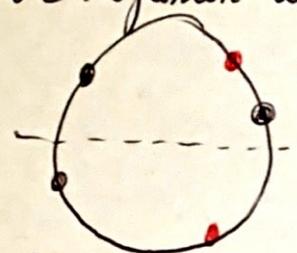


\rightsquigarrow L'identité stabilise tous les colliers: $3^5 = 243$ $\text{ordre}(\tau_1) = \text{ppcm}(\text{ordre}(15347), \text{ordre}(26))$
 \rightarrow Une rototo stabilise uniquement les colliers monochromes
 $X(n) = 3.$ $= \text{ppcm}(5, 2) = 10.$

\rightarrow Une réflexion stabilise les colliers symétriques



$$X(s) = 27$$

$$N = \frac{1 \times 243 + 9 \times 3 + 5 \times 27}{16} = \frac{243 + 27 + 135}{16} = 39$$

Groupe Symétrie

$$\text{Ex 23} \quad \tau_1 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 1 & 4 & 3 & 2 & 7 & 8 & 6 & 5 \end{pmatrix}, \quad \tau_2 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 5 & 6 & 4 & 7 & 3 & 2 & 1 \end{pmatrix}$$

a) Decompose τ_1 & τ_2 en \prod cycles à supports disjoints

$$\tau_1 = (24)(5768), \quad \tau_2 = (15347)(26)$$

b) et ordre & signature de τ_1 & τ_2 .

$\text{ordre}(\sigma) = \text{ppcm}(\text{ordre}(\text{tg } R \text{ cycles}))$

$$\begin{aligned} \text{ordre}(\tau_1) &= \text{ppcm}(\text{ordre}(24), \text{ordre}(5768)) \\ &= \text{ppcm}(2, 4) = 4. \end{aligned}$$

$\text{signature}(\tau) = \varepsilon(\tau) ?$

$$\varepsilon(\tau_1) = \varepsilon((24)) \times \varepsilon((5768)) = (-1)^4 \times (-1)^3 = 1$$

$$\varepsilon(\tau_2) = \varepsilon((15347)) \times \varepsilon((26)) = (-1)^4 \times (-1)^2 = -1$$

c) calculer τ_1^{175} & τ_2^{1999}

$$\tau_1^{175} = \tau_1^{175} [4]$$

$$175 = 4 \times 43 + 3$$

$$= (\tau_1^4)^{43} \times \tau_1^3 = (\text{Id})^{43} \times \tau_1^3 = \tau_1^3$$

$$= (24)^3 \times (5768)^3$$

$$= (24) \times (5867) \quad \text{et j'envoie le nbr } \frac{4}{3} \text{ le } 3^{\text{e}} \text{ nbr suivant}$$

$$\tau_1^{175} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 1 & 4 & 3 & 2 & 8 & 7 & 5 & 6 \end{pmatrix}$$

on regarde dans le sens

$$\tau_2^{1999} = ?$$

$$1999 = 6 \times 200 - 4$$

$$\tau_2^{1999} = (\tau_2^{10})^{200} \times \tau_2^{-4} = \tau_2^{-4} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 7 & 6 & 5 & 3 & 1 & 2 & 4 \end{pmatrix}$$

Ex 27 a) Mq S_n est engendré par les $n-1$ transpositions $(12), (13), \dots, (1n)$

$$\boxed{m=2} \quad S_2 = \{\text{id}, (12)\} = \langle (12) \rangle.$$

$$\boxed{m=3} \quad S_3 = \{\text{id}, (12), (23), (13), (123), (132)\}$$

$$(12) \circ (13) = (132), \quad (123) = (13) \circ (12)$$

$$(23) = (12) \circ (13) \circ (12)$$

Raisonnons Par Récurrence / Supposons $m > 3$:

Supposons S_{m-1} est engendré par $(12), \dots, (1, m-1)$
Soit $\tau \in S_m$:

$$\bar{\tau} = (1, m)(1, \tau(m)) \tau$$

$$\text{alors } \bar{\tau}(m) = (1, m) \circ (1, \tau(m)) \circ (\tau(m))$$

$$\bar{\tau}(m) = (1, m)(1) = m$$

$$\text{Dc } \bar{\tau} \in S_{m-1} = \langle (12), \dots, (1, m-1) \rangle$$

$$\tau = (1, \tau(m))(1, m) \bar{\tau}$$

$$\tau \in \langle (1, 2), \dots, (1, m-1), (1, m) \rangle$$

Dc (PR) S_m est engendré par $(12), \dots, (1m)$

$$\boxed{M2} \quad (i, j) = (1, i)(1, j)(-1, i)$$

et les transpositions engendrent S_m , de S_m est engendré par $(1, 2), \dots, (1, m)$.

Ex 27

a) Mq S_n est engendré par les
n-1 transpositions $(1,2), (1,3), \dots, (1,n)$

$\boxed{m=2}$

$$S_2 = \{ \text{id}, (1,2) \} = \langle (1,2) \rangle .$$

et les transpositions engendrant S_m , de S_m
est engendré par $(1,2), \dots, (1,n)$.

$\boxed{m=3}$

$$S_3 = \{ \text{id}, (1,2), (2,3), (1,3), (1,2,3), (1,3,2) \}$$

$$(1,2) \circ (1,3) = (1,3,2), \quad (1,2,3) = (1,3) \circ (1,2)$$

$$(1,3) = (1,2) \circ (1,3) \circ (1,2)$$

Raisonnée Par Recurrence

Supposons $m \geq 3$:

$$\text{Soit } \sigma \in S_m, \text{ considérons } \overline{\sigma} = (m-1, n) \dots (\sigma(m)-1, \sigma(m)+2) (\sigma(m), \sigma(m)+1) \sigma$$

Supposons S_{m-1} est engendré par $(1,2), \dots, (1,m-1)$
soit $\tau \in S_{m-1}$:

$$\begin{aligned} \overline{\sigma} &= (m-1, n) \circ \dots \circ ((\sigma(m)+1, \sigma(m)+2) \circ (\sigma(m), \sigma(m)+1) \sigma) \\ &= (m-1, n) \circ \dots \circ ((\tau(m_1)+1, \tau(m_1)+2) \circ (\tau(m_1), \tau(m_1)+1)). \\ &\vdots \\ \overline{\sigma} &= (1, m)(1, \tau(m)) \circ \dots \\ &\quad \vdots \\ &= \overline{\sigma}(m) = n \end{aligned}$$

Or

$$\overline{\sigma}(m) = (1, m) \circ (1, \tau(m)) \circ (\tau(m))$$

$$\overline{\sigma}(m) = (1, m)(1) = m$$

Or $\overline{\sigma} \in S_{m-1} = \langle (1,2), \dots, (1,n-1) \rangle$

Toute permute de que les $n-1$ premiers sont $1, \dots, n-1$
de P HDR, $\overline{\sigma} \in \langle (1,2), \dots, (n-1)n \rangle$

$$\sigma = (1, \sigma(m))(1, m)$$

$$\sigma \in \langle (1,2), \dots, (1,n-1), (1,n) \rangle$$

Or PR est engendré par $(1,2), \dots, (1,n)$

(38)

$\boxed{M2}$ $(i,j) = (1,i)(1,j)(-1,i)$

$\boxed{M3}$

$\boxed{M4}$

$\boxed{M5}$

$\boxed{M6}$

$\boxed{M7}$

$\boxed{M8}$

$\boxed{M9}$

$\boxed{M10}$

$\boxed{M11}$

$\boxed{M12}$

$\boxed{M13}$

$\boxed{M14}$

$\boxed{M15}$

$\boxed{M16}$

$\boxed{M17}$

$\boxed{M18}$

$\boxed{M19}$

$\boxed{M20}$

$\boxed{M21}$

$\boxed{M22}$

$\boxed{M23}$

$\boxed{M24}$

$\boxed{M25}$

$\boxed{M26}$

$\boxed{M27}$

$\boxed{M28}$

$\boxed{M29}$

$\boxed{M30}$

$\boxed{M31}$

$\boxed{M32}$

$\boxed{M33}$

$\boxed{M34}$

$\boxed{M35}$

$\boxed{M36}$

$\boxed{M37}$

$\boxed{M38}$

$\boxed{M39}$

$\boxed{M40}$

$\boxed{M41}$

$\boxed{M42}$

$\boxed{M43}$

$\boxed{M44}$

$\boxed{M45}$

$\boxed{M46}$

$\boxed{M47}$

$\boxed{M48}$

$\boxed{M49}$

$\boxed{M50}$

$\boxed{M51}$

$\boxed{M52}$

$\boxed{M53}$

$\boxed{M54}$

$\boxed{M55}$

$\boxed{M56}$

$\boxed{M57}$

$\boxed{M58}$

$\boxed{M59}$

$\boxed{M60}$

$\boxed{M61}$

$\boxed{M62}$

$\boxed{M63}$

$\boxed{M64}$

$\boxed{M65}$

$\boxed{M66}$

$\boxed{M67}$

$\boxed{M68}$

$\boxed{M69}$

$\boxed{M70}$

$\boxed{M71}$

$\boxed{M72}$

$\boxed{M73}$

$\boxed{M74}$

$\boxed{M75}$

$\boxed{M76}$

$\boxed{M77}$

$\boxed{M78}$

$\boxed{M79}$

$\boxed{M80}$

$\boxed{M81}$

$\boxed{M82}$

$\boxed{M83}$

$\boxed{M84}$

$\boxed{M85}$

$\boxed{M86}$

$\boxed{M87}$

$\boxed{M88}$

$\boxed{M89}$

$\boxed{M90}$

$\boxed{M91}$

$\boxed{M92}$

$\boxed{M93}$

$\boxed{M94}$

$\boxed{M95}$

$\boxed{M96}$

$\boxed{M97}$

$\boxed{M98}$

$\boxed{M99}$

$\boxed{M100}$

c) Posons $t = (1\ 2)$ & $p = (1\ 2 \dots m)$.

Mq $\{t, p\}$ engendre S_m .

On a $t = (1\ 2)$.

$$ptp^{-1} = (2, 3) \quad \dots \quad p^{m-2}t^{m-2} = (m-1, m)$$

$$p^2t^2p^{-2} = (3, 4)$$

En, on vient de montrer les transpositions $(1, 2), \dots, (m-1, m)$ engendent S_m .

Done $S_m = \langle t, p \rangle$.

