n \text{ fois}}$

$= \left(f(\frac{p}{nq})\right)^n$

$= 1_G$

Donc $\forall x \in \mathbb{Q}$, on a $f(x) = 1_G$ et par suite f est trivial

2, $f : G \longrightarrow G$, $x \longmapsto x^d$

a, Mq f est un endomorphisme

soient $x, y \in G$, on a
$f(xy) = (xy)^d$
$= \underbrace{(xy)\cdot(xy)\cdot\dots\cdot(xy)}_{d \text{ fois}}$
$= x^d y^d$ car G est abelien
et par suite f est un morphisme car morphisme de G dans G

b, Mq $n \wedge d = 1$ alors f est automorphisme
Mq $\ker(f) = \{1_G\}$

soit $x \in G$ tq $f(x) = 1_G$
$f(x) = 1_G$
$\Rightarrow x^d = 1_G$
$\rightarrow o(x) \mid d$ or $o(x) \mid n$ d'après Lagrange

et par suite $o(x) \mid n \wedge d = 1$

$\Rightarrow o(x) \mid 1 \Rightarrow o(x) = 1$
$\Rightarrow x = 1_G$

donc $\ker(f) = \{1_G\}$ et par conséquent f est bijective
$|G|$ fini.

C, supposons n est impair

n impair $\Rightarrow \exists k \in \mathbb{N}$ tq

$n = 2k+1$

soit $x \in G$, alors $x^n = 1_G$

$x^n = 1_G \Rightarrow x^{2k+1} = 1_G$

$\Rightarrow x^{2k} x = 1_G$

$\Rightarrow x = x^{-2k}$

$= (x^{-k})^2$

puis que $x^{-k} \in G$,

donc x est un carré dans G

$f : G \longrightarrow G$

$x \longmapsto x^2$

n impair $\rightarrow n \wedge 2 = 1$

$\Rightarrow f$ autom

$\Rightarrow$ surjectif

$\Rightarrow y \in G \Rightarrow \exists x \in G$ tq

$y = x^2$

3, soit $C = (i, j, k)$ un cycle de S_n et $\sigma \in S_n$

Calculons

$\sigma \circ C \circ \sigma^{-1}$

soit $x = \{1, 2, 3, 4\}$

$\sigma \circ C \circ \sigma^{-1}(x) = \sigma(C(\sigma^{-1}(x)))$

1er Cas $\sigma^{-1}(x) \in \{i, j, k\}$

$\Rightarrow x \in \{\sigma(i), \sigma(j), \sigma(k)\}$

$C(\sigma^{-1}(x)) \in \{i, j, k\}$

$\sigma \circ C \circ \sigma^{-1}(x) \in \{\sigma(i), \sigma(j), \sigma(k)\}$

2ème Cas $\sigma^{-1}(x) \notin \{i, j, k\}$

$\Leftrightarrow x \notin \{\sigma(i), \sigma(j), \sigma(k)\}$

Alors $C(\sigma^{-1}(x)) = \sigma^{-1}(x)$

en outre

$\sigma \circ C \circ \sigma^{-1}(x) = \sigma \circ \sigma^{-1}(x) = x$

$\sigma \circ C \circ \sigma^{-1} = (\sigma(i), \sigma(j), \sigma(k))$

Exercice 3

$[x, y] = x^{-1} y^{-1} x y$

1, Mq $[G, G] \triangleleft G$

Soit $g \in G$

Mq $g^{-1} [G, G] g \subset [G, G]$

Soit $y \in g \cdot [G, G] g^{-1}$. Alors

$\exists x, z \in G$ tq

$y = g x^{-1} z^{-1} x z g^{-1}$

$g[x, z] g^{-1} = [gxg^{-1}, gzg^{-1}]$.

(1)

(1) $g x^{-1} z^{-1} x z g^{-1}$

(2) $(gxg^{-1})^{-1} (gzg^{-1})^{-1} (gxg^{-1}) (gzg^{-1})$

$g x^{-1} g^{-1} g z^{-1} g^{-1} g x g^{-1} g z g^{-1}$

$g x^{-1} z^{-1} x z g^{-1}$

donc $[G,G] \triangle G$ évidente

2) déterminons $[G,G]$ puis

$G/[G,G]$ si G est commutatif.

soient x, y
$x^{-1}y^{-1}xy = x^{-1}xy^{-1}y$
$= 1_G$

donc $[G,G] = \{1_G\}$ et donc

$G/[G,G] = G$

$H \trianglelefteq G$

G/H groupe $\quad xRy \Rightarrow x^{-1}y \in H$

$G/\{1\} \Rightarrow xRy \in x^{-1}y \in \{1\}$

$\in x = y$

$G/H = \{\bar{x},\ x \in G\}$

$G/\{1\} = \{\bar{x},\ x \in G\}$

$= \{\{x\},\ x \in G\}$

$= G$

3) mq $G/[G,G]$ est commutatif

$G/[G,G] = \{\bar{g} = g.[G,G],\ g \in G\}$

$H \triangle G \Rightarrow G/H$ groupe

$\bar{x} = x.H = \{x.h,\ h \in H\}$

$[G,G] \triangleleft G \Rightarrow G/[G,G]$ groupe

$\bar{g} = g.[G,G] = \{g.[x,y], x,y \in G\}$

$\bar{g_1}.\bar{g_2} = \bar{g_2}.\bar{g_1}$

$\overline{g_1 g_2} \overset{?}{=} \overline{g_2 g_1}$

$(g_1 g_2)^{-1}(g_2 g_1) \in [G,G]$

$g_2^{-1} g_1^{-1} g_2 g_1$

$[g_2, g_1]$

$g_2^{-1} g_1^{-1} g_2 g_1 = [g_2, g_1] \in [G,G]$

$\Rightarrow (g_1 g_2)^{-1}(g_2 g_1) \in [G,G]$

$\Rightarrow \overline{g_1 g_2} = \overline{g_2 g_1}$

$\Rightarrow \bar{g_1}.\bar{g_2} = \bar{g_2}.\bar{g_1}$

$\bar{x}.\bar{y} = \bar{y}.\bar{x}$
$\overline{xy} = \overline{yx}$
$(xy)^{-1} yx \in H$

Exercice 5 [10pt]

1) $S_n \times \mathbb{K}[X_1, X_2, \dots, X_n] \to \mathbb{K}[X_1, \dots, X_n]$

$(\sigma, P(X_1, \dots, X_n)) \longmapsto P(X_{\sigma(1)}, \dots, X_{\sigma(n)})$

1) Montrons que l'application ainsi définie est une action de groupe.

Soient $\sigma, \alpha \in S_n$ et $P \in \mathbb{K}[X_1, \dots, X_n]$

- $(\sigma \circ \alpha) \cdot P(X_1, \dots, X_n) = P(X_{\sigma\circ\alpha(1)}, \dots, X_{\sigma\circ\alpha(n)})$

$\sigma \cdot (\alpha \cdot P(X_1, \dots, X_n)) = \sigma \cdot$

déterminons l'orbite du polynôme $\prod_{1 \le i < j \le n} (X_i - X_j)$

Posons $P(X_1, \dots, X_n) = \prod_{1 \le i < j \le n} (X_i - X_j)$

$S_n \cdot P = \{ \sigma \cdot P(X_1, \dots, X_n) \mid \sigma \in S_n \}$

$P(X_1, X_2, X_3) = \prod_{1 \le i < j \le 3} (X_i - X_j)$

$= (X_1 - X_2)(X_1 - X_3)(X_2 - X_3)$

$Id \cdot P(X_1, X_2, X_3) = P(X_1, X_2, X_3)$

$(12) \cdot P(X_1, X_2, X_3) = (X_2 - X_3)(X_2 - X_1)(X_3 - X_1) = P(X_1, X_2, X_3)$

$(23) \cdot P(X_1, X_2, X_3) = (X_1 - X_3)(X_1 - X_2)(X_3 - X_2) = -P(X_1, X_2, X_3)$

$S_3 \cdot P = \{ \pm P \}$

$P = \prod_{1 \le i < j \le n} (X_i - X_j)$

$\Rightarrow \sigma \cdot P = \prod_{1 \le i < j \le n} (X_{\sigma(i)} - X_{\sigma(j)})$

$= (-1)^{I(\sigma)} P$

où $I(\sigma)$ = nbre d'inversion de σ

/ couple (i,j) avec $i<j$ $\sigma(i) > \sigma(j)$

$\Rightarrow \sigma \cdot P = \varepsilon(\sigma) P \in \{ \pm P \}$

$\Rightarrow S_n \cdot P \subset \{ \pm P \}$

$P \in S_n \cdot P$ car $P = id_{[\![1,n]\!]} \cdot P$

$-P \in S_n \cdot P$ car $-P = (12) \cdot P$

$\Rightarrow \{ \pm P \} \subset S_n \cdot P$

Par suite $S_n \cdot P = \{ \pm P \}$

Ex) $\gamma : G \longrightarrow Aut(G)$

$g \longmapsto \gamma(g)$

$G \longrightarrow G$

$x \longmapsto \gamma(g)(x) = g x g^{-1}$

a, Déterminons $\ker \gamma$.

$\ker \gamma = \{g \in G / \gamma(g) = id_G\}$

$= \{g \in G / \gamma(g)(x) = x \ \forall x \in G\}$

$= \{g \in G / gx = xg, \ \forall x \in G\}$

$= Z(G)$

$\boxed{\ker \gamma = Z(G)}$

b, rq $Int(G) = Im(\gamma)$

rq $Int(G) \lhd Aut(G)$

$Int(G) = \{\gamma(g) / g \in G\} \subset Aut(G)$

Soit $\varphi \in Aut(G)$. Montrons que $\varphi Int(G) \varphi^{-1} \subset Int(G)$

$\varphi \circ \gamma(g) \circ \varphi^{-1} \in Int(G), \ \forall \gamma(g) \in Int(G)$?

$\varphi \circ \gamma(g) \circ \varphi^{-1}(x) = \varphi \circ \gamma(g)(\varphi^{-1}(x))$

$= \varphi(g \varphi^{-1}(x) g^{-1})$

$= \varphi(g) \varphi(\varphi^{-1}(x)) \varphi(g^{-1})$

$= \varphi(g) x (\varphi(g))^{-1}$

$= \gamma(\varphi(g))(x), \ \forall x \in G$

Par suite, $\varphi \circ \gamma(g) \circ \varphi^{-1} = \gamma(\varphi(g)) \in Int(G)$

Donc $Int(G) \lhd Aut(G)$

c, calculons $Aut(S_3)$ et $Int(S_3)$

$G = S_3$

$$\begin{array}{ccc} S_3 & \xrightarrow{\ \gamma\ } & Aut(S_3) \\ \pi \downarrow & \overline{\gamma} \nearrow & \uparrow i \\ S_3/\ker(\gamma) & \xrightarrow{\sim} & Im(\gamma) \end{array}$$

$S_3/Z(S_3) = Int(S_3)$

Déterminons $Z(S_3)$

$Z(S_3) = \{\sigma \in S_3 / \sigma \circ x = x \circ \sigma \ \forall x \in S_3\}$

$|Z(S_3)| \in \{1, 2, 3, 6\}$

on peut passer par le tableau manuel

$(12) \circ (23) = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = (123)$

$(23) \circ (12) = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$

$(12) \circ (23) \neq (23) \circ (12)$

$S_3 = \{id, (12), (13), (23), (123), (132)\}$

• $|Z(S_3)| = 6$

$|Z(S_3)| = 6 \Rightarrow S_3 = Z(S_3)$

$\Rightarrow (S_3, \circ)$ commutatif, ce qui est absurde.

• $|Z(S_3)| = 3$

$|Z(S_3)| = 3 \Rightarrow \left|S_3 / Z(S_3)\right| = 2$

$\Rightarrow \dfrac{S_3}{Z(S_3)}$ est cyclique

$\Rightarrow (S_3, \circ)$ est commutatif, ce qui est absurde.

• $|Z(S_3)| = 2$

$|Z(S_3)| = 2 \Rightarrow \left|S_3 / Z(S_3)\right| = 3$

$\Rightarrow \dfrac{S_3}{Z(S_3)}$ est cyclique

$\Rightarrow (S_3, \circ)$ est commutatif, ce qui est absurde

Donc $|Z(S_3)| = 1$ et par conséquent $Z(S_3) = \{id_{[1,3]}\}$

$\Rightarrow Int(S_3) \cong \dfrac{S_3}{Z(S_3)} \cong \dfrac{S_3}{\{id\}} \cong S_3$

$Aut(S_3) = \{\varphi : S_3 \to S_3 / \varphi \text{ aut}\}$

$\forall \varphi \quad S_3 = \langle \alpha = (12), \beta = (123) \rangle$

$|\langle \alpha, \beta \rangle| \, | \, |S_3| = 6$

$|\langle \alpha, \beta \rangle| \in \{1, 2, 3, 6\}$

De plus $id, \alpha, \beta, \beta^2 = (132) \in \langle \alpha, \beta \rangle$

$\Rightarrow |\langle \alpha, \beta \rangle| \geq 4$

$\Rightarrow \langle \alpha, \beta \rangle = 6$

Un auto de S_3 sera déterminé par $f(\alpha)$ et $f(\beta)$

3 possibilités : $(12), (13), (23)$

2 possibilités : $(123), (132)$

$f : G \longrightarrow G$ auto (morphisme bijectif)

$\Rightarrow o(f(x)) = o(x)$

$(f(x))^{o(f(x))} = e$

$\Rightarrow f(x^{o(f(x))}) = e$

$\Rightarrow x^{o(f(x))} \in \ker f = \{e\}$ car f injective

$\Rightarrow x^{o(f(x))} = e$

$\Rightarrow o(x) \mid o(f(x))$

$\Rightarrow o(x) \leq o(f(x))$

~~$\Rightarrow (f(x) = 0)$~~

$x^{o(x)} = e$

$\Rightarrow f(x^{o(x)}) = e$

$\Rightarrow (f(x))^{o(x)} = e$

$\Rightarrow o(f(x)) \mid o(x)$

$\Rightarrow o(f(x)) \leq o(x)$

~~Donc~~ $o(f(x)) = o(x)$

Par suite

$|Aut(S_3)| = 6$

$$\begin{array}{ccc} S_3 & \xrightarrow{\varphi} & Aut(S_3) \\ \downarrow & \overset{\sim}{\searrow} & \uparrow i \\ & \xrightarrow{\sim} & Im\varphi = Int(S_3) \end{array}$$

$S_3 / Ker\varphi = Z(S_3) = \{id\}$

$|Int S_3| = |S_3| = 6 = |Aut S_3|$

Par suite $Aut(S_3) = Int(S_3) \overset{\sim}{=} S_3$

Exercice

(1) Si $\sigma \in S_n$ on pose $P_\sigma = (P_{ij})$ avec $P_{ij} = \delta_{i\sigma(j)}$. Vérifions que l'ensemble $\mathcal{P}$ des matrices de cette forme (i.e matrices de permutations) est un groupe isomorphe à S_n

$\sigma \mapsto P_\sigma = (P_{ij} = \delta_{i\sigma(j)}) \in M_n(\mathbb{K})$

$(1\,2\,3) \in S_3$

$$P_{(1\,2\,3)} = \begin{pmatrix} \delta_{1\sigma(1)} & \delta_{1\sigma(2)} & \delta_{1\sigma(3)} \\ \delta_{2\sigma(1)} & \delta_{2\sigma(2)} & \delta_{2\sigma(3)} \\ \delta_{3\sigma(1)} & \delta_{3\sigma(2)} & \delta_{3\sigma(3)} \end{pmatrix}$$

$$= \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}$$

on a $I_3 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$

On remarque que la $P_{(1\,2\,3)}$ est la permutation $(1\,2\,3)$ des lignes de I_3

$P_\sigma \times P_2 = ?$ $\forall \sigma \in S_n$

$= (a_{ij}) \times P_\alpha (b_{jk}) \in M_n(\mathbb{K})$

$c_{ik} = \sum_{j=1}^{n} a_{ij} b_{jk}$

$= \sum_{j=1}^{n} \delta_{i\sigma(j)} \times \delta_{j\alpha(k)}$

$\begin{cases} i = \sigma(j) \\ j = \alpha(k) \end{cases} \Rightarrow i = \sigma(\alpha(k)) = \sigma \circ \alpha(k)$

Donc si $i = \sigma \circ \alpha(k)$ alors $c_{ik} = 1$

si $i \neq \sigma \circ \alpha(k)$ alors $i \neq \sigma(j)$ ou $j \neq \alpha(k) \Rightarrow \delta_{i\sigma(j)} = 0$ ou $\delta_{j\alpha(k)} = 0$

$\Rightarrow c_{ik} = 0$

En suite $c_{ik} = \delta_{i\,\sigma\circ\alpha(k)}$

$\Rightarrow P_\sigma \times P_\alpha = P_{\sigma\circ\alpha}$

$P_\sigma \times P_{\sigma^{-1}} = P_{\sigma\circ\sigma^{-1}} = P_{id_{[\![1,n]\!]}}$

$= (\delta_{id(ij)}) \in M_n(\mathbb{K})$

$= \delta_{ij} = I_n$

$P_\sigma \in GL_n(\mathbb{K})$

$(P_\sigma)^{-1} = P_{\sigma^{-1}}$

TD3

Exercice 2

~~(1) Soit p un nombre premier~~
~~$p \to n$~~
~~$H \subset G$~~

1, Soit G un groupe avec $|G| = 200 = 5 \times 40$

a) le nombre de 5-sylow de G et 40 2-sylow

Soit n_5 le nombre de 5-sylow n_{40} celui de 2-sylow

D'après le 3ème théorème de sylow, on a :

$n_5 \equiv 1 [5]$ et $n_5 | 40$

$n_5 \in \{1, 40\}$

* $n_{40} \equiv 1 [40]$ et $n_{40} | 5$ $\quad n_{40} = 1$

b, on suppose qu'il existe un unique 5-sylow noté H_5 et un unique 40-sylow

Ainsi, ces deux (02) sous-groupes sont cyclique

$|H_5| = 5$ qui est un nombre premier donc H_5 est cyclique et $|H_{40}| = 40$ qui est premier donc H_{40} est cyclique.

(ii) En notant x un generateur de H_5 et y un generateur de H_{40} : $\forall y \exists i \in \mathbb{Z}$ / $yxy^{-1} = x^i$.

$n_5 = 1 \Rightarrow$ l'unique $H_5 \Delta G$

$\Rightarrow \forall y \in G,\ yH_5y^{-1} \subset H_5$

or $H_5 = \langle x \rangle = \{1, x, x^2, \dots, x^{p-1}\}$

$\Rightarrow yxy^{-1} \in \langle x \rangle$

$\Rightarrow \exists i \in [1, p-1]$ tq $yxy^{-1} = x^i$

Mq $\phi : H_5 \longrightarrow H_5$, $x \longmapsto yxy^{-1} = x^i$ est automorphisme.

Soit $a, b \in H_5 = \langle x \rangle$, $\exists l, k \in [0, 4]$, $a = x^l$, $b = x^k$

$\phi(ab) = \phi(x^l x^k)$
$= yx^l x^k y^{-1}$
$= yx^l y^{-1} yx^k y^{-1}$
$= \phi(x^l)\phi(x^k)$
$= \phi(a)\phi(b)$

~~Donc ϕ est un automorphisme~~

$\ker \phi = \{a \in H_5 / \phi(a) = 1\}$

$a \in H_5, \exists l \in [0,4] / a = x^l$

$\phi(a) = \phi(x^l) = 1$

$\Rightarrow yx^l y^{-1} = 1$

$yx^l y^{-1} = 1$

$\Rightarrow yx^l = y$

$\Rightarrow x^l = 1 \Rightarrow a = 1$

$\ker \phi = \{1\} \Leftrightarrow \phi$ est injective

$|H_5| = 5$ fini alors ϕ est bijective.

D'où ϕ est un automorphisme reduisons que 5 ne divise pas i.

Supposons $5 / i$, $\exists a \in \mathbb{Z}$ / $i = 5a$

Donc $x^i = x^{5a} = (x^5)^a = 1^a$

$x^i = 1 \Leftrightarrow yxy^{-1} = 1 \Leftrightarrow x = 1$

$\Rightarrow H_5 = \langle x \rangle = \langle 1 \rangle = \{1\}$ absurde

5 ne divise pas i

iii, Mq $\phi^{40} = id$?

~~$\phi^2(x)$~~ $= \phi(x) = yxy^{-1}$

$\phi^2(x) = y\phi(x)y^{-1}$
$= yyxy^{-1}y^{-1}$
$= y^2 x y^{-2}$

$\phi^k(x) = y^k x y^{-k}$

$\phi^{40}(x) = y^{40} x y^{-40}$
$= x$ Car $o(y) = 40$

Autre méthode

$\phi^2(x) = \phi \circ \phi(x)$

$= \phi(x^i)$

$= (x^i)^i = x^{i^2}$

$\phi^k(x) = x^{i^k}$

Hq $i^{4k+1} \equiv 1[5]$

$\phi^{4k+1}(x) = x$

$x^{i^{4k+1}} = x$

$x^{-1} x^{i^{4k+1}} = 1$

$\Rightarrow x^{i^{4k+1}-1} = 1$

$5 \mid i^{4k+1} - 1 \Rightarrow i^{4k+1} \equiv 1[5]$

~~$i^{4k+1} \equiv i[5]$~~

$\begin{cases} 5 \nmid i \\ 5 \text{ premier} \end{cases} \Rightarrow i^{5-1} \equiv 1[5]$ (petit THM de Fermat)

$\Rightarrow i^4 \equiv 1[5]$

$\Rightarrow \begin{cases} (i^4)^{4k} \equiv 1[5] \\ i \equiv i[5] \end{cases}$

$\Rightarrow i^{4k+1} \equiv i[5]$

Observation

$\begin{cases} \phi^k(x) = x^{i^k} \\ \phi^k = y^k x y^{-k} \end{cases}$

$x^{i^{4k+1}} = y^{4k+1} x y^{-4k-1}$

$= 1_G x 1_G$

$x^{i^{4k+1}-1} = 1_G \Rightarrow o(x) = 5 \mid i^{4k+1} - 1$

$\Rightarrow i^{4k+1} \equiv i[5]$

$i^{4k+1} = 5a + i$

$x^{i^{4k+1}} = \underbrace{(x^5)^a}_{=1_G} \cdot x^i$

$\phi^{4k+1}(x) = x^i$

$\phi^{4k+1}(x) = \phi(x)$

$\phi(x) = x$

$\phi = id$

$\phi^{4k+1}(x) = x^{i^{4k+1}} = x^{5k+1} = (x^5)^k x = x$

iv, Déduisons que $G \simeq \mathbb{Z}/2005$

Lemme : Soit G un groupe, N et H des sous groupes de G.

$N \triangleleft G$, $NH = G$, $N \cap H = \{1\}$

alors : $G \simeq N \times H$

$a \in H_5 \cap H_{401} \Rightarrow a \in H_5$ et $a \in H_{401}$

$\Rightarrow o(a) | 5$ et $o(a) | 401$

$\Rightarrow o(a) \in Div(5, 401) = \{1\}$ car $5 \wedge 401 = 1$

$\Rightarrow o(a) = 1$

$\Rightarrow a^1 = e_G$

$\Rightarrow a = e_G$

$H_5 \cap H_{401} = \{e_G\}$

Mq $H_5 H_{401} = G$?