Ex 31 Soit G \textcircled{g} , H \textcircled{g} de G . Ds chq x ,

vérifier si \textcircled{g} agit bien d'une act, déterminer les stabilisat \textcircled{b} , les orbites, & élire équoclasse,

a) G agit sur lui-m^ñ p translat à gauche: $g \cdot x = g^n$.

► **NEUTRE**: $1_G \cdot x = 1_G x = x$

► **ASSOCIATIVITÉ**: $g \cdot (h \cdot x) = g \cdot (hx) = ghx = (gh) \cdot x$.

⇒ C'est bien une act de \textcircled{g} de G à lui-m^ñ.

(39) g^6

• Stabilisat \textcircled{b}

Soit $x \in G$,

$$\text{Stab}_x = \{g \in G \mid g \cdot x = x\} = \{g \in G \mid gx = x\}$$

$\text{Stab}_x = \{1_G\}$

• Orbites:

soit $x \in G$,

$$\text{Orb}_x = \{g \cdot x \mid g \in G\} = \{g^n \mid g \in G\}$$

soit $y \in G$, $y = (y^{-1})x = (y^{-1}) \cdot x \in \text{Orb}_x$

Done $\boxed{\text{Orb}_x = G}$

• Equal aux classes:

$$\text{hyp: } \frac{|G|}{|\text{Orb}_x|} \times |\text{Orb}_x| = |G| \quad \text{on appelle } x \text{ représentant de l'équoclass}$$
$$|G| = \sum_{i=1}^n |\text{Orb}_{x_i}| = \sum_{i=1}^n |\text{Orb}_{x_i}| = \sum_{i=1}^n |\text{Stab}_{x_i}|$$

$$\downarrow |G| = |G| = |G/\text{Orb}|$$

b) G agit sur lui-même par conjugaison: $g \cdot x = gng^{-1}$

Action

neutre associatif

- $1_G \cdot x = 1_G x 1_G^{-1} = x$
- $g \cdot (h \cdot x) = g \cdot (hnh^{-1}) = ghnh^{-1}g^{-1}$
 $= (gh)x(gh)^{-1}$
 $= (gh) \cdot x.$

C'est bien une action de G sur lui-même.

Stabilité

Soit $x \in G$,

$$\text{Stab}_x = \{g \in G, g \cdot x = x\}$$

$$= \{g \in G, gag^{-1} = x\} =$$

$$\boxed{\text{Stab}_x = \{g \in G, gx = xg\}}$$

$= Z_G(x)$: la centralisation de x .

Orbites

$$\text{Orb}_x = \{g \cdot x \mid g \in G\} = \{gxg^{-1} \mid g \in G\}$$

Orbite de x est l'ensemble des éléments
 $g \cdot x = gng^{-1} = x$ conjugués à x , i.e. sa classe

math
ord
algébr

égaux aux classes.

$$|X| = \sum_{i=1}^n |\Omega_{x_i}| = \sum_{i=1}^n |G/\text{stab}_{x_i}|$$

$$|G| = \sum_{i=1}^n |\text{classe de conjugaison de } x_i|$$

$$|G| = \sum_{i=1}^n |G/Z_G(x_i)|.$$

c) G agit par conjugaison sur l'ens des conjugués de H .

$$\text{Soit } g \cdot (g^1 H g^{1-1}) = g(g^1 H g^{1-1})g^{-1}$$

Ac

$$g \cdot (g^1 H g^{1-1}) = (gg)H(gg)^{-1} \quad \text{de c'est bien pris un conjugué de } H.$$

$$\bullet 1_G(g^1 H g^{1-1}) = 1_G g^1 H g^{1-1} 1_G^{-1} = g^1 H g^{1-1}$$

$$\bullet g \cdot (g^1 \cdot g^{11} H g^{11-1}) = g(g^1(g^{11} H g^{11-1})g^{1-1})g^{-1} \\ = (gg')(g^{11} H g^{11-1})(gg')^{-1}$$

$$= (gg'), (g^{11} H g^{11-1}).$$

Stabilisateur

soit $gHg^{-1} \in X$,

$$S_{stab}(gHg^{-1}) = \{ g' \in G, g' \cdot (gHg^{-1}) = gHg^{-1} \}$$

$$= \{ g' \in G, g'gHg^{-1}g'^{-1} = gHg^{-1} \}$$

$$= N_G(gHg^{-1}) \text{ nous allons montrer.}$$

$$\textcircled{5} \text{ Normalisatrice } N_G(H) = \{ g \in G, gHg^{-1} = Hg \}$$

Orbites:

soit $gHg^{-1} \in X$,

$$\mathcal{O}_{gHg^{-1}} = \{ g' \cdot (gHg^{-1}) \text{ pour } g' \in G \}$$

$$= \{ g'(gg^{-1})g'^{-1} \text{ pour } g' \in G \}$$

$$= \{ (g'g)H(g'g)^{-1} \text{ pour } g' \in G \}$$

$$\text{On note } g'' \in G, g'' = (g'g^{-1})g$$

$$\text{Donc } g''Hg''^{-1} \in \mathcal{O}_{gHg^{-1}}$$

Q.C l'orbite est X , l'en de tous les conjugués de H .

Égalité aux classes:

$$|X| = \sum_{i=1}^n |\mathcal{O}_{x_i}| = \sum_{i=1}^n |G/S_{stab}(x_i)|$$

$$\text{nb: } \# \text{ de conjugués de } H = |G/S_{stab}(H)| = [G : N_G(H)]$$

\textcircled{6} soit $\varphi: G \rightarrow H$ M.D.F.

alors $\bar{\varphi}: G/\ker \varphi \xrightarrow{\sim} \text{Im } \varphi$ est un isomorphisme

\textcircled{7} $N_G(\bar{\varphi})$ est bien defined

\rightarrow soit $g, g' \in G$ tq $gg'^{-1} \in \ker \varphi$

$$\text{alors } \varphi(gg'^{-1}) = 1_H = \varphi(g)\varphi(g')^{-1} = 1_H \Rightarrow \varphi(g) = \varphi(g')$$

et $\bar{\varphi}$ est bien définie, et elle est image de $\text{Im } \varphi$

\rightarrow soit $\bar{g}, \bar{g}' \in G/\ker \varphi$;

$$\bar{\varphi}(\bar{g} \cdot \bar{g}') = \varphi(gg') = \varphi(g) \cdot \varphi(g') = \bar{\varphi}(\bar{g}) \bar{\varphi}(\bar{g}')$$

c'est bien un M.D.F.

\rightarrow soit $h \in \text{Im } \varphi, \exists g \in G$ tq $h = \varphi(g) = \bar{\varphi}(\bar{g}) \in \text{Im } \bar{\varphi}$

$\bar{\varphi}$ est bien surjective.

\Leftrightarrow si $\bar{\varphi}(\bar{g}) = 1_H \Rightarrow \varphi(g) = 1_H$ de $g \in \ker \varphi$ dc $\bar{g} = \bar{1}_G$

$\Rightarrow \bar{\varphi}$ bien injective

UNIVERSITÉ DE LILLE

Enseignant responsable: Pierre DÈBES

Filière: Licence 5ème Semestre

Matière: M51

Année universitaire: 2021/2022

Date, heure et lieu: vendredi 19 novembre 2021 à 10h au Bâtiment A5

Durée de l'épreuve: 2 heures

8h

Chacune des deux parties devra être rédigée sur une copie différente.

Ni calculatrice ni documents.

Le barême est donné à titre indicatif.

UNE ATTENTION PARTICULIÈRE SERA PORTÉE
À LA RIGUEUR ET LA PRÉCISION DE LA RÉDACTION.

PARTIE I (cours)

Question 1 [1,5 pts]: Donner la définition

- (a) d'un ensemble infini,
(b) d'un ensemble dénombrable.

Question 2 [3,5 pts]: Soient G un groupe et H un sous-groupe de G

(a) Donner la définition de la relation de congruence à gauche sur G modulo H .

(b) Sans justifier que cette relation est une relation d'équivalence sur G , montrer que toutes ses classes d'équivalence sont des ensembles équivalents à H .

→ (c) Application: énoncer et démontrer le théorème de Lagrange pour un groupe G fini.

Question 3 [3,5 pts]: (a) Donner

(a-1) la définition de l'action d'un groupe G sur un ensemble X ,

(a-2) pour $x \in X$, les définitions de l'orbite de x et du stabilisateur de x sous l'action de G .

(b) Supposant G et X finis, donner et démontrer la formule liant, pour $x \in X$ donné, les cardinaux du groupe G , de l'orbite de x et du stabilisateur de x sous l'action de G .

Question 4 [1,5 pts]: Enoncer un des trois "théorèmes d'isomorphisme" de la théorie des groupes.

T.S.V.P.

$$\text{6)} \quad \varphi: G \rightarrow G', \quad \forall g \in G \quad \text{des 3: isom} \\ \bar{\varphi} = \varphi \circ \varphi^{-1}: G/G' \rightarrow G'/G$$

$$G/G' \cong G'/G$$

$$\varphi: G \rightarrow G', \quad \text{6) groupe, } \mathbb{K} \text{ (sous) de } G, \quad \mathbb{K}' \text{ (sous) de } G'$$

$$G/\mathbb{K} \cong G'/\mathbb{K}'$$

$$\sigma(g_1 \dots g_p) \sigma^{-1} = (\sigma(1) \dots \sigma(p))$$

PARTIE II (exercices) + Q

Exercice 1 [3,5 pts]: Soient G un groupe fini et p un nombre premier divisant l'ordre de G . Soit X l'ensemble des p -uplets $(g_1, \dots, g_p) \in G^p$ tels que le produit $g_1 \dots g_p$ vaut 1 (l'élément neutre de G). On note σ le p -cycle $(1 \ 2 \ \dots \ p)$ et $\rho : \langle \sigma \rangle \rightarrow \text{Bij}(X)$ l'action du groupe engendré par σ (dans le groupe symétrique S_p) sur l'ensemble X définie par

$$\rho(\sigma^k)(g_1, \dots, g_p) = (g_{\sigma^k(1)}, \dots, g_{\sigma^k(p)}) \quad ((g_1, \dots, g_p) \in X, k \in \mathbb{Z}).$$

- (a) Déterminer le cardinal de X en fonction de p .
- (b) Quels sont les points fixes de l'action ρ ? Stab_x .
- (c) Montrer que G possède un élément d'ordre p .