$H_5 \cap H_{401} = \{e_G\}$

$\Rightarrow H_5 H_{401} \cong H_5 \times H_{401}$

$\Rightarrow |H_5 H_{401}| = |H_5 \times H_{401}|$

$= |H_5| \cdot |H_{401}|$

$= 5 \times 401$

$= |G|$

donc $H_5 \cdot H_{401} < G$

$|H_5| |H_{401}| = |G| \Rightarrow$

$H_5 H_{401} = G$

D'après le lemme,

$G \cong H_{401} \times_\phi H_5$

$\cong H_{401} \times H_5$ car ϕ morphisme trivial

$\cong \mathbb{Z}/401\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}$

$G \cong \mathbb{Z}/(401 \times 5)\mathbb{Z}$ {lemme chinois car hors}

$G = \mathbb{Z}/2005\mathbb{Z}$

Exercice 1

Soit G un groupe tq $|G| = 200$

Mq G n'est pas simple

on a $|G| = 200 = 8 \times 5^2$

$8 \wedge 5 = 1$

$|G|$ est de la forme $m p^n$ avec p premier et $m \wedge 5 = 1$ donc d'après le 1er théorème de Sylow, $\exists$ un 5 sous groupe de Sylow de G et un sous groupe H tq $|H| = 5^2$.

Aussi d'après le 3e théorème de Sylow, le nombre de 5-Sylow n_5 est tq

$\begin{cases} n_5 | 8 \\ n_5 \equiv 1 [5] \end{cases}$

$\begin{cases} n_5 | 8 \\ n_5 \equiv 1 [5] \end{cases} \Leftrightarrow \begin{cases} n_5 \in \{1, 2, 4, 8\} \\ n_5 = 1 + k5 \text{ avec } k \in \mathbb{N} \end{cases}$

Par suite $n_5 = 1 \Rightarrow$ d'unique $H_5 \trianglelefteq G$

$\Rightarrow G$ n'est pas simple.

Exercice 3

* $|G| = 30 = 5 \times 3 \times 2$

Détermine n_5 le nombre de 5-sylow.
Soit H_5 les 5-Sylow

$$\begin{cases} n_5 \equiv 1[5] \\ n_5 \mid 6 \end{cases} \Rightarrow n_5 \in \{1, 6\}$$

$$\begin{cases} n_2 \equiv 1[2] \\ n_2 \mid 15 \end{cases} \Rightarrow n_2 \in \{1, 3, 5, 15\}$$

$$\begin{cases} n_3 \equiv 1[3] \\ n_3 \mid 10 \end{cases} \Rightarrow n_3 \in \{1, 10\}$$

triplet (n_2, n_3, n_5)

le triplet minimal contenant pas 1 est (n_2, n_3, n_5)

$= (3, 10, 6)$

$\Rightarrow$
- 3 2-Sylow H_2^1, H_2^2, H_2^3
- 10 3 Sylow : $H_3^1, H_3^2, \dots, H_3^{10}$
- 6 5 Sylow : $H_5^1, \dots H_5^6$

Lemme

$H, K \subset_{sg} G$

$H \neq K$

$|H| = p = |K|$ (p premier) $\Rightarrow H \cap K = \{e_G\}$

Preuve

$H \cap K \subset_{sg} H \Rightarrow |H \cap K| \mid |H| = p$

$\Rightarrow |H \cap K| \in \{1, p\}$

$|H \cap K| = p \Rightarrow H \cap K = H$

$\Rightarrow H = K$ absurde

Donc $|H \cap K| = 1$

$H \cap K = \{e_G\}$ contient $p-1$ éléments d'ordre p

- 3 2-Sylow $(H_2^1, H_2^2, H_2^3) \longrightarrow 3(2-1)$
- 10 3-Sylow $(H_3^1, \dots H_3^{10}) \longrightarrow 10 \times (3-1)$
- 6 5-Sylow $(H_5^1, \dots H_5^6) \longrightarrow 6 \times (5-1)$

Le triplet minimal ne contenant pas 1
$(n_2, n_3, n_5) = (3, 10, 6)$

$\Rightarrow |G|$ serait donc au moins égal à
$3(2-1) + 10(3-1) + 6 \times (5-1) + 1$
$= 48 > 30$ absurde
Donc nécessairement un des $n_i = 1$, $i \in \{2, 3, 5\}$
prenons $(n_2, n_3, n_5) = (3, 1, 6)$
$3 \times (2-1) + 1 \times (3-1) + 6(5-1) + 1$
$= 30$

• pour $|G| = 42$

$|G| = 7 \times 2 \times 3$

d'après le 3e théo de Sylow

$$\begin{cases} n_7 \equiv 1[7] \\ n_7 \mid 6 \end{cases} \Rightarrow n_7 \in \{1, 2, 3, 6\}$$

donc $n_7 = 1$

Par suite d'unicité 7-Sylow de G est distingué donc G n'est pas simple

• pour $|G| = 105$

$|G| = 105 = 21 \times 5 = 7 \times 3 \times 5$

$$\begin{cases} n_7 \equiv 1[7] \\ n_7 \mid 15 \end{cases} \Rightarrow n_7 \in \{1, 15\}$$

$$\begin{cases} n_3 \equiv 1[3] \\ n_3 \mid 35 \end{cases} \Rightarrow n_3 \in \{1, 7\}$$

$$\begin{cases} n_5 \equiv 1[5] \\ n_5 \mid 21 \end{cases} \Rightarrow n_5 \in \{1, 21\}$$

Soit (n_3, n_5, n_7) le triplet minimale ne contenant pas 1

$(n_3, n_5, n_7) = (7, 21, 15)$

$|G| = 7 \times (3-1) + 21 \times (5-1) + 15 \times (7-1)$

$= 189 > 105$ absurde

donc nécessairement un des n_i : $i \in \{3, 5, 7\}$ prenons $(n_3, n_5, n_7) = (7, 2$

2, Généralisons aux groupes avec p, q, r distincts et premiers on a

$p > q > r$

$|G| = pqr$

D'après le 3e théo de Sylow

$$\begin{cases} n_p \equiv 1[p] \\ n_p \mid qr \end{cases}$$

$n_p \mid qr \Rightarrow n_p \in \{1, q, r, qr\}$

• si $n_p = q$ alors $p \mid q-1$ avec $p \leq q-1 < q$ absurde car $p > q$ donc $n_p \neq q$

• si $n_p = r \Rightarrow p \mid r-1$ et donc $p \leq r-1 < r$ absurde car $p > r$ donc $n_p \neq r$.

donc $n_p \in \{1, qr\}$

$$\begin{cases} n_q \equiv 1[2] \\ n_q \mid pr \end{cases}$$

$n_q \mid pr \Rightarrow n_q \in \{1, p, r, pr\}$

- si $n_q = p$ alors $q \mid p-1$ et donc $q \leq p-1 < q$ donc n_q peut être égale à p
- si $n_q = r$ alors $q \leq r-1 < r$ absurde car $q > r$ donc $n_q \neq r$

donc $n_q \in \{1, p, pr\}$

$$\begin{cases} n_r \equiv 1 [r] \\ n_r \mid pq \end{cases}$$

$\Rightarrow n_r \mid pq \Rightarrow$ ~~div et~~

$n_r \in \{1, p, q, pq\}$.

- si $n_r = p$ alors $r \leq p-1 < p$ donc n_r peut être egale à p
- si $n_r = q$ alors $r \leq q-1 < q$ n_r peut être egale à q

$n_r \in \{1, p, q, pq\}$

Soit (n_r, n_p, n_q) le triplet minimal ne contenant pas 1

$(n_r, n_p, n_q) = (q, qr, p)$

donc $|G| = q(r-1) + qr(p-1) + [(q-1)+1]$

$= (p-1)(q-1) + qr + p$

p et q premiers $\Rightarrow p \geq 2$ et $q \geq 2$

donc $\begin{cases} p-1 \geq 1 \\ q-1 \geq 1 \end{cases} \Rightarrow (p-1)(q-1) \geq 1$

Donc $(p-1)(q-1) + pqr \geq 1 + pqr > pqr$

Absurde

donc necessairement un des $n_i = 1$

$i \in \{r, p, q\}$

Par suite H_i est l'unique i-sylow distingué dans G donc G n'est pas simple.

Exercice 4

On suppose qu'il existe une groupe simple G d'ordre 180

1, Montrons que si $n_5 = 6$ alors il existe un morphisme non-trivial et injectif $\phi : G \longrightarrow S_6$

$Sp(G) = \{$ p-sylow de $G\}$

$|Sp(G)| = n_p$

$* \quad G \times Sp(G) \cdots Sp(G)$

$(g, H_p) \longmapsto g * H_p = g H_p g^{-1}$

$\Rightarrow \exists \phi : G \longrightarrow \text{Sym}(Sp(G)) \cong S_{n_p}$

$g \longmapsto \phi(g) : Sp(G) \longrightarrow Sp(G)$

$H_p \longmapsto \phi(g)(H_p) = g H_p g^{-1}$

$n_5 = 6$

$\phi : G \longrightarrow S_6$

$g \longmapsto \phi(g) : [\![1,6]\!] \longrightarrow [\![1,6]\!]$

$x \longmapsto \phi(g)(x) = g x g^{-1}$

$S_5(G) = \{5\text{-sylow de } G\}$

$|S_5(G)| = n_5 = 6$

* $G \times S_5(G) \cdots S_5(G)$

$(g, H_5) \longmapsto g * H_5 = g H_5 g^{-1}$

$\Rightarrow \exists \phi : G \longrightarrow \mathrm{Sym}(S_5(G)) \cong S_{n_5} = S_6$

$g \longmapsto \phi(g) : S_5(G) \longrightarrow S_5(G)$

$H_5 \longmapsto \phi(g)(H_5) = g H_5 g^{-1}$

* Mq ϕ est non trivial

Supposons ϕ trivial

$\Rightarrow \forall g \in G \quad \phi(g) = \text{neutre de } \mathrm{Sym}(S_5(G)) = id_{S_5(G)}$

$\Rightarrow \forall g \in G \ \forall H_5 \in S_5(G)$

$\phi(g)(H_5) = id_{S_5(G)}(H_5)$

$\| \qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad$

$g H_5 g^{-1} = H_5$

$\Rightarrow H_5 \triangle G$ absurde car G est supposé simple

Donc ϕ est non trivial

* Mq ϕ est injectif

$\ker \phi \triangleleft G \Rightarrow \ker \phi = \{e\}$ ou G

Car G supposé simple

• $\ker \phi = G \Rightarrow \phi$ est trivial absurde.

Donc $\ker \phi = \{e\}$ et ϕ injectif

2) En utilisant la signature $\varepsilon : S_6 \longrightarrow \{-1, 1\}$.

Montrons que G s'identifie à un sous-groupe de A_6

$$\begin{array}{ccccc} G & \xrightarrow{\phi} & S_6 & \xrightarrow{\varepsilon} & \{-1,1\} \\ \downarrow & & & & \uparrow i \\ G/\ker(\varepsilon\circ\phi) & \xrightarrow{\cong} & & & \mathrm{im}(\varepsilon\circ\phi) \end{array}$$

$\ker(\varepsilon \circ \phi) \triangle G \Rightarrow \ker(\varepsilon\circ\phi) = \{e_G\}$ ou G

car G supposé simple

• Si $\ker(\varepsilon\circ\phi) = \{e_G\}$

$G/\ker(\varepsilon\circ\phi) = G/\{e_G\} = G \cong$

$\Rightarrow |G| = |\mathrm{im}(\varepsilon\circ\phi)| \leq |\{-1, 1\}| = 2$ absurde

Donc $\ker(\varepsilon\circ\phi) = G$

$\Rightarrow \forall g \in G, \ \varepsilon\circ\phi(g) = 1$

$\varepsilon(\phi(g)) = 1$

$\Rightarrow \forall g \in G \quad \phi(g) \in \ker \varepsilon$

$\Rightarrow \mathrm{im}\,\phi \subset \ker \varepsilon = A_6$

$\uparrow$

G

Donc G s'identifie à un sg de A_6

1er THM d'iso

$$\begin{array}{ccc} G & \longrightarrow & S_6 \\ \downarrow & & \uparrow \\ G/\ker\phi & \xrightarrow{\cong} & \mathrm{im}\,\phi \end{array}$$

$G/\{e_G\} \cong G$

b) En utilisant A_6 simple, montrer que $n_5 = 36$

$180 = 2^2 \times 3^2 \times 5$

$n_5 | 36 \Rightarrow n_5 \in \{1, 2, 3, 4, 6, 9, 12, 18, 36\}$

$n_5 \equiv 1[5] \Rightarrow n_5 = \{1, 6, 36\}$

* $n_5 = 1 \Rightarrow \exists! H_5$ 5-sylow

$\Rightarrow H_5 \triangleleft G$ absurde car G simple

Donc $n_5 \neq 1$

* $n_5 = 6$ alors l'étude $\phi(G)(H_5) = id_{S_3(G)}(H_5)$ dit que $G \cong H \subset_{Sg} A_6$

$\Rightarrow [A_6 : H] = \frac{|A_6|}{|H|} = \frac{|A_6|}{|G|}$

$= \frac{6!/2}{180} = 2$

$\Rightarrow H \triangleleft A_6$ absurde car A_6 simple

Donc $n_5 \neq 6$

Par suite $n_5 = 36$

c) $n_3 | 20 \Rightarrow n_3 \in \{1, 2, 4, 5, 10, 20\}$

$n_3 \equiv 1[3] \Rightarrow n_3 \in \{1, 4, 10\}$

* $n_3 = 1 \Rightarrow \exists! H_3$ 3-sylow

$\Rightarrow H_3 \triangleleft G$ absurde car G simple

Donc $n_3 \neq 1$

* $n_3 = 4$

$3\phi : G \longrightarrow Sym(S_3(G)) \cong S_4$

$g \longmapsto \phi(g) : S_3(G) \to S_3(G)$

$H_3 \longmapsto gH_3g^{-1}$

$\ker\phi \triangleleft G \Rightarrow$

$\ker\phi = \{e\}$ ou G

$\ker\phi = G \Rightarrow \phi$ trivial

$\Rightarrow g \in G, \phi(g) = id_{S_3(G)}$

$\Rightarrow H_3 \in S_3(G)$

$\phi(g)(H_3) = id_{S_3(G)}(H_3)$

$gH_3g^{-1} = H_3$

$H_3 \triangleleft G$ absurde

Par suite $\ker\phi = \{e\}$

1er THM

$G/\ker\phi = G/\{e\} = G$

$|G| = |\mathrm{Im}\,\phi| \leq |S_4| = 4! = 24$

$180 \leq 24$ absurde

Donc $n_3 \neq 4$

et $n_3 = 10$

Si $M_g \subset C_G(g) < G$

* $G \times G/C_G(g) \longrightarrow G/C_G(g)$

$(x, \bar{y}) \longmapsto x * \bar{y} = \overline{xy} = xy\,C_G(g)$

$\bar{y} = y\,C_G(g)$

$G/C_G(g) = \{\bar{y}, y \in G\}$

$= \{y \cdot C_G(g), y \in G\}$.

On a: $e_G \in C_G(g)$ en effet,

$ye_G = e_G$

Soient $x, y \in C_G(g)$

$x, y \in C_G(g) \Rightarrow \begin{cases} gx = xg \\ gy = yg \end{cases}$

on a: $gxy = (gx)y = (xg)\cdot y$

$= x(gy) = xyg$

Ainsi $xy \in C_G(g)$

$x \in C_G(g) \Rightarrow gx = xg$

$\Rightarrow x^{-1}gxx^{-1} = x^{-1}xgx^{-1}$

$\Rightarrow x^{-1}g = gx^{-1}$

Ainsi $x^{-1} \in C_G(g)$

Par conséquent $C_G(g) < G$

puisque $C_G(g) < G$ alors d'après le théorème de Lagrange $|C_G(g)| \,/\, |G| = 180$

$|C_G(g)| \in \{1, 2, 3, 6, \ldots, 180\}$

Comme $s, g, g^{-1} \in C_G(g)$ alors

$|C_G(g)| \in \{3, 6, \ldots, 180\}$

$|C_G(g)|$ S, T 3-sylow $\Rightarrow |S| = |T| = 9$

$\Rightarrow$ S et T sont abeliens

S abelien et $g \in S \Rightarrow \forall s \in S, gs = sg$

$\Rightarrow S \subset C_G(g)$

$\Rightarrow |S| \,/\, |C_G(g)|$

$\Rightarrow 9 \,/\, |C_G(g)|$

$\Rightarrow |C_G(g)| \in \{9, 18, 36, 45, 90, 180\}$

Supposons $|C_G(g)| = 180 = |G|$

$|C_G(g)| = 180 \Rightarrow C_G(g) = G$

$\Rightarrow gx = xg, \forall x \in G$

$\Rightarrow g \in Z(G)$

$\Rightarrow \langle g \rangle < Z(G)$

$\Rightarrow \forall x \in G, x\langle g \rangle = \langle g \rangle x$

$\Rightarrow \langle g \rangle \triangleleft G$, ce qui est absurde.

Donc $|C_G(g)| \in \{9, 18, 36, 45, 90\}$

Par ailleurs

$S \cup T < C_G(g)$

Car S et T ~~$< C_G(g)$~~ sont abeliens

$S \cup T \subset C_G(g) \Rightarrow |S \cup T| \leq |C_G(g)|$

$\Rightarrow |S| + |T| - |T \cap S| \leq |C_G(g)|$

or $T \cap S \subsetneq T \Rightarrow |T \cap S| < |T| = 9$

$\Rightarrow -|T \cap S| > -9$

$\Rightarrow |S| + |T| - |T \cap S| > |S| + |T| - 9$

$\Rightarrow |C_G(g)| \geq |S| + |T| - |T \cap S| > 9$

$\Rightarrow |C_G(g)| \in \{18, 36, 45, 90\}$

si $|C_G(g)| = 90$ alors $[G : C_G(g)] = e$

donc

$C_G(g) \lhd G$ ce qui est absurde

car G est simple.

Ainsi $|C_G(g)| \in \{18, 36, 45\}$

On sait que G agit sur $G/C_G(g)$

par $G \times G/C_G(g) \longrightarrow G/C_G(g)$

$(x, yC_G(g)) \longmapsto xyC_G(g)$

$= xy\,C_G(g)$

$(x, \bar{y}) \longmapsto x * \bar{y} = \overline{xy}$

Alors $\exists\, \phi : G \longrightarrow \mathrm{Sym}(G/C_G(g))$

un morphisme défini par

$\phi : G \longrightarrow \mathrm{Sym}(G/C_G(g))$

$x \longmapsto \phi(x) : G/C_G(g) \longrightarrow G/C_G(g)$

$\bar{y} \longmapsto \phi(x)(\bar{y}) = \overline{xy}$

Mq ϕ est non trivial

Supposons que ϕ est trivial

ϕ trivial $\Rightarrow \forall x \in G,\ \phi(x) = Id_{G/C_G(g)}$

$\Rightarrow \forall x \in G, \forall \bar{y} \in G/C_G(g)$

$\phi(x)(\bar{y}) = \bar{y}$

$\Rightarrow \forall x \in G \ \forall \bar{y} \in C_G(g)$

$\overline{xy} = \bar{y}$

$\Rightarrow xy \cdot y^{-1} \in C_G(g)$

$\Rightarrow x \in C_G(g),\ \forall x \in G$

$\Rightarrow C_G(g) = Z(G)$ absurde

Mq ϕ est injectif

Puisque $\ker\phi \lhd G$ et G est simple alors

$\ker\phi = \{C_G\}$ ou $\ker\phi = G$

Supposons que $\ker\phi = G$

$\ker\phi = G$ alors ϕ est trivial, ce qui est absurde

par suite $\ker\phi = \{C_G\}$,

donc ϕ est injectif

D'après le 1er théo d'isomorphisme, on a

$G \xrightarrow{\ \phi\ } \mathrm{Sym}(G/C_G(g))$

$\pi \downarrow \qquad \nearrow j$

$G/\ker\phi \xrightarrow{\ \bar{\phi}\ } \mathrm{Im}\,\phi$

$G/\ker\phi \simeq G \simeq \mathrm{Im}\,\phi$

Or $\mathrm{Sym}(G/C_G(g)) \simeq S_{|G/C_G(g)|}$

donc $G \simeq \mathrm{Im}\, d < \mathrm{Sym}(G/C_G(g))$

alors $|G| \mid |S_k|$ avec $k = |G/C_G(g)|$

or $|C_G(g)| \in \{18, 36, 45\}$

si $|C_G(g)| = 18$ alors $k = \frac{180}{18} = 10$ et $|S_{10}| = 10!$ possible

si $|C_G(g)| = 36$ alors $k = 5$

$|S_5| = 5!$ impossible

si $|C_G(g)| = 45$ alors $k = 4$

$|S_4| = 4!$ impossible

Par conséquent $|C_G(g)| = 18$

6) soit H un groupe d'ordre 18.

$|H| = 18 = 2 \times 3^2$

D'après le 3e théo de Sylow, on a :

$$\begin{cases} n_3 \equiv 1[3] \\ n_3 \mid 2 \end{cases} \Rightarrow n_3 = 1$$

Ainsi H admet un unique 3-Sylow.

Comme $|C_G(g)| = 18$ alors $C_G(g)$ admet un unique 3-Sylow donc $S = T$.

Par suite s'il n'existe pas 3-Sylow distincts contenant un même élément $g \neq e$

7) supposons qu'il existe un groupe simple G d'ordre 180

$|G| = 180$ alors $\begin{cases} n_5 = 36 \\ n_3 = 10 \end{cases}$

$H_5^i \cap H_5^j = \{e_G\}$, pour $i \neq j$

$H_3^i \cap H_3^j = \{e_G\}$, d'après 5) et 6) pour $i \neq j$

le nombre d'élément de G serait

$36 \times (5-1) + 10(3^2 - 1) + 1$

(contribution des H_5 ; H_3 ; neutre)

$= 144 + 80 + 1 > 180 = |G|$

TD 4

Exercice 1

1, Mq $\sqrt{I}$ est un Idéal de A

$\sqrt{I} = \{ x \in A / \exists n \geq 1, x^n \in I \}$

* $\sqrt{I} \neq \phi$, $0_A \in \sqrt{I}$ car $0_A^n = 0_A \in I$

Soient $x, y \in \sqrt{I}$, il existe $n, m \geq 1 / x^m \in I$ et $y^n \in I$

Mq $x - y \in \sqrt{I}$

Cherchons $\alpha \geq 1$ tq $(x-y)^\alpha \in I$

Prenons $\alpha = m + n + 1 \geq 1$

Vérifions que $(x-y)^{m+n+1} \in I$

A est commutatif on a

$$(x-y)^{m+n+1} = \sum_{k=0}^{m+n+1} C_{m+n+1}^k x^k (-y)^{m+n+1-k}$$

$$= \sum_{k=0}^{m} C_{m+n+1}^k x^k (-y)^{m+n+1-k} + \sum_{k=m+1}^{m+n+1} C_{m+n+1}^k x^k (-y)^{m+n+1-k}$$

$$= (-y)^n \underbrace{\left(\sum_{k=0}^{m} C_{m+n+1}^k x^k y^{k-m} (m+1-k) \right)}_{\in A} + x^m \underbrace{\sum_{k=m+1}^{m+n+1} C_{m+n+1}^k x^{k-m} (-y)^{m+n+1-k}}_{\in A}$$