Exercice 2 [3 pts]: Soit G un groupe. On note $\varphi : G \rightarrow \text{Aut}(G)$ le morphisme de conjugaison sur G , qui, à tout élément $g \in G$ associe l'automorphisme $\varphi_g : G \rightarrow G$ défini par $\varphi_g(x) = gxg^{-1}$ ($x \in G$).

- (a) Quel est le noyau $\ker(\varphi)$ du morphisme φ ?
- (b) Montrer que le centre $Z(G)$ du groupe G est un sous-groupe distingué de G . (On rappelle que $Z(G) = \{x \in G \mid xy = yx \text{ pour tout } y \in G\}$).
- (c) Montrer que si le groupe quotient $G/Z(G)$ est monogène, alors le groupe G est abélien.

Exercice 3 [3,5 pts]: Soient G un groupe et \mathcal{S} le sous-ensemble de G constitué des éléments d'ordre 2.

- (a) Montrer que le sous-groupe $\langle \mathcal{S} \rangle \subset G$ engendré par \mathcal{S} est distingué. (Indication: on montrera d'abord que l'ensemble \mathcal{S} est stable par conjugaison, puis on le montrera pour le groupe $\langle \mathcal{S} \rangle$).
- (b) Montrer que si G est d'ordre pair, alors $\mathcal{S} \neq \emptyset$.
- (c) On suppose ici que le groupe G est d'ordre pair et est un groupe simple. Montrer que G est engendré par ses éléments d'ordre 2.

Hdg Δ^6
 $\mathcal{H} \subset Z(G)$
 dc
 $2(6) + \text{grd}$
 n

$\text{max } \langle \mathcal{S} \rangle = \{a^k, k \in \mathbb{Z}\} \text{ si } G \text{ monogène}$
 $\langle \mathcal{S} \rangle = \{a^n, n \in \mathbb{N}\}$.

$\langle \mathcal{S} \rangle = \{a^2, a \in \mathcal{S}\}$
 $\langle \mathcal{S} \rangle = \{a^2\}$ $\Rightarrow G \text{ commutatif}$.

$$[G:H].|H|=|G|$$

$$|H| \Big| \frac{|G|}{d^{n_{ab}}}$$

$|G|=2k$
 \mathcal{S} ordre 2
 $G/\langle a^2 \rangle \cong \text{Dmp. } \langle a^2 \rangle \cong G$
 $a^2 = e$
 $G/\langle 2(6) \rangle \cong G$
 stabil.

$x \in \ker \varphi \text{ si } \varphi(x) = e'$
 $gxg^{-1} = e'$
 $\boxed{gx = g}$

$$G / \langle a^2 \rangle$$

$a \cdot x = x$
 $a^2 = e$
 $\varphi(ab^{-1}) = \varphi(a)\varphi(b)^{-1}$
 $\varphi(a) = \varphi(b)$

$$g'g'' = g''g'$$

$x^{ab^{-1}} = x$
 $x^b = x^a$
 $x^a = x^b$

TD-3 - Anneau

Ex 1 soit A l'ens des appli $f \in C^0([0,1], \mathbb{R})$
 tq $f(0) = f(1)$.

a) Mg A (muni de la somme & du produit des f.s) est un anneau commutatif.

b) L'anneau A est-il intègre?

c) Vérifier $I = \{f \in A, f(\frac{1}{2}) = 0\}$ est un idéal de A . Est-il principal?

a) Mg A est stable par \oplus & \otimes : \leftarrow

soit $f, g \in A$,

• $f+g \in C^0([0,1], \mathbb{R})$ et

$$(f+g)(0) = f(0) + g(0) = f(1) + g(1) = (f+g)(1).$$

• $f \otimes g \in C^0([0,1], \mathbb{R})$ &

$$(fg)(0) = f(0)g(0) = f(1)g(1) = (fg)(1)$$

Donc $f+g, fg \in A$.

Mg $(A, +)$ est \textcircled{g} abélien

L'addit. sur A est l'addit. sur \mathbb{R} point par point. Comme $(\mathbb{R}, +)$ est associatif et commutatif, c'est aussi le cas cas pour $(A, +)$.

Le neutre est $0_A : x \mapsto 0$, qst bien cont & $0_A(0) = 0_A(1) = 0$

$$\text{En effet, } (f + 0_A)(x) = f(x) + 0_A(x) = f(x)$$

L'inverse de f est $-f : x \mapsto -f(x)$.

$$\text{En effet, } (f + (-f))(x) = f(x) - f(x) = 0.$$

$$\text{Donc } f + (-f) = 0_A.$$

Donc $(A, +)$ est \textcircled{g} abélien.

Mg (A, \times) est un monoïde (^{associatif}_{+ neutre}) commutatif

L'associativité & la commutativité découlent de celles de (\mathbb{R}, \times) .

Le neutre est $1_A : x \mapsto 1$, cont & tq $1_A(0) = 1_A(1) = 1$

$$(f \cdot 1_A)(x) = f(x) \cdot 1_A(x) = f(x)$$

Donc (A, \times) est bien un monoïde commutatif

• \times est distributive sur $+$

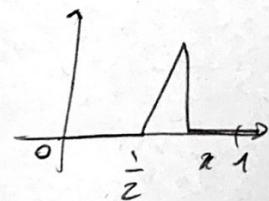
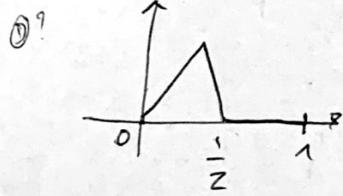
$$\begin{aligned}(f(g+h))(x) &= f(x)(g(x) + h(x)) \\&= f(x)g(x) + f(x)h(x) \\&= (fg + fh)(x).\end{aligned}$$

Donc $(A, +, \times)$ est bien un anneau commutatif.

b) Construisons $f, g \in A$ tels que $fg = 0$,

i.e. $\forall x \in [0, 1]$, $f(x)g(x) = 0$.

De plus en chaque x , une des 2 fonctions est nulle,
mais pour chacune, \exists point où elle ne
s'annule pas.



DC A pas intégre.

\times est distributive sur +

$$(f(g+h))(x) = f(x)(g(x) + h(x)) = f(x)g(x) + f(x)h(x)$$

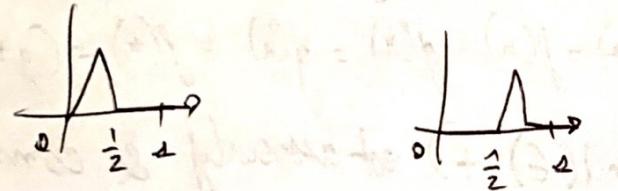
$$= (fg + fh)(x)$$

Donc $(A, +, \times)$ est bien anneau commutatif.

②) Construisons $f, g \in A \setminus \{0\}$ tq $fg = 0$,

$$\text{si } \forall x \in [0,1], f(x)g(x) = 0.$$

De ce que dans \mathbb{R} , une des 2 fonctions est nulle, mais pour chacune, \exists point où elle ne s'annule pas.



De A pas intègre.

I idéal de A si $\begin{cases} (I, +) \text{ est } (A, +) \\ \forall a \in A, \forall i \in I, ai \in I. \end{cases}$

I idéal ppf de A si $\forall n \in A, (n) = \{an, a \in A\}$.

c) Vérifier $I = \{f \in A, f(\frac{1}{2}) = 0\}$ est un idéal de A . Est-il principal ?

$$\text{soit } f, g \in I, (f+g)(\frac{1}{2}) = f(\frac{1}{2}) + g(\frac{1}{2}) = 0$$

$$\text{Donc } f+g \in I.$$

$$\text{soit } f \in A, g \in I, (fg)(\frac{1}{2}) = f(\frac{1}{2}) \cdot g(\frac{1}{2}) = f(\frac{1}{2}) \cdot 0 = 0$$

$$\text{Donc } f \cdot g \in I.$$

\Rightarrow cl I est un idéal de A.

soit $f \in I$, montrons que f engendre pas I.

Montrons $\sqrt{|f|}$ n'est pas dans I

$\rightarrow f$ est cont de $|f|$ puis $\sqrt{|f|}$ est cont.

$$\sqrt{|f(0)|} = \sqrt{|f(1)|} \text{ et } \sqrt{|f(\frac{1}{2})|} = \sqrt{|0|} = 0.$$

$$\text{Donc } \sqrt{|f|} \in I.$$

Sous qu'il existe $g \in A$ tq $\sqrt{|f|} = g \cdot f$

$$\text{Alors } g = \frac{\sqrt{|f|}}{f} = \pm \frac{1}{\sqrt{|f|}}$$

Si une telle $f \circ g$ ne serait pas définie et $(f \circ g)(0) = f(g(0)) = f(0) = 0$
 en $\frac{1}{2}$, de celle n'existe pas.

i.e., $\nexists f \in I, (f) \neq I$

I n'est donc pas principal.

Ex2: soit $(G, +)$ $\textcircled{9}$ commutatif.

On munir l'ens $\text{End}(G)$ des endomorphismes
 de groupes de G de la loi de composition interne +

$$\text{def } f+g : \begin{cases} G \rightarrow G \\ x \mapsto f(x) + g(x) \end{cases}$$

M $\ddot{\alpha}$ $(\text{End}(G), +, 0)$ est un anneau.

soit $f, g \in \text{End}(G)$,

$f+g$ et $f \circ g$ st des endomorphismes.

En effet,

$$(f+g)(0) = f(0) + g(0) = 0$$

$$\begin{aligned} (f+g)(x+y) &= f(x+y) + g(x+y) = \\ &= f(x) + f(y) + g(x) + g(y) \\ &= (f+g)(x) + (f+g)(y). \end{aligned}$$

$$\begin{aligned} (f \circ g)(x+y) &= f(g(x+y)) = f(g(x) + g(y)) \\ &= (f \circ g)(x) + (f \circ g)(y). \end{aligned}$$

M $\ddot{\alpha}$ $(\text{End}(G), +)$ est un $\textcircled{9}$ abélien.

soit $f, g, h \in \text{End}(G)$, $x \in G$,

$$((f+g)+h)(x) = f(x) + g(x) + h(x) = (f+(g+h))(x)$$

$$\text{et } (f+g)(x) = f(x) + g(x) = g(x) + f(x) = (g+f)(x).$$

Donc $(\text{End}(G), +)$ est associatif & commutatif.

Le neutre est $0: x \mapsto 0$. Il est bien un endomorphisme.

$$\text{et } (0+f)(x) = 0(x) + f(x) = f(x)$$

L'inverse de f est $-f: x \mapsto -f(x)$

car $(f+(-f))(x) = f(x) - f(x) = 0 = 0(x)$ & $-f$ est bien un endomorphisme.