$(-y)^n \in I$, $\left(\sum_{k=0}^{m} \ldots \right) \in A$ donc $\in I$

$x^m \in I$, $\sum_{k=m+1}^{m+n+1} \ldots \in A$ donc $\in I$

$0 < 1 \leq m+1-k \leq m+1$

$0 < 1 \leq 2k - m \leq n+1$

$0 < m+1 \leq m+n+1-k \leq n$

Par suite $\sqrt{I} \subset \sqrt{(A,+)}$

- Mq $A \cdot \sqrt{I} \subset \sqrt{I}$

Soient $y \in \sqrt{I}$ et $x \in A$, alors
$\exists m > 0 / y^m \in I$
Cherchons $n > 1 / (xy)^n \in I$
$(xy)^m = x^m y^m \in I$ Car I idéal
$\in A$ $\in I$
Par conséquent $xy \in \sqrt{I}$

2) a Supposons que les diviseurs de zéro de A/I sont nilpotent.
Mq I primaire

Soient $x, y \in A$
$\begin{cases} xy \in I \\ x \notin I \end{cases} \Rightarrow \begin{cases} \bar{x}\bar{y} = \bar{0} \\ \bar{x} \neq \bar{0} \end{cases}$
$\Rightarrow \begin{cases} \bar{x} \cdot \bar{y} = \bar{0} \\ \bar{x} \neq \bar{0} \end{cases}$

- Si $\bar{y} \neq \bar{0}$ alors $\bar{y}$ est un diviseur de zéro
$\Rightarrow \bar{y}$ est nilpotent
$\Rightarrow \exists m > 1 / \bar{y}^m = \bar{0} \Rightarrow y^m \in I$
$\Rightarrow y \in \sqrt{I}$
- Si $\bar{y} = \bar{0}$ alors $y \in I$
$y^1 \in I$
$y \in \sqrt{I}$

Par suite, I est primaire

Supposons I primaire
Soient $\bar{x}$ un diviseur de zéro de A/I.
Montrons que $\bar{x}$ est nilpotent

$\bar{x}$ un diviseur de zéro
$\Rightarrow \bar{x} \neq \bar{0}$ et $\exists \bar{y} \in A/I, \bar{y} \neq \bar{0}$ tq $\bar{x} \cdot \bar{y} = \bar{0}$

$\Rightarrow \overline{xy} = \bar{0} \Rightarrow xy \in I$ et $y \notin I$
$\Rightarrow x \in \sqrt{I}$
$\Rightarrow \exists n \geq 1 / x^n \in I$
$\Rightarrow \overline{x^n} = \bar{0}$
$\Rightarrow \bar{x}^n = \bar{0}$

$\Rightarrow \bar{x}$ est nilpotent.

b, Supposons I un idéal premier
Soient $(x, y) \in A^2$, $xy \in I$ et I
Mq $y \in \sqrt{I}$
$xy \in I$
$\Rightarrow y \in I$ Car I est
$\Rightarrow y^1 \in I$
$\Rightarrow y \in \sqrt{I}$

Donc I est primaire.

c, Supposons I primaire
Soient $x, y \in A$ $x \cdot y \in \sqrt{I}$
$xy \in \sqrt{I} \Rightarrow \exists m \geq 1, (xy)^m = I$
$\Rightarrow x^m \cdot y^m \in I$
Supposons $x^m \notin I$.
Alors $y^n \in \sqrt{I}$ Car
I est primaire
$y^n \in \sqrt{I} \Rightarrow \exists m \geq 1 / (y^n)^m \in I$
$\Rightarrow y^{nm} \in I$
$y \in \sqrt{I}$

$\bar{x} - \bar{b} \in \bar{I} \Leftrightarrow x \in I$

Supposons $y^n \notin I$ et $x^n \cdot y^n \in I$

$y^n \notin I$

$x^n y^n \in I$

① $x^n \notin I$

② $y^n \notin I$

③ $x^n \cdot y^n \in I$

Exercice 2

On considère l'anneau $\mathbb{Z}[i\sqrt{5}]$ et on définit la norme N par $N(z) = z\bar{z}$

1, Montrons que $N(zz') = N(z)N(z')$

$N(zz') = zz'\overline{zz'}$

$= zz'\bar{z}\bar{z'}$

$= z\bar{z}\, z'\bar{z'}$

$= N(z)N(z')$

2, Montrons que $N(z) = 1 \Leftrightarrow z \in \mathbb{Z}[i\sqrt{5}]^\times$

Supposons que $N(z) = 1 \Rightarrow z \in \mathbb{Z}[i\sqrt{5}]$

$N(z) = 1$

$\Rightarrow z\bar{z} = 1$

$\Rightarrow z \in \mathbb{Z}[i\sqrt{5}]^\times$ et $z^{-1} = \bar{z}$

Supposons que $z \in \mathbb{Z}[i\sqrt{5}]^\times$ et montrons que $N(z) = 1$

$z \in \mathbb{Z}[i\sqrt{5}]^\times \Rightarrow z' \in \mathbb{Z}[i\sqrt{5}]$

(q $zz' = 1 \Rightarrow N(zz') = N(1)$

$\Leftrightarrow N(z)N(z') = 1$

3, Montrons que $\mathbb{Z}[i\sqrt{5}]$ n'est pas factoriel

$\mathbb{Z}[i\sqrt{5}] = \{a + ib\sqrt{5}, a, b \in \mathbb{Z}\}$

$N : \mathbb{Z}[i\sqrt{5}] \longrightarrow \mathbb{N}$

$z \longmapsto N(z) = z\bar{z}$

$= (a + ib\sqrt{5})(a - ib\sqrt{5})$

$= a^2 + 5b^2 \in \mathbb{N}$

$N(6) = N(6 + 0i\sqrt{5})$

$= 6^2 + 5 \times 0^2$

$= 36 + 1 \Rightarrow 6 \in \mathbb{Z}[i\sqrt{5}]^\times$

$6 = 3 \times 2$

$6 = (1 + i\sqrt{5})(1 - i\sqrt{5})$

Vérifions que 2, 3, $(1 + i\sqrt{5})$ $(1 - i\sqrt{5})$ sont des irréductibles dans $\mathbb{Z}[i\sqrt{5}]$

Supposons que $z = zz'$ et Mq z ou $z' \in \mathbb{Z}[i\sqrt{5}]^\times$

$z = zz' \Rightarrow N(z) = N(zz')$

$\Rightarrow N(z) = N(z)N(z')$

$\Rightarrow 4 = N(z)N(z')$

$\Rightarrow (N(z), N(z')) \in \{(1,4), (4,1), (2,2)\}$ car $\text{im}\, N \subseteq \mathbb{N}$

si $(N(z), N(z')) = (2,2)$ alors $a^2 + 5b^2 = 2$ impossible dans $\mathbb{Z}$.

Donc $(N(z), N(z')) \in \{(1,4), (4,1)\}$

i.e z ou z' inversible et z est irréductible.

$z - b \in I \Leftrightarrow z \in I$

Supposons $y^n \in I \cdot x^n \cdot y^n \in I$

$y^n \in I$ | ① $x^n \notin I$

$x^n y^n \in I$ | ② $y^n \in I$

③ $x^n \cdot y^n \in I$

Exercice 2

1) Considère l'anneau $\mathbb{Z}[i\sqrt{5}]$ et on définit la norme N par $N(z) = z\bar{z}$

1, Montrons que $N(zz') = N(z)N(\bar{z})$

$N(zz') = zz'\overline{zz'}$

$= zz'\bar{z}\bar{z}'$

$= z\bar{z}\, z'\bar{z}'$

$= N(z)N(z')$

2) Montrons que $N(z) = 1 \Leftrightarrow z \in \mathbb{Z}[i\sqrt{5}]^\times$

Supposons que $N(z) = 1 \Rightarrow z \in \mathbb{Z}[i\sqrt{5}]$

$N(z) = 1$

$\Rightarrow z\bar{z} = 1$

$\Rightarrow z \in \mathbb{Z}[i\sqrt{5}]^\times$ et $z^{-1} = \bar{z}$

Supposons que $z \in \mathbb{Z}[i\sqrt{5}]^\times$ et montrons que $N(z) = 1$

$z \in \mathbb{Z}[i\sqrt{5}]^\times \Rightarrow z' \in \mathbb{Z}[i\sqrt{5}]$

tq $zz' = 1 \Rightarrow N(zz') = N(1)$

$\Leftrightarrow N(z)N(z') = 1$

$\Rightarrow N(z) = 1$ Car $N(z) \in \mathbb{N}$

3, Montrons que $\mathbb{Z}[i\sqrt{5}]$ n'est pas factoriel

$\mathbb{Z}[i\sqrt{5}] = \{a + ib\sqrt{5}, a, b \in \mathbb{Z}\}$

$N : \mathbb{Z}[i\sqrt{5}] \longrightarrow \mathbb{N}$

$z \longmapsto N(z) = z\bar{z}$

$= (a+ib\sqrt{5})(a-ib\sqrt{5})$

$= a^2 + 5b^2 \in \mathbb{N}$

$N(6) = N(6 + 0i\sqrt{5})$

$= 6^2 + 5 \times 0^2$

$= 36 \neq 1 \Rightarrow 6 \in \mathbb{Z}[i\sqrt{5}]^\times$

$6 = 3 \times 2$

$6 = (1 + i\sqrt{5})(1 - i\sqrt{5})$

Vérifions que 2, 3, $(1+i\sqrt{5})$ $(1-i\sqrt{5})$ sont des irréductibles dans $\mathbb{Z}[i\sqrt{5}]$

Supposons que $z = zz'$ et Mq z ou $z' \in \mathbb{Z}[i\sqrt{5}]^\times$

$z = zz' \Rightarrow N(z) = N(zz')$

$\Rightarrow N(z) = N(z)N(z')$

$\Rightarrow 4 = N(z)N(z')$

$\Rightarrow (N(z), N(z')) \in \{(1,4), (4,1), (2,2)\}$ car $\mathrm{im}\, N \subseteq \mathbb{N}$

si $(N(z), N(z')) = (2,2)$ alors $a^2 + 5b^2 = 2$ impossible dans $\mathbb{Z}$.

Donc $(N(z), N(z')) \in \{(1,4), (4,1)\}$

i.e z ou z' inversible et z est irréductible.

De même on vérifie que 3 est irréductible.

$1+i\sqrt{5} = zz'$

$\Rightarrow N(1+i\sqrt{5}) = N(zz')$

$\Rightarrow 6 = N(z) \times N(z')$

$\Rightarrow (N(z), N(z')) \in \{(1,6),(6,1),(2,3),(3,2)\}$

Si $(N(z), N(z')) = (2,3)$ alors

$$\begin{cases} 2 = a^2 + 5b^2 \\ 3 = a^2 + 5b^2 \end{cases}$$

$\Rightarrow$ n'admet pas de solution dans $\mathbb{Z}$

Donc $(N(z), N(z')) \in \{(1,6),(6,1)\}$

Vérifions voir si les facteurs sont associés.

Supposons que 3 est associé à $(1+i\sqrt{5})$

$3 = z \times (1+i\sqrt{5})$ avec $z \in \mathbb{Z}[i\sqrt{5}]$

$\Rightarrow N(3) = N(z)\, N(1+i\sqrt{5})$

$\Rightarrow 9 = 1 \times 6$ absurde

de même 3 n'est pas associé à $(1-i\sqrt{5})$ et 2 n'est pas associé à chacun de ces facteurs.

Par conséquent $\mathbb{Z}[i\sqrt{5}]$ n'est pas factoriel.

4) Montrons que $\mathbb{Z}[i\sqrt{5}] \cong \mathbb{Z}[X]/(X^2+5)$

Soit $\varphi : \mathbb{Z}[X] \longrightarrow \mathbb{Z}[i\sqrt{5}]$

$P \longmapsto P(i\sqrt{5})$

Mq φ est un morphisme d'anneaux

Soient $P(X)$ et $q(X) \in \mathbb{Z}[X]$

$\varphi(P \times q)(X) = \varphi(P(X) \times q(X))$

$= P(i\sqrt{5})\, q(i\sqrt{5})$

$= \varphi(P(X)) \times \varphi(q(X))$

$\varphi(P+q)(X) = \varphi(P(X) + q(X))$

$= P(i\sqrt{5}) + q(i\sqrt{5})$

$= \varphi(P(X)) + \varphi(q(X))$

$1_{\mathbb{Z}[X]} = 1 \times X^0 + 0 \times X^1 + 0X^2 + \dots$

$1_{\mathbb{Z}[i\sqrt{5}]} = 1 + 0 \times i\sqrt{5}$

$\varphi(1_{\mathbb{Z}[X]}) = 1(i\sqrt{5})^0 + 0 \cdot (i\sqrt{5})^2 + \dots$

$= 1$

$= 1 + 0 \times i\sqrt{5} = 1_{\mathbb{Z}[i\sqrt{5}]}$

Montrons que φ est surjective

Soit $z \in \mathbb{Z}[i\sqrt{5}]$ alors $\exists a, b \in \mathbb{Z}$

$z = a + i\sqrt{5}\, b$ cherchons $P \in \mathbb{Z}[X]$ /

$\varphi(P) = z$

$P(i\sqrt{5}) = a + i\sqrt{5}\, b$

Prenons $P(X) = a + bX$

déterminons Ker φ

$\operatorname{Ker}\varphi = \{P \in \mathbb{Z}[X] / \varphi(P) = 0\}$

$= \{P \in \mathbb{Z}[X] / P(i\sqrt{5}) = 0\}$

$P(i\sqrt{5}) = 0 \Rightarrow i\sqrt{5}$ et $-i\sqrt{5}$ sont des racines de P car $a, b \in \mathbb{Z}$

$\Rightarrow X^2+5 \mid P$ car le coefficient dominant de x^2+5 est $1 \in \mathbb{Z}^\times$

$\Rightarrow P \in (x^2+5) \Rightarrow \ker\varphi \subset (X^2+5)$

De plus $(X^2+5) \subset \ker\varphi$ car

$\varphi(x^2+5) = (i\sqrt{5})^2 + 5 = 0$

$(x^2+5) \overset{\text{def}}{=} (x^2+5)\cdot\mathbb{Z}[X]$ i.e multiples de x^2+5

$$\begin{array}{ccc} \mathbb{Z}[X] & \longrightarrow & \mathbb{Z}[i\sqrt{5}] \\ \downarrow & & \uparrow i \\ \mathbb{Z}[X]/\ker\varphi & \xrightarrow{\simeq} & \mathbb{Z}[X]/(x^2+5) \end{array} \quad \text{im}\varphi = \mathbb{Z}[i\sqrt{5}]$$

$\mathbb{Z}[X]/\ker\varphi = \mathbb{Z}[X]/(x^2+5)$

D'après le 1er Thm d'isomorphisme

$\mathbb{Z}[i\sqrt{5}] \overset{\simeq}{=} \mathbb{Z}[X]/(x^2+5)$

5, Déterminons $\text{Frac}(\mathbb{Z}[i\sqrt{5}])$

$$\text{Frac}(\mathbb{Z}[i\sqrt{5}]) = \left\{ \frac{z}{z'} \mid z, z' \in \mathbb{Z}[i\sqrt{5}] \right\}$$

$$= \left\{ \frac{a+i\sqrt{5}b}{a'+i\sqrt{5}b'} \mid a,b \in \mathbb{Z} \text{ et } (a',b') \in \mathbb{Z}^2 \setminus \{(0,0)\} \right\}$$

$= \mathbb{Q}[i\sqrt{5}]$ Après avoir rendu rationnel le dénominateur z'.

$$\frac{z}{z'} = \frac{z\bar{z}'}{z\bar{z}'} = \frac{z\bar{z}'}{|z'|^2} \in \mathbb{Z}[i\sqrt{5}] \in \mathbb{Q}[i\sqrt{5}]$$

$\in \mathbb{N}$

Exercice

1, Simplifions $A[X]/(x-a)$ où $a \in A$ avec A un anneau

Cherchons un morphisme d'anneau φ tq $\ker\varphi = (x-a)$

Dans $A[X]/(x-a) \cong A, \bar{P} = P(a)$

$$\overline{x-a} = \bar{0}$$
$$\Rightarrow \bar{x} - \bar{a} = \bar{0}$$
$$\Rightarrow \bar{x} = \bar{a}$$

$A = \mathbb{Z}$, $a = 2$ | $\mathbb{Z}[X]/(x-2)$

soit $P(x) = 5x^3 + 2x^2 + 6x - 1$

$$= \bar{5}\bar{x}^3 + \bar{2}\bar{x}^2 + \bar{6}\bar{x} - \bar{1}$$
$$= 5\times\bar{2}^3 + \bar{2}\times\bar{2}^2 + \bar{6}\bar{2} - \bar{1}$$
$$= \overline{59}$$

Intuitivement $A[X]/(x-a) \cong A$

Stratégie trouver $\varphi : A[X] \to A$ tq:

1. φ morphisme d'anneau
2. ~~Ker~~ φ surjectif
3. $\ker\varphi = (x-a)$
4. Conclure avec le 1er THm d'isom

soit $\varphi : A[X]/(X-a) \longrightarrow A$

$P(X) \longmapsto \varphi(P(X)) = P(a)$

* Surjectivité :

Soit $b \in A$ cherchons $P(X) \in A[X]$ tq

$P(a) = b$

il suffit de prendre $P(X) = b^{A} \in A[X]$

$= b X^0 + 0 X^1 + \dots + 0 X^n$

• $\varphi(X-a) = a - a = 0$

$\Rightarrow (X-a) \subset \ker\varphi$

• Soit d un diviseur de $X-a$ dans A

$1_A \in A^\times$

$X - a = 1_A \cdot X - a \in A[X]$

Donc $P \in \ker\varphi \Rightarrow P(X) = 0$

$\Rightarrow (X-a) / P$

$\Rightarrow \ker\varphi \subset (X-a)$

* $\mathbb{Z}[X]/(2X-1)$

$\varphi : \mathbb{Z}[X] \longrightarrow \mathbb{Q}$

$P(X) \longmapsto P(\frac{1}{2})$

$\ker\varphi = \{ P(X) \in \mathbb{Z}[X] / P(\frac{1}{2}) = 0 \}$

$2 \times \frac{1}{2} - 1 = 0$ donc $2X-1 \in \ker\varphi$

$(2X-1) \subset \ker\varphi$

• Mq $P(X) \in (2X-1)$

Effectuons la div eucl de $P(X)$ par $2X-1$ dans $\mathbb{Q}[X]$ (Euclidien car $\mathbb{Q}$ un corps)

$P(X) = (2X-1) Q(X) + R(X)$

$Q(X), R(X) \in \mathbb{Q}[X]$

$\deg R < \deg(2X-1) = 1$

$\Rightarrow R(X) =$ cste $\in \mathbb{Q}$

$R(X) = 0$ car $P(\frac{1}{2}) = 0$

Mq $Q(X) \in \mathbb{Z}[X]$

$a_0 + a_1 X + a_2 X^2 + \dots + a_n X^n = (2X-1)(b_0 + b_1 X + b_2 X^2 + \dots + b_{n-1} X^{n-1}), b \in \mathbb{Q}$

on veut Mq $b \in \mathbb{Z}$

$\Rightarrow \begin{cases} -b_0 = a_0 \Rightarrow b_0 = -a_0 \in \mathbb{Z} \\ a_1 = 2b_0 - b_1 \Rightarrow b_1 = 2b_0 - a_1 \\ \qquad = -2a_0 - a_1 \in \mathbb{Z} \\ \vdots \end{cases}$

$b_i \in \mathbb{Z}$ et $Q(X) \in \mathbb{Q}[X]$

$P(X) = (2X-1) \underbrace{Q(X)}_{\in \mathbb{Z}[X]}$

$\ker\varphi \subset (2X-1)$

$\mathbb{Q} = \{P(\frac{1}{2}) \mid P \in \mathbb{Z}[X]\}$

$= \mathbb{Z}[\frac{1}{2}] \subsetneq \mathbb{Q}$

$\mathbb{Z}[\frac{1}{2}] \overset{\text{exple}}{=} 5 + \frac{1}{2} + 6 \times (\frac{1}{2})^2 + 4 \times (\frac{1}{2})^3$

$P \longmapsto P(\frac{1}{2})$

$\mathbb{Z}[X] \xrightarrow{\varphi} \mathbb{Q}$

$\mathbb{Z}[X] \twoheadrightarrow \mathbb{Z}[\frac{1}{2}] = \mathrm{Im}\,\varphi$

$\mathbb{Z}[X]/(2X-1) \cong \mathrm{Im}\,\varphi$

$= \mathbb{Z}[X]/\ker\varphi$

$P \longmapsto f(P) = P(\frac{1}{2})$

$\mathbb{Z}[X] \xrightarrow{f} \mathbb{Z}[\frac{1}{2}]$

$\exists\, \psi : \mathbb{Z}[\frac{1}{2}] \to \mathbb{Z}[X]/(2X-1)$

$\mathbb{Z}[X]/(2X-1)$

Car $(2X-1) \subset \ker f$

Construire $\psi : \mathbb{Z}[\frac{1}{2}] \to \frac{\mathbb{Z}[X]}{(2X-1)}$

$\psi \circ \varphi = id$, $\frac{1}{2} \longmapsto \overline{X}$

$\varphi \circ \psi = id$

$\star\ \mathbb{R}[X]/(X^2+1) \cong \mathbb{R}[i] \overset{\text{def}}{=} \{P(i) \mid P(X) \in \mathbb{R}[X]\}$

$i^k \in \{1, -1, i, -i\}$

$= \mathbb{C}$

$5i^4 + 6i^2 - 4i = 5 - 6 - 4i$

$= -1 - 4i$

soit $\varphi : \mathbb{R}[X] \longrightarrow \mathbb{C}$, $P(X) \longmapsto P(i)$

$\varphi(X^2+1) = 0$

$\Rightarrow (X^2+1) \in \ker\varphi$

$P \in \ker\varphi \Rightarrow P(i)$ et $P(-i) = 0$

$\Rightarrow (X^2+1) \mid P(X)$ (div dans $\mathbb{R}[X]$ car $\mathbb{R}$ corps)

$\Rightarrow P \in (X^2+1)$

Soit $z \in \mathbb{C}$, $z = a+ib$ $a, b \in \mathbb{R}$

cherchons $P \in \mathbb{R}[X] \mid P(i) = z$

il suffit de prendre

$P(X) = a + bX$

$P(i) = a + bi = z$

$\star\ \mathbb{Z}[X]/(X^2+1)$

$\varphi : \mathbb{Z}[X] \longrightarrow \mathbb{C}$

$P(X) \longmapsto P(i)$

$(X^2+1) \subset \ker\varphi$

M $\ker \varphi \subset (x^2+1)$

Soit $P \in \ker \varphi \Rightarrow P(x) = 0$
Coefficient dominant de x^2+1 est $1 \in \mathbb{Z}^\times$