Mq $(\text{End}(G), \circ)$ est associative & possède un neutre.

soit $f, g, h \in \text{End}(G)$, $x \in G$,

$$(f \circ g) \circ h(x) = f(g(h(x))) = (f \circ (g \circ h))(x)$$

Le neutre est l'identité Id_G , c'est bien un endomorphisme & $f \in \text{End}(G)$, $x \in G$,

$$(f \circ \text{Id}_G)(x) = f(x) = (\text{Id}_G \circ f)(x).$$

Enfin, \circ est distributive sur $+$:

soit $f, g, h \in \text{End}(G)$, $x \in G$,

$$\text{alors } (f \circ (g+h))(x) = f(g(x) + h(x))$$

$$= f(g(x)) + f(h(x)) \text{ car } f \in \text{End}(G)$$

$$(f \circ (g+h))(x) = (f \circ g + f \circ h)(x)$$

$$\& ((f+g) \circ h)(x) = (f+g)(h(x))$$

$$= f(h(x)) + g(h(x))$$

$$= (f \circ h + g \circ h)(x).$$

Donc $(\text{End}(G), +, \circ)$
est bien un anneau.

Ex 4 Anneau de Boole

Soit E un ens (m) . On note $\mathcal{P}(E)$ l'ens des paires de E . La différence symétrique de 2 paires X & Y de E est déf Δ :

$$X \Delta Y = (X \cup Y) \setminus (X \cap Y) = (X \setminus Y) \cup (Y \setminus X)$$

a) Mq $(\mathcal{P}(E), \Delta, \cap)$ est un anneau commutatif.
Est-il intégré?

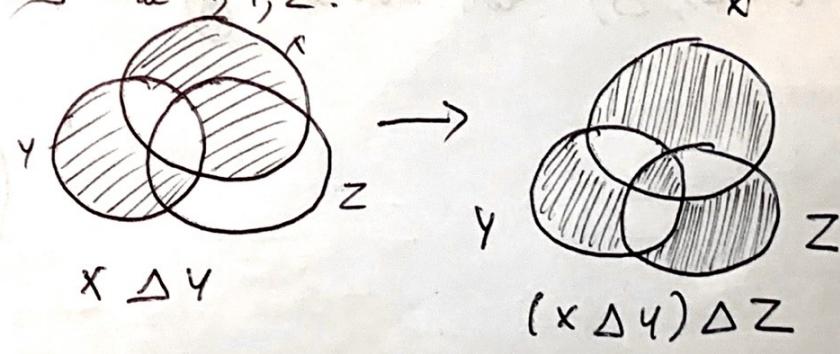
→ gabella g' addi
→ \otimes dist, assoc, e neutre
→ ici commutativity.

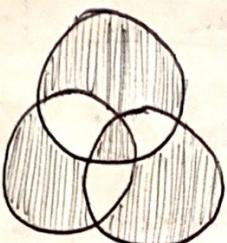
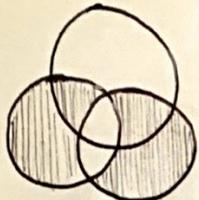
(i) Mq $(\mathcal{P}(E), \Delta)$ est \otimes abélien.

$$X \Delta Y = (X \cup Y) \setminus (X \cap Y) = (Y \cup X) \setminus (Y \cap X) = Y \Delta X$$

Cela démontre que la diag de Venn est aussi acceptée.

Pour mq l'associativité, on va utiliser un diag de Venn. Ce sera une preuve suffisante car un tel diag présente tous les intersections de X, Y, Z .





$Y \Delta Z$

$X \Delta (Y \Delta Z)$

$$\text{d'où } X \Delta (Y \Delta Z) = (X \Delta Y) \Delta Z.$$

Donc Δ est associative.

→ Le neutre est \emptyset :

$$X \Delta \emptyset = \emptyset \Delta X = \emptyset \cup X = X \quad \forall X \in P(E).$$

$$\begin{aligned} \text{Soit } X \in P(E), \quad X \Delta X &= (X \cup X) \setminus (X \cap X) \\ &= X \setminus X = \emptyset. \end{aligned}$$

Donc X est son propre opérateur.

$(P(E), \Delta)$ est bien un \textcircled{g} abélien.

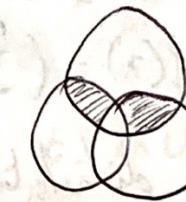
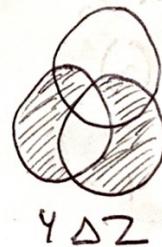
2) $(P(E), \cap)$ est un monoïde (i.e associative + neutre)
Commutatif

(trivial mg \cap est associative & commutative).

E est le neutre : soit $X \in P(E)$, $X \cap E = X$

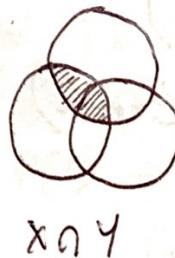
Donc $(P(E), \cap)$ est un monoïde commutatif.

3) \cap est distributive sur Δ

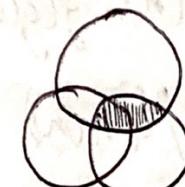


$Y \Delta Z$

$X \cap (Y \Delta Z)$



&



$X \cap Z$

$(X \cap Y) \Delta (X \cap Z)$

et

$(P(E), \Delta, \cap)$ est un anneau (commutatif).

NB: Comme \cap est commutative, on a aussi

$$(X \Delta Y) \cap Z = (X \cap Z) \Delta (Y \cap Z)$$

Est-il intègre? (ie n'admet pas de diviseurs de 0)
 $\forall a, b \in A^2, ab=0 \Leftrightarrow a=0 \text{ ou } b=0$

Si $|E| \geq 2$: soit $x, y \in E$, $x \neq y$

alors $\{x\} = \emptyset$, $\{y\} = \emptyset$ mais $\{x\} \cap \{y\} = \emptyset$
 $P(E)$ n'est pas intègre.

Si $|E|=1$:

$$P(E) = \{\emptyset, E\} \simeq \frac{\mathbb{Z}/2\mathbb{Z}}{\mathbb{Z}}$$

bien intègre.

b) I idéal de $P(E)$, Mg tels $x, y \in I$:

on a $P(x) \subset I$ et $x \cup y \in I$

soit $x \in I$, soit $A \in P(x)$, alors $A = A \cap x \in I$.

car $A \in P(E)$, $x \in I$

Donc $P(x) \subset I$.

• $x, y \in I$,

• $x \Delta y \in I$

• $x \cap y \in I$.

$$\bullet x \cup y = (\underbrace{x \Delta y}_{\in I}) \Delta (\underbrace{x \cap y}_{\in I}) \in I.$$

c) Mg si E est fini alors les idéaux de $P(E)$ sont exactement les $F \in E$ à $|F| \leq |E|$.

Analyse / Synthèse

soit I un idéal de $P(E)$,

soit $F \in I$ de cardinal maximal.

D'après b), $P(F) \subset I$.

Mg que $P(F) = I$. En effet, supp par l'^o qu'il existe $x \in I \setminus P(F)$

alors $x \cup F \in I$, et $|x \cup F| > |F|$, contradiction.

$$\Rightarrow I = P(F)$$

→ Mg $P(F)$ est un idéal :

• Soit $A \in P(E)$, $x \in P(F)$, $A \cap x \subset x \subset F$

• $\emptyset \in P(F)$ et si $x, y \in P(F)$, $x \Delta (-y) = x \Delta y \in P(F)$

$\Rightarrow P(F)$ est bien un idéal de $P(E)$.

AIS:
 \circ \exists un objet I .

o plus: mg le plus d'obj.

o Δ des objets mg.

49

Idéal
◦ stable par Δ
◦ $P(F)$

◦ (I, Δ) est de (A, Δ) .

d) Supposons que $E \neq \emptyset$. Montrons que $I = \{paires finies de E\}$ est un idéal de $\mathcal{P}(E)$ qui n'est pas de la forme $\mathcal{P}(F)$ ou $F \subseteq E$.

Mg I est un idéal de $\mathcal{P}(E)$.

- $|I| = 0$ donc $\emptyset \in I$.

et si $x, y \in I$, $x \Delta (-y) = x \Delta y$

et $|x \Delta y| \leq |x| + |y| < \infty$

Donc I est \oplus de $(\mathcal{P}(E), \Delta)$.

- Soit $A \in \mathcal{P}(E)$, $x \in I$,

$|A \cap x| \leq |x| < \infty$ de $A \cap x \in I$.

$\Rightarrow I$ est un idéal de $\mathcal{P}(E)$.

Supposons pour l'instant que $I = \mathcal{P}(F)$ ou $F \subseteq E$.

- $\forall x \in E$, $\{x\} \in I = \mathcal{P}(F)$ de $x \in F$.

- Donc $E \subseteq F$, de $F = E$

- De $I = \mathcal{P}(E)$, mais alors $I \ni E$, alors que E est infini. Contradiction

I est de bien un idéal de $\mathcal{P}(E)$ qui ne s'écrive pas sous la forme $\mathcal{P}(F)$ où $F \subseteq E$.

Ex

Un élément d'un anneau A est idempotent si $a^2 = a$ & est nulpotent si $\exists n \in \mathbb{N}^*$ que $a^n = 0$

a) Mg aucun inversible de A soit nulpotent.
Soit $a \in A$ inversible, a n'est pas un diviseur de zéro, donc il ne peut pas être nulpotent.

Autre preuve : Supposons $a^n = 0$, alors $0 = a^{-m} \cdot a^m = (a^{-1} \cdot a)^m = 1^m = 1$
Contradiction. Donc a n'est pas nulpotent.

b) Mg 1 est l'unique élément idempotent inv. de A.

Soit $a \in A$ idempotent & inversible

$$a^2 = a \xrightarrow{\times a^{-1}} a \cdot a^{-1} = a^{-1} \cdot a \rightarrow a = 1.$$

$1 \cdot 1 = 1^2 = 1$ donc 1 est inversible

& idempotent.

c) Mg si a est élé nulpotent de A
alors $1-a$ est inversible.

soit $a \in A$ nulpotent, $\exists m > 0$ tq $a^m = 0$

$$1 - \underline{1 - a^m} = (1-a)(1+a+a^2+\dots+a^{m-1})$$

$$= (1-a)(1+a+a^2+\dots+a^{m-1})$$

Donc $1-a$ est inversible et $(1-a)^{-1} =$
 $= 1+a+a^2+\dots+a^{m-1}$

Mg si a est un élé idempotent de A ,
alors $1-a$ est idempotent.

soit $a \in A$ idempotent,

$$(1-a)^2 = 1-2a+a^2 = 1-2a+a$$

$$(1-a)^2 = 1-a$$

Donc $1-a$ est idempotent.

d) Déterminer les nulpotents & les idempotents d'un anneau intègre.

soit A intègre, suppose $a^n = 0$, alors comme A est intègre, $a = 0$.

Donc 0 est le seul nulpotent (et en effet, $0^2 = 0$)

soit $a \in A$ idempotent, $a^2 = a$
 $a^2 - a = 0 \rightarrow a(a-1) = 0$

Comme A est intègre, $a = 0$ ou $a-1 = 0$, de $a = 1$.

Cpl : 0 & 1 st les seuls idempotents.

En effet $0^2 = 0$ & $1^2 = 1$.

$$ax^2 + bx + c$$

$$\begin{array}{ccc} \Delta & & \int_{\substack{a,c \\ b,c \\ a,b}} \\ x_1 & x_2 & \\ ab=0 & & b=0 \\ \hookrightarrow x=0 & \text{ou} & \end{array} \quad \text{51}$$

Ex 8 soit $f: A \rightarrow B$ un MDA,

a) l'image d'un idéal de A par f est-il un idéal de B ?

b) l'image réciproque d'un idéal de B par f est-il un idéal de A ?

Demande: Essayer de mg le résultat
à si c'était bon et si l'une des
hypothèses n'est pas vérifiée alors l'asser-
tora fausse.

a) soit $I \subset A$ idéal, $f(I)$ est-il un
idéal de B ?

• $(I, +)$ est un MDG de $(A, +)$ & f est
un MDG de $(f(I), +)$ est MDG de $(B, +)$.

• soit $b \in B$, $f(a) \in f(I)$,

b. $f(a) = b = f(u)$? non
pas possible.

Pas possible d'aller plus loin quand
 $f: A \rightarrow B$ n'est pas surjective.

Ca $f: \mathbb{R} \rightarrow \mathbb{C}$, $x \mapsto x$, c'est un morphism.

• $f(\mathbb{R}) = \mathbb{R}$ et \mathbb{R} n'est pas un idéal de \mathbb{C}
(car pas stable par multiplication d'un élé de \mathbb{C})

@ $i \cdot 1 = i$
 $\mathbb{P} \cap \mathbb{A}$
 $\mathbb{C} \cap \mathbb{R} = \mathbb{R}$

On a construit un contre-exemple : en général,
 $f(I)$ n'est pas un idéal de B .

b) soit $J \subset B$ un idéal, $f^{-1}(J)$ est-il un idéal
de A ?

• $f(0) = 0 \in J$ dc $0 \in f^{-1}(J)$,
soit $a, a' \in f^{-1}(J)$, alors $f(a-a') = \underline{f(a)} - \underline{f(a')} \in$
 $\underset{\in J}{\in J}$

Donc $a-a' \in f^{-1}(J)$,

Donc $(f^{-1}(J), +)$ est sg de $(A, +)$.

soit $a \in A$, $a' \in f^{-1}(J)$,
 $f(a \cdot a') = \underline{f(a)} \cdot \underline{f(a')} \in J$.

$f(a \cdot a) = \underline{f(a)} \cdot \underline{f(a)} \in J$.

Donc $a \cdot a' \in f^{-1}(J) \Rightarrow f^{-1}(J)$ est bien un
idéal de A .

Ex9: Existe-t-il un MDA de \mathbb{R} vers \mathbb{Q} .

soit $f: \mathbb{R} \rightarrow \mathbb{Q}$ un MDA.

$$f(2) = f(1+1) = f(1) + f(1) = 2.$$

$$\text{aussi } f(\sqrt{2})^2 = f(\sqrt{2}^2) = f(2) = 2$$

De $f(\sqrt{2})$ vérifie l'équation $x^2 = 2$.

Mais cette équation n'a pas de solution dans \mathbb{Q} .

De \nexists MDA $\mathbb{R} \rightarrow \mathbb{Q}$.

Ex10 soit $A = \{M_{a,b,c} \mid a, b, c \in \mathbb{Q}\}$.

$$I = \{M_{a,b,c} \mid a+b+c=0\} \text{ où } M_{a,b,c} = \begin{pmatrix} a & b & c \\ c & a & b \\ b & c & a \end{pmatrix}$$

a) $M_g A$ et \otimes -@ commutatif de $M_3(\mathbb{C})$.

$$A = \{M_{a,b,c} \mid a, b, c \in \mathbb{C}\}$$

b) $M_g (A, +)$ @ abélien de $M_3(\mathbb{C})$

c) mon ride : $O_3 = M_{0,0,0} \in A$

d) stable par \otimes : $M_{a,b,c}, M_{d,e,f} \in A$.

$$M_{a,b,c} - M_{d,e,f} = \begin{pmatrix} a & b & c \\ c & a & b \\ b & c & a \end{pmatrix} - \begin{pmatrix} d & e & f \\ f & d & e \\ e & f & d \end{pmatrix}$$

$$= \begin{pmatrix} a-d & b-e & c-f \\ c-f & a-d & b-e \\ b-e & c-f & a-d \end{pmatrix}$$

et $M_{a,b,c} - M_{d,e,f} \in A$.

Done $(A, +)$ & $(M_3(\mathbb{C}), +)$ (avec on est à \mathbb{Q})
(abélien & multiplication)

⇒ M_g neutre $\in A$

→ I_3 est le neutre de $(M_3(\mathbb{C}), +)$ et $I_3 = M_{1,0,0} \in A$

⇒ $M_g A$ est stable par multiplication.

soit $M_{a,b,c}, M_{d,e,f} \in A$,

$$M_{a,b,c} M_{d,e,f} = \begin{pmatrix} a & b & c \\ c & a & b \\ b & c & a \end{pmatrix} \begin{pmatrix} d & e & f \\ f & d & e \\ e & f & d \end{pmatrix} = \begin{pmatrix} ad+bf+ce & ae+bd+ef & af+be+cd \\ ae & +bd & be+cd \\ cd+af & +ef & cf+ad \end{pmatrix}$$

$$= M_{ad+bf+ce, ae+bd+ef, af+be+cd}$$

Done A est bien stable par multiplication.

De plus, cette $\boxed{\text{ff}}$ permet de vérifier que

$$M_{a,b,c} M_{d,e,f} = M_{d,e,f} M_{a,b,c}$$

a) A est @ commutatif de $M_3(\mathbb{C})$.

53

Q) Mg I est un idéal (pl) maximal de A.

intuit: considérer apply $M_{a,b,c} \in A \mapsto a+b+c \in \mathbb{C}$.

$$\text{Idéal} = \begin{cases} (I, +) & \text{sg } (A, +) \\ a_n \in I, \forall a \in A, \forall n \in I \end{cases}$$

► Mg $(I, +)$ ⊕ de $(A, +)$ ↙
stabil et stable.

$$\bullet O_3 = M_{0,0,0} \in I \text{ car } 0+0+0=0.$$

$$\bullet M_{a,b,c} - M_{d,e,f} = M_{a-d, b-e, c-f}$$

si $M_{a,b,c}, M_{d,e,f} \in I$.

$$\text{alors } (a-d) + (b-e) + (c-f) = (a+b+c) - (d+e+f) = 0$$

$$\text{de } M_{a,b,c} - M_{d,e,f} \in I.$$

Donc c'est bien un ⊕ de $(A, +)$.

$$\bullet \text{ Soit } M_{a,b,c} \in A, M_{d,e,f} \in I$$

Mg $a_n \in I, \forall n \in A, \forall n \in I$:

$$M_{a,b,c} M_{d,e,f} = M_{ad+bf+ce, ae+bd+cf, af+be+cd}$$

$$\text{et } (ad+bf+ce) + (ae+bd+cf) + (af+be+cd)$$

$$= (a+b+c)(d+e+f) = 0$$

De $M_{a,b,c} M_{d,e,f} \in I \Rightarrow I$ est bien un idéal de A.

Mg I principal:

Il faut mg $\exists M_{d,e,f} \in I$ tq

$$I = (M_{d,e,f}) \text{ i.e. } \forall M_{x,y,z} \in I,$$

$$\exists M_{a,b,c} \in A \text{ tq } M_{x,y,z} = M_{a,b,c} \cdot M_{d,e,f}$$

→ si $M_{d,e,f}$ est inversible, $M_{a,b,c} = M_{x,y,z} \cdot M_{d,e,f}^{-1}$

Il suffit de trouver une matrice $M_{d,e,f} \in I$ inversible.

$$\text{On peut prendre } M_{d,e,f} = \begin{pmatrix} 1 & j & j^2 \\ j^2 & 1 & j \\ j & j^2 & 1 \end{pmatrix}, \quad j = e^{2\pi i / 3}$$

Q $\mathbb{C}(G)$
onrait

| Mg idéal maximal sur A/M corps

Mg I maximal:

$$\text{soit } \Psi: M_{a,b,c} \rightarrow a+b+c$$

$$\begin{aligned} \text{On a déjà mgé } \Psi(x-y) &= \Psi(x) - \Psi(y) \\ \Psi(ny) &= \Psi(n) \Psi(y). \end{aligned}$$

$$\text{Df, } \Psi(O_3) = \Psi(M_{0,0,0}) = 0+0+0=0$$

$$\Psi(I_3) = \Psi(M_{1,0,0}) = 1+0+0=1$$

De Ψ est $\frac{\text{MDA}}{\text{A}}: A \rightarrow \mathbb{C}$.

$$\text{Df, } I = \text{Ker } \Psi$$

On peut appliquer le Thm d'isomorphisme, i

$$A/I = A/\text{Ker } \varphi \cong \text{Im } \varphi = \mathbb{C} \quad \text{car}$$

car $z \in \mathbb{C}$ vérifie $z = \varphi(z \cdot I_3)$ φ corps.

Donc A/I est un corps $\Rightarrow I$ est idéal maximal.