$\Rightarrow \exists Q(x), R(x) \in A[x]$ tq

$P(x) = (x^2+1)Q(x) + R(x)$

avec $\deg R < 2$

$\Rightarrow P(x) = (x^2+1)Q(x) + ax + b$

$P(i) = ai + b$
$P(i) = 0 \Rightarrow ai + b = 0$
$\Rightarrow a = 0$ et $b = 0$

$\Rightarrow P \in (x^2+1)$

$\mathbb{Z}[x] \subseteq \mathbb{Z}[i]$

$* \ \mathbb{Z}[x]/(x^2+x+1) \cong \mathbb{Z}[j]$

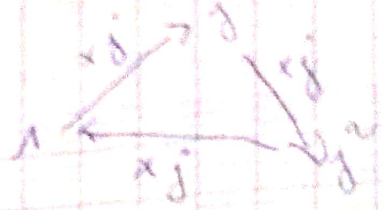
$\| $

$\{ P(j), P \in \mathbb{Z}[x] \}$

$j \in \{1, j, j^2\}$

$| \ j + j + 1 = 0$

$\mathbb{Z}[j] = \{ a + bj, a, b \in \mathbb{Z} \}$



$* \ \mathbb{Z}[i]/(7+i) \cong \mathbb{Z}/50\mathbb{Z}$

$N(7+i) = 7^2 + 1^2 = 50$

$\overline{7+i} = \overline{0}$
$\overline{7} = -\overline{i}$
$\overline{7}^2 = \overline{-1}$
$\overline{50} = \overline{0}$

$\varphi : \mathbb{Z}[i] \longrightarrow \mathbb{Z}/50\mathbb{Z}$

$a + bi \longmapsto \varphi(a+bi)$
$= a\varphi(1) + b\varphi(i)$
$= a\overline{1} + b\overline{43}$
$= \overline{a + 43b}$

$\varphi(7+i) = \overline{0}$
$\varphi(7) + \varphi(i) = \overline{0}$
$7\varphi(1) + \varphi(i) = \overline{0}$
$7\overline{1} + \varphi(i) = \overline{0}$
$\varphi(i) = -\overline{7} = \overline{43}$

Mq $\ker \varphi = (x^2+1)$

Soit $P \in \ker \varphi \Rightarrow P(x) = 0$
Coefficient dominant de x^2+1 est $1 \in \mathbb{Z}^\times$

$\Rightarrow \exists Q(x), R(x) \in A[x]$ tq

$P(x) = (x^2+1)Q(x) + R(x)$

avec $\deg R < 2$

$\Rightarrow P(x) = (x^2+1)Q(x) + ax + b$

$P(i) = ai + b$
$P(i) = 0 \Rightarrow ai + b = 0$
$\Rightarrow a = 0$ et $b = 0$

$\Rightarrow P \in (x^2+1)$

$\mathbb{Z}[x] \cong \mathbb{Z}[i]$

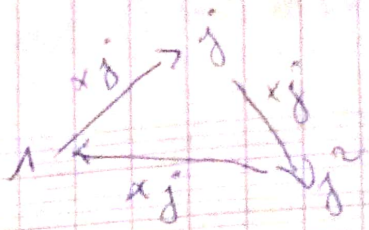
$\# \mathbb{Z}[x]/(x^2+x+1) \cong \mathbb{Z}[j]$

$\| \quad f\ P(j),\ P \in \mathbb{Z}[x]$

$j^k \in \{1, j, j^2\}$

$| \ j + j + 1 = 0$

$\mathbb{Z}[j] = \{ a + bj \mid a, b \in \mathbb{Z} \}$



$\# \mathbb{Z}[i]/(7+i) \cong \mathbb{Z}/50\mathbb{Z}$

$\overline{7+i} = \overline{0}$ | $N(7+i) = 7^2 + 1^2 = 50$

$\overline{7} = -\overline{i}$
$\overline{7}^2 = \overline{-1}$
$\overline{50} = \overline{0}$

$\varphi : \mathbb{Z}[i] \longrightarrow \mathbb{Z}/50\mathbb{Z}$

$a + bi \longmapsto \varphi(a+bi)$
$= a\varphi(1) + b\varphi(i)$
$= a \cdot \overline{1} + b\overline{43}$
$= \overline{a + 43b}$

$\varphi(7+i) = \overline{0}$
$\varphi(7) + \varphi(i) = \overline{0}$
$7\varphi(1) + \varphi(i) = \overline{0}$
$7 \cdot \overline{1} + \varphi(i) = \overline{0}$
$\varphi(i) = -\overline{7} = \overline{43}$

$\mathbb{Z}[i\sqrt{3}] \longrightarrow \mathbb{Z}/50\mathbb{Z}$

$a+ib \longrightarrow f(\beta) = \overline{a+43b}$

① f morphisme
② $\ker f$
③ $\mathrm{Im} f$

soit $\beta = a+ib$ et $\beta' = x+iy \in \mathbb{Z}[i]$

$f(\beta+\beta') = f(a+x+i(b+y))$
$= \overline{a+x+43(b+y)}$
$= \overline{a+43b} + \overline{x+43y}$
$= f(\beta) + f(\beta')$

$\beta\beta' = (a+ib)(x+iy)$
$= (ax-by) + i(ay+bx)$

$f(\beta\beta') = \overline{ax-by+43(ay+bx)}$
$f(\beta)f(\beta') = \overline{(a+43b)(x+43y)}$

$= \overline{(ax+43ay+43bx+1849by)}$

$f(\beta)f(\beta') = \overline{ax-by+43(ay+bx)}$

$f(\beta)f(\beta') = f(\beta)f(\beta')$

* $f(1_{\mathbb{Z}[i]}) = f(1+0i)$
$= \overline{1} = 1_{\mathbb{Z}/50\mathbb{Z}}$

Donc f est un morphisme d'anneaux

② $\ker f$

$f(7+i) = \overline{7+43} = \overline{50} = \overline{0}$

Ainsi $(7+i) \subset \ker f$

Soit $\beta \in \ker f$, avec $\beta = a+ib$

$f(\beta) = 0 \Rightarrow \overline{a+43b} = \overline{0}$
$\Rightarrow a+43b \in 50\mathbb{Z}$
$\Rightarrow \exists k \in \mathbb{Z}$ tq
$a+43b = 50k$
$\Rightarrow a = 50k-43b$
$\Rightarrow \beta = 50k-43b+ib$
$= 50k-50b+7b+ib$
$= 50(k-b)+(7+i)b$
$= (7+i)(7-i)(k-b)+(7+i)b$
$\beta = (7+i)[(7-i)(k-b)+b]$
$\Rightarrow \beta \in (7+i)$

$\Rightarrow \ker f \subset (7+i)$

* Surjective
Soit $\overline{y} \in \mathbb{Z}/50\mathbb{Z}$
Cherchons $\beta \in \mathbb{Z}[i]$ tq

$f(\beta) = \overline{y}$
Prenons $\beta = (y-43)+i$

$f(\beta) = \overline{y-43+43}$
$= \overline{y}$

$\Rightarrow f$ est surjective

$\mathrm{Im} f = \mathbb{Z}/50\mathbb{Z}$

$n \in \mathbb{N}^*$

Exercice 6

1, Décomposition

$P(x) = 6x^n - 6x^{n-1} + 24x^2 - 12x - 12$

$P(1) = 6 - 6 + 24 - 12 - 12$

$P(1) = 0$

$P'(x) = 6nx^{n-1} - 6(n-1)x^{n-2} + 48x - 12$

$P'(1) = 6n - 6n + 6 + 48 - 12$

$= 42 \neq 0$

1 est une racine simple

effectuons la division euclidienne de $P(x)$ par $(x-1)$ dans ~~$\mathbb{Z}[x]$~~ $\mathbb{Q}[x]$

$$\begin{array}{l|l} 6x^n - 6x^{n-1} + 24x^2 - 12x - 12 & x-1 \\ 0 \quad 0 \quad 24x^2 - 12x - 12 & 6x^{n-1} + 24x + 12 \\ \quad\quad 0 \quad 12x - 12 & \\ \quad\quad\quad 0 \quad 0 & \end{array}$$

$P(x) = (x-1)(6x^{n-1} + 24x + 12)$

$= 6(x-1)(x^{n-1} + 4x + 2)$

$\mathbb{Z}/2$

$4^4, 2^2 \times 2$ $\Rightarrow x^{n-1} + 4x + 2$ est irréductible dans $\mathbb{Q}[x]$

$2/1$

De plus

$c(x^{n-1} + 4x + 2) = PGCD(1, 4, 2)$

$= 1$

Donc $x^{n-1} + 4x + 2$ est irréductible dans $\mathbb{Z}[x]$

Par suite

$P(x) = 2 \times 3 (x-1)(x^{n-1} + 4x + 2)$

2, montrons que $x^4 - 10x^3 + 21x^2 - 10x + 1$ est irréductible dans $\mathbb{Z}[x]$.

Considérons $\varphi : \mathbb{Z}[x] \longrightarrow \mathbb{Z}/2\mathbb{Z}$

$P \longmapsto \varphi(P)$

morphisme de réduction modulo p.

$\pi_p : \mathbb{Z}[x] \longrightarrow \mathbb{Z}/p\mathbb{Z}[x]$

$P(x) = \sum_{k=0}^{n} a_k x^k \longmapsto \pi_p(P(x)) = \sum_{k=0}^{n} \overline{a_k} x^k$

$\pi_2 : \mathbb{Z}[x] \longrightarrow \mathbb{Z}/2\mathbb{Z}[x]$

$P(x) \longmapsto \overline{1}x^4 + (\overline{-10})x^3 + \overline{21}x^2 + (\overline{-10})x + \overline{1}$

$= \overline{1}x^4 + \overline{1}x^2 + \overline{1}$

Vérifions si

$\overline{1}x^4 + \overline{1}x^2 + \overline{1} = \pi_2(P)$

est irréductible dans $\mathbb{Z}/2\mathbb{Z}[x]$

$\mathbb{Z}/2\mathbb{Z} = \{\overline{0}, \overline{1}\}$

- $\overline{1}\,\overline{0}^4 + \overline{1}\,\overline{0} + \overline{1} = \overline{1} \neq \overline{0}$
- $\overline{1}\,\overline{1}^4 + \overline{1}\,\overline{1}^2 + \overline{1} = \overline{3} = \overline{1} \neq \overline{0}$

X^4+X^2+1 n'admet pas de racines simples dans $\mathbb{Z}/2\mathbb{Z}$

Supposons
$X^4+X^2+1 = (X^2+aX+b)(X^2+cX+d)$

$= X^4 + (a+c)X^3 + (d+ac+b)X^2 + (ad+bc)X + bd$

$\Rightarrow \begin{cases} a+c=0 & (1) \\ d+ac+b=1 & (2) \\ ad+bc=0 & (3) \\ bd=1 & (4) \end{cases}$

$(1) \Rightarrow b=1=d$ ou $b=d=-1$

$(2) \Rightarrow ac=1$

$(1) \Rightarrow a=c=1$

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

$P(X) = \sum_{k=0}^{n} a_k X^k \in \mathbb{Z}[X] \subset \mathbb{Q}[X]$

$\frac{p}{q}$ PGCD $p \wedge q = 1$ est racine de $P(X)$

$\Rightarrow P\left(\frac{p}{q}\right) = 0$

$\Rightarrow \sum_{k=0}^{n} a_k \left(\frac{p}{q}\right)^k = 0$

$\Rightarrow a_n \frac{p^n}{q^n} + \frac{p^{n-1}}{q^{n-1}} a_{n-1} + \dots + a_0 = 0$