Anneaux d'entiers & Entiers de Gauss

Ex 21 (Anneau d'entiers)

soit $w \in \mathbb{C} \setminus \mathbb{Q}$, $w^2 \in \mathbb{Z}$. ($\text{@ } w = \sqrt{2}$ ou $w = i$)

soit 1^{er} env $\mathbb{Z}[w]$ & appli $N: \mathbb{Z}[w] \rightarrow \mathbb{Z}$ par

$$\mathbb{Z}[w] = \{a + bw, a, b \in \mathbb{Z}\}$$

$$\& N(a + bw) = a^2 - w^2 b^2.$$

a) M_q $\mathbb{Z}[w]$ est sa de \mathbb{C} .

- ↪ 1) $(\mathbb{Z}[w], +)$ sa abélien $(\mathbb{C}, +)$
- 2) $\mathbb{Z}[w]$ stable p^r multiplication
- 3) neutre de $\mathbb{Z}[w] \in \mathbb{C}$.

$$\rightarrow \frac{\mathbb{Z}[w]}{\langle \omega \rangle} \triangleleft \mathbb{C}$$

$$\omega = 0 + \omega w \in \mathbb{Z}[w]$$

$$\text{si } (a + wb), (c + wd) \in \mathbb{Z}[w]$$

$$(a + wb) + (c + wd) = (a + c) + \omega(b + d) \in \mathbb{Z}[w].$$

• Stable par \times

soit $a + wb, c + wd \in \mathbb{Z}[w]$,

$$(a + wb)(c + wd) = ac + wbc + wad + w^2 bd \\ = (ac + w^2 bd) + \omega(bc + ad) \in \mathbb{Z}[w].$$

• $1 \in \mathbb{Z}[w]$, en effet, $1 = 1 + 0 \cdot w \in \mathbb{Z}[w]$

$\Rightarrow \mathbb{Z}[w]$ est sa de \mathbb{C} .

b) M_q $(1, w)$ est une \mathbb{Z} -base de $\mathbb{Z}[w]$,
i.e. $\forall z \in \mathbb{Z}[w], \exists! (a, b) \in \mathbb{Z}^2, z = a + bw$

L'^e existence d'une telle décompos^o provient de la définition de $\mathbb{Z}[w]$.

Supp $a + bw = c + dw$ alors $a - c = \omega(d - b)$

or $w \notin \mathbb{Q}$, de $a - c = 0 \Leftrightarrow d - b = 0$

$$\Rightarrow (a, b) = (c, d).$$

La décomp est de uniq.

c) $M_9 \quad \varphi: \mathbb{Z}[\omega] \rightarrow \mathbb{Z}[\omega]$

$$a + \omega b \mapsto a - \omega b$$

est endomorphisme de l'anneau $\mathbb{Z}[\omega]$

M_9 est MDA :

$$\circ \varphi(a + \omega b + c + \omega d) = \varphi((a+c) + \omega(b+d))$$

$$= (a+c) - \omega(b+d) = a - \omega b + c - \omega d = \varphi(a + \omega b) + \varphi(c + \omega d).$$

$$\circ \varphi((a + \omega b)(c + \omega d)) = \varphi((ac + \omega^2 bd + \omega(ad + cb)))$$

$$= (ac + \omega^2 bd) - \omega(ad + cb)$$

$$= (a - \omega b)(c - \omega d)$$

$$= \varphi(a + \omega b) \varphi(c + \omega d)$$

$$\circ \varphi(1) = \varphi(1 + 0\omega) = 1 - 0\omega = 1.$$

al $\varphi: \mathbb{Z}[\omega] \rightarrow \mathbb{Z}[\omega]$ est un endomorphisme d'anneaux.

$$d) M_9 \quad N(xy) = N(x)N(y) \quad \forall x, y \in \mathbb{Z}[\omega]$$

$$N(a + \omega b) = a^2 - \omega^2 b^2$$

$$\Rightarrow N((a + \omega b)(c + \omega d)) = N((ac + \omega^2 bd + \omega(ad + cb)))$$

$$\begin{aligned} &= (ac + \omega^2 bd)^2 - \omega^2(ad + cb)^2 \\ &= a^2 c^2 + \cancel{\omega^2 acbd} + \omega^4 b^2 d^2 - \cancel{\omega^2 a^2 d^2} \\ &= (a^2 - \omega^2 b^2)(c^2 - \omega^2 d^2) = N(a + \omega b)N(a - \omega b) \end{aligned}$$

e) $M_9 \quad x \in \mathbb{Z}[\omega]$ est irréductible si $N(x) = \pm 1$

\Rightarrow soit $x \in \mathbb{Z}[\omega]$, supposez x est irréductible

$$\text{alors } 1 = nn^{-1} \Rightarrow N(1) = N(nn^{-1}) = N(x)N(x^{-1})$$

$$\Rightarrow 1 = N(x)N(x^{-1})$$

Donc $N(x) \mid 1$, d'où $N(x) = \pm 1$.

$$\begin{aligned} (\Leftarrow) \quad x = a + \omega b, \text{ supp } N(x) = a^2 - \omega^2 b^2 = \pm 1 \\ (a + \omega b)(a - \omega b) = \pm 1. \end{aligned}$$

Donc $x = a + \omega b$ est irréductible.

g) lorsque $w^2 \leq 0$ vérifier que $x \in \mathbb{Z}[w]$ est inv si $N(x) = 1$.

Qd $w^2 \leq 0 \rightarrow N(a+wb) = a^2 - w^2 b^2 \geq 0$
 & $a+wb \in \mathbb{Z}[iw]$. La norme
 est tjs positive dc le résultat de e)
 devient "x est inv si $N(x)=1$ ".

g) soit $z \in \mathbb{Z}[w]$ non-nul tq $N(z) \neq \pm 1$
 & les diviseurs (ds \mathbb{Z}) de $N(z)$ appartiennent
 à l'image de N appartenant à $\{\pm 1, \pm N(z)\}$.
 Mq z est irréductible.

Spp z n'est pas irréductible. Alors $z = ab$ dc
 a, b non-inv $N(z) = N(a) \cdot N(b)$
 Donc $N(a)$ divise $N(z)$ mais n'est ni ± 1 ,
 ni $\pm N(z)$. Par contraposé, les hypo de l'exo
 impliquent que z soit irréductible.

fin ex 22

57

Ex 25: Entiers de Gauss

L'anneau des entiers de Gauss est le sa

$\mathbb{Z}[i] = \{a+ib \mid a, b \in \mathbb{Z}\}$ de \mathbb{C} .

La norme de $z = a+ib \in \mathbb{Z}[i]$ est l'entier

$$N(z) = a^2 + b^2 \in \mathbb{N}$$

a) Déterminer les élts inv de $\mathbb{Z}[i]$.

$$\mathbb{Z}[i] - \mathbb{Z}[\sqrt{-1}] = \mathbb{Z}[w] \text{ et } w^2 = -1$$

Comme $w^2 \leq 0$, selon (21.f), $z = a+ib$
 est inversible ssi $N(z) = a^2 + b^2 = 1$.

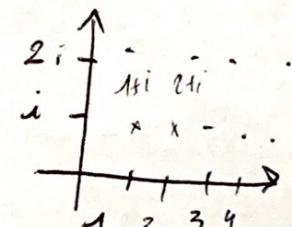
On a 4 possibilités: $(a, b) \in \{(\pm 1, 0), (0, \pm 1)\}$
 Les inversibles de $\mathbb{Z}[i]$ st dc $\{\pm 1, \pm i\}$.

b) soit $u, v \in \mathbb{Z}[i] \neq v \neq 0$.

Mq $\exists q, r \in \mathbb{Z}[i]$ tq $u = vg + r$ & $N(r) < N(v)$
et $\mathbb{Z}[i]$ est pl.

soit $u, v \in \mathbb{Z}[i], v \neq 0$, alors $\frac{u}{v} \in \mathbb{Q}[i]$

réseau
de
points



(D6) $\phi(n) = \text{card}((\mathbb{Z}/n\mathbb{Z})^*)$
 $= \text{nbr des } k \in \{1, \dots, n\} \text{ tels que } k \perp n = 1$

@ $\phi(6) = 2$ f' indication de l'an

$$\phi(p) = p-1$$

(P8) Soit $n \in \mathbb{N}^*$ alors $n = \sum_{d|n} \phi(d)$.

@ $6 = \phi(1) + \phi(2) + \phi(3) + \phi(6)$
 $6 = 1 + (2-1) + (3-1) + 2$

DM Soit $n \in \mathbb{N}^*$, on sait \forall diviseur d de n ($d > 0$), $\exists !$ \mathcal{G}_d de $\mathbb{Z}/n\mathbb{Z}$ d'ordre d .

Soit $\mathcal{G}_d = \{\text{elts d'ordre } d \text{ ds } \mathbb{Z}/n\mathbb{Z}\}$

On a $\mathcal{G}_d \subset \mathcal{G}_d$ (puisque un elt d'ordre d engendre un \mathcal{G}_d de $\mathbb{Z}/n\mathbb{Z}$ d'ordre d , dc \mathcal{G}_d).

On a de $\mathcal{G}_d = \{\text{elts d'ordre } d \text{ ds } \mathcal{G}_d\}$
 $= \{\text{elts d'ordre } d \text{ ds } \mathbb{Z}/d\mathbb{Z}\}$

car $\mathcal{G}_d \simeq \mathbb{Z}/d\mathbb{Z}$

al \mathcal{G}_d = générateur de $\mathbb{Z}/d\mathbb{Z}$
 $\mathbb{Z}/n\mathbb{Z} = \bigsqcup_{d|n} \mathcal{G}_d$
 les cardinaux donnent

$$n = \sum_{d|n} \phi(d)$$

8.4 (Th) Chinois : si m & n st 2 entiers > 0 ,
 p.e. $\Rightarrow (\star) \mathbb{Z}/mn\mathbb{Z} \simeq \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$.

DM : d'appli $\Psi : \mathbb{Z} \rightarrow \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$
 $x \mapsto (x+m\mathbb{Z}, x+n\mathbb{Z})$

est un MDA et

$$\ker \Psi = \{x \in \mathbb{Z}, \begin{cases} x+m\mathbb{Z} = m\mathbb{Z} \\ x+n\mathbb{Z} = n\mathbb{Z} \end{cases}\}$$

$$= \{x \in \mathbb{Z}, \frac{m}{\text{lcm}(m, n)} | x\}$$

$$= \{x \in \mathbb{Z}, \text{lcm}(m, n) | x\} \text{ car } \text{lcm}(m, n) = 1$$

al $\ker \Psi = mn\mathbb{Z}$ & $\mathbb{Z}/mn\mathbb{Z} \simeq \text{Im } \Psi \subset \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$

cl $\ker \varphi = mn\mathbb{Z}$ & $\mathbb{Z}/mn\mathbb{Z} \cong \text{Im } \varphi \subset \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$

de card mn

de card $m \times n$

de p^{x-1}

Les entiers x ds $[1, p^x]$ premiers à p^x
sont les entiers entre 1 & p^x sauf
multiples de p .

$$\text{D'où } \text{Im } \varphi = \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}.$$

Rq (voir (Ex 15))

(*) donne: Pour m, n pos

$$(\mathbb{Z}/mn\mathbb{Z})^\times \underset{\text{groupes}}{\sim} (\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z})^\times = (\mathbb{Z}/m\mathbb{Z})^\times \times (\mathbb{Z}/n\mathbb{Z})^\times$$

$$(A_1 \times A_2)^\times = A_1^\times \times A_2^\times$$

ce q'a pos conséquence (en regardant les cardinaux)

$$\boxed{\Phi(mn) = \Phi(m) \times \Phi(n)} \quad \text{si } \text{pgcd}(m, n) = 1.$$

Rq: si p est premier, et $x \in \mathbb{N}$

$$\boxed{\Phi(p^x) = p^x - p^{x-1}}$$

Dm $x \in \mathbb{N}, \dots ;$, $\text{pgcd}(n, p^x) = 1$

$$\Leftrightarrow p \nmid n$$

$$\begin{aligned} @ \Phi(18) &= \Phi(2^2 \cdot 3) = \Phi(2^2) \Phi(3) \\ &= (2^2 - 2)(3 - 3^0) \\ &= 4. \end{aligned}$$

§ Cryptographie

Chapitre Polynômes

$$K[x] \stackrel{\text{def}}{=} \left\{ \sum_{m=0}^N a_m x^m, a_0, \dots, a_N \in K \right\}$$

où K est un anneau commutatif
 $\mathbb{C}[x], \mathbb{R}[x], \mathbb{Z}_{\geq 2}[x], (K[x], +, \cdot)$ et @ com @.

$\boxed{a_N x^N}$ \Rightarrow $\mathbb{Z}_{\geq 2}[x] \in \text{pos intz}$ $\deg P = 0$
coeff dominant $\Rightarrow \deg \text{du polynôme} \neq 0$,

$$\begin{aligned} \deg(P+Q) &\leq \max(\deg P, \deg Q) \\ \deg(PQ) &= \deg(P) + \deg(Q). \end{aligned}$$

(P86) K corps, \Rightarrow 1) $\mathbb{K}[x]$ intègre
2) L'ens $(\mathbb{K}[x])^X$ s/s inv = \mathbb{K}^*

van (P85, P86)

(D) 1) $P = \sum_{n=0}^m a_n x^n, Q = \sum_{n=0}^m b_n x^n, \neq 0$

$n = \deg(P), m = \deg(Q) \Rightarrow a_m \neq 0, b_m \neq 0.$

$\deg(PQ) = \deg(P) + \deg(Q) = m+n$ & le coeff dominant du poly PQ est $a_m b_m \neq 0$ & $PQ \neq 0.$
Donc $\mathbb{K}[x]$ est intègre.

2) Preuve de $(\mathbb{K}[x])^X = K^X$ $\text{pr } K @ \text{intègre}$:

(C) évident

(C) soit $P \in (\mathbb{K}[x])^X$ i.e. $\exists Q \in \mathbb{K}[x]$ tq

(*) $P \times Q = 1$. Alors $\deg P + \deg Q = 0$

de $\deg P = \deg Q = 0$

i.e. $P, Q \in K$ et (*) dit que $P \in K^X$.

(P87) (FT Taylor) $K_m[x] = \{ P \in K[x], \deg P \leq m \}$
 $P \in K_m[x] \& a \in K:$

$$P(x) = \sum_{k=0}^m \frac{P^{(k)}(a)}{k!} (x-a)^k$$

(D) (2^e monômes).



2. Division Euclidienne

(P88) soit K un $@$ intègre, soit $P \in K[x]$,
on appelle $P \neq 0$ & coeff dominant de P
est inversible do K & $\deg P \geq 1$.

Pour $F \in K[x]$, $\exists Q, R \in K[x]$,
tq $F = PQ + R$ & $\deg(R) < \deg(P)$.

Le couple (Q, R) est uniq.

2M soit $F \in K[X]$,

(A) PR si $m = \deg(F)$

• $m=0$: on a $F = D_n P + F$ et $\deg(F) = 0 < \deg P$

• suppose $m \geq 1$ & $\deg F = m$:

on écrit $F = f_m X^m + \dots + f_0$

$P = p_d X^d + \dots + p_0$ où $d = \deg P$.

1^{er} cas : si $m < d$, on a :

$F = 0 \cdot P + F$ et $\deg F = m < d = \deg P$.

2^{er} cas : si $m \geq d$

$F - P \cdot \left(\sum_{j=m}^d p_j^{-1} X^{m-d} \right)$ est un polynôme de $\deg \leq m-1$. $\exists P$ hypo.

¶ NDR, $\exists Q_1, R_1 \in K[X]$ tq

$$F - P \left(\sum_{j=m}^d p_j^{-1} X^{m-d} \right) = Q_1 P + R_1$$

de $\deg R_1 < \deg P$.

Cela donne :

$$F = \underbrace{P \left(Q_1 + \sum_{j=m}^d p_j^{-1} X^{m-d} \right)}_{\sim} + R_1$$

on a $\deg R = \deg R_1 < \deg P$.

(B) Sous $F = PQ_1 + R_1 = PQ_2 + R_2$
si $\deg R_1 < \deg P$, $\deg R_2 < \deg P$.

$$\text{Alors } P(Q_1 - Q_2) = R_2 - R_1$$

Mais $\deg(R_2 - R_1) \leq \max(\deg R_1, \deg R_2) < \deg P$.

et $\deg(P(Q_1 - Q_2)) > \deg P$ sauf si $Q_1 - Q_2 = 0$

d'où $Q_1 = Q_2$ et $R_1 = R_2$ □

(C) si K est un corps, $K[X]$ est un \mathbb{Z} euclidien & dc principal.

↳ Vérifie de ppt's (L) Gauss, Euclide, Bézout décomp II est inductible.

3. Racines d'un polynôme

Démons, K est un corps.

(D) Racine d'un polynôme

$$P(x) = \underbrace{(x-a)}_{\in K} Q + R \quad R = P(a)$$

remplacer $x=a$

① Multiplicité.

④ P ∈ K[X], K corps, app. a_1, \dots, a_m racines de P de multiplicité respective m_1, \dots, m_n . Alors P est divisible par

$$(X-a_1)^{m_1} \cdot (X-a_2)^{m_2} \cdots (X-a_m)^{m_n}$$

④ Si P ∈ K[X] est un polynôme non-nul alors le nbr de racines distinctes de P ds K est $\leq \deg P$.

DM Si a_1, \dots, a_m st les racines distinctes de P & m_1, \dots, m_n leurs multiplicités, ∃ Q ∈ K[X] tq $P = Q \times (X-a_1)^{m_1} \cdots (X-a_m)^{m_n}$. On obtient $\deg P \geq \deg Q + m_1 + \dots + m_n > 0 + \underbrace{1+ \dots + 1}_n$

(P92, 93)

si a racine de multiplicité k. du P, devient racine de mult k-1 en P'.

voil DM

a racine de P de multp k si

$$P(a) = P'(a) = P''(a) = \dots = P^{(k-1)}(a) = 0 \text{ et } P^{(k)}(a) \neq 0.$$

§ 4. Polynômes irréductibles

K[X] est @ pl.

$$(K[X])^* = K^* = K^* = K \setminus \{0\}.$$

④ P ∈ K[X] dit irréductible si

∀ F, G ∈ K[X], P = FG équivaut

à $F \in K[X]^*$ ou $G \in K[X]^*$, ce q équivaut à $\deg F = 0$ ou $\deg G = 0$.

④ $\bullet \deg P = 1 \Rightarrow P$ irréductible

• si $P(a) = 0, a \in K, \deg P \geq 2$

$\Rightarrow P$ est réductible

$$P = (X-a)Q$$

Pb matiq: Quels st les irréductibles de $K[x]$?

La réponse dépend de K .

(P95) ($K = \mathbb{C}$).

Les irréductibles de $\mathbb{C}[x]$ st les seuls polynômes de deg 1.

(P96). Les irréductibles de $\mathbb{R}[x]$ st de 2 types :

- les polynômes de deg 1.
- les polynômes de deg 2 sans racine ds $\mathbb{R}(\otimes x^2+1)$.

Preuve P95 : $K = \mathbb{C}$,

- les polynômes de deg 1 st irréduct (trivs)
- soit $P \in \mathbb{C}[x]$ irréductible. D'après le

(H) d'Alm'bert Gauss, P a une racine $a \in \mathbb{C}$.

Donc $P = (x-a) Q + Q \in \mathbb{C}[x]$, comme

P est irréductible, $\deg Q = 0$ ie $\deg P = 1$.

(H) d'A-G : Tt $P \in \mathbb{C}[x]$ de deg $n \geq 1$ admet racine 55 ds \mathbb{C} .

$$\text{Écrivons } \frac{u}{v} = x + iy$$

$$\exists n' + iy' \in \mathbb{Z}[i] \text{ tel que } |n'-n| \leq \frac{1}{2}$$

$$\text{Posons } q = n' + iy', \quad |y' - y| \leq \frac{1}{2}.$$

$$u - qv = v \left(\frac{u}{v} - q \right)$$

$$= v((x+iy) - (n'+iy'))$$

$$r := v((x-n') + i(y-y'))$$

$$N((x-n') + i(y-y')) = (x-n')^2 + (y-y')^2 \\ \leq \frac{1}{2^2} + \frac{1}{2^2} < 1.$$

$$\text{Donc } N(r) = N(v)N((x-n') + i(y-y')) \\ < N(v)$$

On a bien $\mathbb{Z}[i]$ n'est pas stalleme
 $\mathbb{Z}[i]$ est euclidien, cf PL.

c) Mg 3 est irréductible dans $\mathbb{Z}[i]$

+ résultat 21.g) ; on calcule la norme de $3i$: $N(3) = 3^2$
 les diviseurs de $N(3)$ ne sont pas ± 1 & $N(3)$ est 3 & -3.