$\Rightarrow a_n p^n + p^{n-1} q a_{n-1} + \dots + a_1 p q^{n-1} + a_0 q^n = 0$

$\Rightarrow p(a_n p^{n-1} + p^{n-2} q a_{n-1} + \dots + a_1 q^{n-1}) = -a_0 q^n$

$\Rightarrow p \mid a_0 q^n$

$\Rightarrow p \mid a_0$ car $p \wedge q = 1$

$\Leftrightarrow a_n p^n = -q(a_{n-1} p^{n-1} + \dots + a_1 p q^{n-2} + a_0 q^{n-1})$

$\Rightarrow q \mid a_n p^n$

$\Rightarrow q \mid a_n$ car $q \wedge p = 1$ (Gauss)

$P(X) = X^4 - 20X^3 + 21X^2 - 10X + 11$

Si $\frac{p}{q}$ est racine de P alors

$p \mid 11$ et $q \mid 1$

donc $P \in \{\pm 1, \pm 11\}$ et $\frac{p}{q} \in \{\pm 1, \pm 11\}$

$\Rightarrow \frac{p}{q} \in \{\pm 1, \pm 11\}$

$P(\pm 1) \neq 0$ et $P(\pm 11) \neq 0$

$\Rightarrow P$ n'admet pas de racine simple

$P \neq (X+\dots)(X^3+\dots)$

Supposons
$P(X) = (X^2+aX+b)(X^2+cX+d)$

$= X^4 + (a+c)X^3 + (b+ac+d)X^2 + (ad+bc)X + bd$

$\Rightarrow \begin{cases} a+c=-20 \\ b+ac+d=21 \\ ad+bc=-10 \\ bd=1 \end{cases}$

$\Rightarrow (b,d) \in \{(1,11),(-1,-11),(1,1),(-1,-1)\}$

* $(b,d) = (1,1)$

$\begin{cases} a+c = -1 \\ ac = 1 \\ 1a+c = -1 \end{cases}$ impossible

* $(b,d) = (-1,-1)$

$\begin{cases} a+c = -1 \\ ac = 1 \\ -1c+a = -1 \end{cases}$ impossible

* $(b,d) = (-1,-1)$

$\begin{cases} a+c = -1 \\ ac = 1 \\ -a-c = -1 \end{cases}$ impossible

* $(b,d) = (-1,-1)$ impossible

Par suite $P(x)$ est irreductible dans $\mathbb{Q}[X]$

Comme $C(P) = 1$ alors P est irreductible dans $\mathbb{Z}[X]$.

3) Factorisons X^5+X+1 dans $\mathbb{Z}[X]$

$P(j) = j^5 + j + 1$

$= j^2 + j + 1 = 0$

Donc $j, \bar{j}$ sont racines de P

la division euclidienne de P par X^2+X+1 dans $\mathbb{Q}[X]$

$$\begin{array}{r|l} X^5+X+1 & X^2+X+1 \\ \hline -X^4-X^3-X & X^3-X^2+1 \\ \hline \end{array}$$

$P(x) = (X^2+X+1)(X^3-X^2+1)$

Vérifions l'irreductibilité de $P_0 = X^3-X^2+1$ dans $\mathbb{Q}[X]$

Supposons que P_0 admet une racine rationnelle $\frac{p}{q}$ avec $p \wedge q = 1$

alors $p/1$ et $q/1$

Donc $p = \pm 1$ et $q = \pm 1$

$\Rightarrow \frac{p}{q} = \pm 1$

$P_0(1) = 1 \neq 0$ $P_0(-1) = -1 \neq 0$

donc P_0 n'admet pas de racine simple.

Donc P_0 est irreductible dans $\mathbb{Q}[X]$

$C(P_0) = PGCD(1,-1,1) = 1$

Par suite P_0 est irreductible dans $\mathbb{Z}[X]$

Donc la factorisat° de P dans $\mathbb{Z}[X]$ et $P(X) = (X^2+X+1)(X^3-X^2+1)$

5) Factorisons $P(x) = X^4 - X^2 + 1$ dans $\mathbb{Z}/n\mathbb{Z}$

Vérifions si $P(x)$ a une racine simple dans $\mathbb{Z}/n\mathbb{Z}$

$\mathbb{Z}/n\mathbb{Z} = \{\bar{0}, \bar{1}, \bar{2}, \dots, \overline{n-1}\}$

$P(\bar{0}) = \bar{0}^4 + \bar{0} + \bar{1} = \bar{1} \neq \bar{0}$

$P(\bar{1}) = \bar{1} + \bar{1} = \bar{0}$

$P(\bar{2}) = \bar{2}^4 + \bar{2} = \bar{0}$

$P(\bar{3}) = \bar{3}^4 + \bar{3} = \bar{0}$

$P(\bar{a}) = \bar{a}^4 + \bar{a} = \bar{a}(\bar{a}^3 + \bar{1}) \neq \bar{0}$

$P(\bar{a}) \neq \bar{0}$

donc P ne possède pas de racines simples dans $\mathbb{Z}/11\mathbb{Z}[X]$

supposons que

$P(X) = (X^2 + aX + b)(X^2 + cX + d)$

$P(X) = X^4 + (a+c)X^3 + (b + ac + d)X^2 + (ad + bc)X + bd$

$$\Rightarrow \begin{cases} a + c = 0 \\ b + ac + d = -1 = 10 \\ bd = 1 \end{cases}$$

$bd = 1 \Rightarrow b, d \in (\mathbb{Z}/11\mathbb{Z})^\times$

$(\mathbb{Z}/11\mathbb{Z})^\times = \{\bar{1}, \dots, \overline{10}\}$

$\Rightarrow (b,d) \in \{(\bar{1},\bar{1}), (\bar{2},\bar{6}), (\bar{3},\bar{4}), (\bar{4},\bar{3}), (\bar{5},\bar{9}), (\bar{6},\bar{2}), (\bar{7},\bar{8}), (\bar{8},\bar{7}), (\bar{9},\bar{5}), (\overline{10},\overline{10})\}$

* $(b,d) = (\bar{1},\bar{1})$

$$\Rightarrow \begin{cases} a + c = \bar{0} \\ ac = \bar{8} \\ a + c = \bar{0} \end{cases}$$

$a^2 + ac = a$

$a^2 + \bar{8} = \bar{0}$

$a^2 = -\bar{8}$

$11 - 8 = 3$

$\Rightarrow 11 = 8 + 3$

$\Rightarrow \overline{2^4} = \bar{5}$

$\Rightarrow \bar{5} = \bar{2}$

$\Rightarrow a^2 = \bar{5}$

$a = \bar{6}$

$c = \bar{5}$

$X^4 - X^2 + 1 = (X^2 + \bar{6}X + \bar{1})(X^2 + \bar{5}X + \bar{1})$ dans $\mathbb{Z}/11\mathbb{Z}[X]$

Exercice 2

$P(X) = X^4 - 10X^2 + 1 \in \mathbb{Q}[X]$

1) Déterminons les racines réelles de P

Posons $X = x^2$

$P(x) = x^2 - 10x + 1$

$P(x) = (x - \sqrt{5 - 2\sqrt{6}})(x + \sqrt{5 - 2\sqrt{6}})$

$\times (x - \sqrt{5 + 2\sqrt{6}})(x + \sqrt{5 + 2\sqrt{6}})$

2) Montrons que P est irréductible dans $\mathbb{Q}$

* les racines simples de P sont toutes irrationnelles donc P ne possède pas de facteurs de deg 1

$P(X) = (X - \alpha)(X + \alpha)(X - \beta)(X + \beta)$

$= (X^2 - \alpha^2)(X^2 - \beta^2)$

$\alpha^2 = 5-2\sqrt{6} \notin \mathbb{Q}$ | $\Rightarrow P(x)$ n'admet pas de racines de deg 2
$\beta^2 = 5+2\sqrt{6} \notin \mathbb{Q}$ |

Mq $\mathbb{Q}[\alpha] = \{a\alpha^3+b\alpha^2+c\alpha+d,$ $a,b,c,d \in \mathbb{Q}\}$

$= \mathbb{Q}\text{-e.v} \langle 1, \alpha, \alpha^2, \alpha^3 \rangle$

$\mathbb{Q}[X] = \{R(\alpha) / R \in \mathbb{Q}[X]\}$

$P(\alpha) = 0 \Rightarrow \alpha^4 - 10\alpha^2 + 1 = 0$
$\Rightarrow \alpha^4 = 10\alpha^2 - 1$
$\Rightarrow \alpha^5 = 10\alpha^3 - \alpha$

Donc $\forall k \geq 4 \quad \alpha^k \in \langle 1, \alpha, \alpha^2, \alpha^3 \rangle$

$R \in \mathbb{Q}[X]$
$\Rightarrow R(\alpha) = \sum_{k=0}^{n} a_k \alpha^k$ $\in \langle 1, \alpha, \dots \alpha^3 \rangle$
$= a_0 + a_1\alpha + a_2\alpha^2 + a_3\alpha^3 + \sum_{k=4}^{n} a_k \alpha^k$

$= \underbrace{a_0 + a_1\alpha + a_2\alpha^2 + a_3\alpha^3}_{\langle 1, \alpha, \dots, \alpha^3 \rangle} + \underbrace{\sum_{k=4}^{n} a_k \alpha^k}_{\langle 1, \alpha, \dots \alpha^3 \rangle}$

$R(\alpha) \in \langle 1, \alpha, \dots, \alpha^3 \rangle$

Autre méthode
$T = PQ + R$, $\deg R < \deg P = 4$

$T(\alpha) = P(\alpha)Q(\alpha) + R(\alpha)$

$T(\alpha) = \dots$

$f : \mathbb{Q}[X] \longrightarrow \mathbb{Q}[\alpha]$
$T \longmapsto f(T) = T(\alpha)$

* f morphisme d'anneaux
* $\ker f = (P)$
* f surj
* $\mathbb{Q}[X]/(P) \simeq \mathbb{Q}[\alpha]$

- $(P) \subset \ker f$?

$f(P) = P(\alpha) = 0 \Rightarrow P \in \ker f$
$\Rightarrow (P) \subset \ker f$

$T \in \ker f \Rightarrow f(T) = 0$
$\| $
$T(\alpha)$

Div Eucl de T par P
$T = PQ + R$
$\deg R < \deg P$

$\deg R < 4$

$R = ax^3 + bx^2 + cx + d$

$0 = R(\alpha) = a\alpha^3 + b\alpha^2 + c\alpha + d$

$\Rightarrow a = b = c = d = 0$
Car $\langle 1, \alpha, \alpha^2, \alpha^3 \rangle$ $\mathbb{Q}$-libre

$\Rightarrow R(X) = 0$
$\Rightarrow T = PQ \in (P)$

$\mathbb{Q}[X] \neq \mathbb{Q}[X]/(P)$

Soit $\overline{T} \in \mathbb{Q}[X]/(P)$

avec $\overline{T} \neq \overline{0} = (P)$

$(\overline{T} = \overline{0} \Leftrightarrow T \in (P))$

$\overline{T} \neq \overline{0} \Leftrightarrow T \notin (P)$

i.e T n'est pas multiple de P.

$\begin{cases} P \wedge T \\ P \text{ irréductible dans } \mathbb{Q}[X] \\ P \wedge T = 1 \\ \exists U, V \in \mathbb{Q}[X] \text{ tq} \end{cases}$

$PU + TV = 1$ (Bezout)

$\Rightarrow \overline{P}\overline{U} + \overline{T}\overline{V} = \overline{1}$

$= \overline{0}\overline{U} + \overline{T}\overline{V} = \overline{1}$

$\Rightarrow \overline{T}\overline{V} = \overline{1}$ donc

$\overline{T} \in \left(\mathbb{Q}[X]/(P)\right)^{\times}$

Conclusion $\mathbb{Q}[X]/(P)$ Corps

$=$

$\mathbb{Q}(\alpha)$