Il est impossible que $N(3) = -3$ car $N(3) \geq 0$. un des cas

De plus si $N(x+iy) = x^2 + y^2 = 3$. On doit être l'un des suivants :

$$\begin{cases} x^2 = 0 \\ x^2 = 1 \\ x^2 = 2 \\ x^2 = 3 \end{cases} \text{ et } \begin{cases} y^2 = 3 \\ y^2 = 2 \\ y^2 = 1 \\ y^2 = 0 \end{cases}$$

IMPOSSIBLE

les seuls diviseurs de $N(3) = 9$ sont ± 1 & ± 3
 en appliquant le résultat de 21.g, on voit que 3 est irréductible dans l'anneau $\mathbb{Z}[i]$.

d) Mg un élément $z \in \mathbb{Z}[i]$ tq $N(z)$ soit premier est irréductible. La réciproque est-elle vraie ?

Si $N(z)$ est premier \Rightarrow ses seuls diviseurs sont ± 1 & $\pm N(z)$.

Les résultats de 21.g. montrent que z est irréductible.

La réciproque est fausse & 8 nous donne un cas où z est irréductible dans $\mathbb{Z}[i]$ mais $N(z) = 9$ n'est pas 1.

e) Vérifier $5 = (2+i)(2-i) = (1+2i)(1-2i)$ & que ceu ne contredit pas la factorialité de $\mathbb{Z}[i]$

$$(2+i)(2-i) = 2^2 - i^2 = 4+1 = 5 \quad \& \quad (1+2i)(1-2i) = 1^2 - (2i)^2 = 1+4=5$$

$$\text{Mais } 2+i = i(1+2i) \quad \& \quad 2-i = -i(1+2i)$$

⑤8 De ces 2 décompositions équivalentes, ce résultat ne contredit pas l'axiome de la décomp en élément irréductible.

g. Décomposer $2, 9, 13, -2+2i, 7+i$ en produit d'irréductibles de $\mathbb{Z}[i]$.

$N(2) = 2^2 - 4$, il n'y a pas de diviseur de 2 $\neq \pm 2$ & ± 1 dont la norme est 2.

$$N(x+iy) = 2 \Rightarrow x^2 + y^2 = 2 \Rightarrow x^2 = 1, y^2 = 1.$$

② $z = (1+i)(1-i)$, de plus $N(1+i) = N(1-i) = 2$ est premier de $1+i$ & $1-i$ et irréductible.

Supposons a & b st pcc $\Rightarrow a$ est inv de $\mathbb{Z}/b\mathbb{Z}$, en effet, on peut écrire $1 = ua + vb$ $\forall u, v \in \mathbb{Z}$ modulo b , ce résultat devient $\bar{1} = \bar{u} \cdot \bar{a} + \bar{v} \cdot \bar{0} = \bar{u} \cdot \bar{a}$. De \bar{a} est inv & $\bar{a}^{-1} = \bar{u}$.

• ③ de 5 par 3: $5 = 2 \times 3 - 1 \Rightarrow -1 = 2 \times 3 - 5$

$$-1 = 2 \times (-126 \times 28 - 5 \times 705) - (1 \times 705 - 25 \times 28)$$

$$\boxed{-1 = 277 \times 28 - 11 \times 705}$$

Dans $\mathbb{Z}/705\mathbb{Z}$, le résultat devient $\bar{1} = \bar{277} \times \bar{28}$. Donc $\bar{28}^{-1} = \bar{277}$ du $\mathbb{Z}/705\mathbb{Z}$.

Ex 18 Résoudre du \mathbb{Z} les systèmes suivants.

$$\begin{cases} 3x \equiv 2 \quad [41] \\ 3x \equiv 4 \quad [7] \end{cases} \quad \begin{cases} x \equiv -3 \quad [99] \\ x \equiv 2 \quad [40] \end{cases} \quad \begin{cases} x \equiv 3 \quad [4] \\ x \equiv -2 \quad [3] \\ x \equiv 7 \quad [5] \end{cases}$$

(E.) L'algorithme d'Euclide étendu entre 11 & 7.

$$11 = 7 + 4 \Rightarrow 4 = 11 - 7$$

$$7 = 2 \times 4 - 1 \Rightarrow 1 = 2 \times 4 - 7 = 2 \times (11 - 7) - 7$$

$$\boxed{1 = 2 \times 11 - 3 \times 7}$$

$$1 \equiv 2 \times 11 [7] \quad \& \quad 1 \equiv -3 \times 7 [11]$$

Construire $y = 2 [11] \& y = 3 [7]$.

$$y = -2 \times 3 \times 7 + 4 \times 2 \times 11 = -42 + 88 = 46$$

TM Chinois: soit m & n 2 entiers pcc, $m \nmid n = 1$ alors l'^④ produit $\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ est isomorphe à l'^④ $\mathbb{Z}/mn\mathbb{Z}$.

Ex 2: Calculer l'inverse de $\bar{28}$ du $\mathbb{Z}/705\mathbb{Z}$.

On va appliquer l'algorithme d'Euclide étendu à 705 & 28.

• ④ de 705 par 28: $705 = 28 \times 25 + 5$
 $\Rightarrow 5 = 1 \times 705 - 25 \times 28$

• ④ de 28 par 5: $28 = 5 \times 5 + 3$

$$\Rightarrow 3 = 28 - 5 \times 5 = 28 - 5 \times (1 \times 705 - 25 \times 28)$$

$$= 126 \times 28 - 5 \times 705$$

$$\begin{cases} 3x \equiv 2 \pmod{11} \\ 3x \equiv 4 \pmod{7} \end{cases} \Leftrightarrow \begin{cases} 3x \equiv 46 \pmod{11} \\ 3x \equiv 46 \pmod{7} \end{cases}$$

Comme 7 & 11 st paires, le \textcircled{M} chinois donne
 $\Leftrightarrow 3x \equiv 46 \pmod{77}$.

Inverse de 3 ds $\mathbb{Z}/77\mathbb{Z}$

$$77 = 26 \times 3 - 1 \Rightarrow 26 \times 3 \equiv 1 \pmod{77}$$

$$\text{Donc } 3^{-1} = \overline{26} \text{ dans } \mathbb{Z}/77\mathbb{Z}$$

$$\Rightarrow x \equiv 26 \times 46 \equiv 41 \pmod{77}$$

Répondre ds \mathbb{Z} $\begin{cases} x \equiv -3 \pmod{99} \\ x \equiv 2 \pmod{140} \end{cases}$

Algo d'Euclide étendu entre gg et 140.

$$1 = 29 \times 140 - 41 \times 99 \quad \leftarrow 140, 99 \text{ paires.}$$

$$\text{Donc } \begin{cases} 29 \times 140 \equiv 1 \pmod{99} \\ -41 \times 99 \equiv 1 \pmod{140} \end{cases}$$

$$\text{Donc } -3 \times 29 \times 140 - 2 \times 41 \times 99 \equiv \begin{cases} -3 \pmod{99} \\ 2 \pmod{140} \end{cases}$$

$$-20 \times 298$$

Comme 99 & 140 st paires, on pt appliquer
le \textcircled{M} chinois :

$$x \equiv -20 \times 298 \pmod{99 \times 140}$$

$$x \equiv 7422 \pmod{-13860}$$

Répondre ds \mathbb{Z} $\begin{cases} x \equiv 3 \pmod{4} \\ x \equiv -2 \pmod{3} \\ x \equiv 7 \pmod{5} \end{cases}$

Algo d'Euclide étendu entre :

$$4 \text{ et } 3 \times 5 = 15:$$

$$1 = 4 \times 4 - 1 \times 15$$

$$3 \text{ et } 4 \times 5 = 20: \quad 1 = 7 \times 3 - 1 \times 20$$

$$5 \text{ et } 3 \times 4 = 12: \quad 1 = 5 \times 5 - 2 \times 12$$

$$\text{Donc } \begin{cases} 1 \equiv -1 \times 15 \pmod{4} \\ 1 \equiv -1 \times 20 \pmod{3} \\ 1 \equiv -2 \times 12 \pmod{5} \end{cases}$$

$$\text{Donc } -3 \times 15 + 2 \times 20 - 7 \times 24 = \begin{cases} 3 \\ -2 \\ 7 \end{cases} \quad \text{soit } \varphi: (\mathbb{Z}/p\mathbb{Z})^* \rightarrow (\mathbb{Z}/p\mathbb{Z})^* \\ y \mapsto y^2.$$

$$-45 + 40 - 168 = -173$$

$$\Rightarrow \boxed{x \equiv 7 \pmod{60}} \quad \text{on } 3, 4, 5 \\ \text{par } 2 \vdash 2$$

Ex6 (Carres de $\mathbb{Z}/p\mathbb{Z}$), soit p un nbr premier $\neq 2$.

Batt Mq -1 est un carré ds $\mathbb{Z}/p\mathbb{Z}$

si $p \equiv 1 \pmod{4}$. On note $C(p)$ tq

$$C(p) = [x \in \mathbb{Z}/p\mathbb{Z} \mid \exists y \in \mathbb{Z}/p\mathbb{Z}, x = y^2]$$

a) Mq $C(p)^*$ est \textcircled{sg} multiplicatif de $(\mathbb{Z}/p\mathbb{Z})^*$ de cardinal $\frac{p-1}{2}$.

indic Considérons $x \in (\mathbb{Z}/p\mathbb{Z})^* \mapsto x^2 \in C(p)^*$.

b) Soit $x \in (\mathbb{Z}/p\mathbb{Z})^*$. Mq $x \in C(p)^*$ in $x^{\frac{p-1}{2}} = 1$.

indic: user poly de deg n à coeff ds un corps au polyn n racines.

φ est un MDG:

$$\begin{aligned} \varphi(1) &= 1^2 = 1 \\ \varphi(xy) &= (xy)^2 = x^2y^2 = \varphi(x)\varphi(y) \end{aligned}$$

De plus $C(p)^* = \text{Im } \varphi$.

Donc $C(p)^*$ est un \textcircled{sg} de $(\mathbb{Z}/p\mathbb{Z})^*$.

D'après le TH d'isomorphisme,

$$\frac{(\mathbb{Z}/p\mathbb{Z})^*}{\ker \varphi} \simeq \text{Im } \varphi \Rightarrow |C(p)^*| = \frac{|(\mathbb{Z}/p\mathbb{Z})^*|}{|\ker \varphi|}$$

$$|(\mathbb{Z}/p\mathbb{Z})^*| = p-1.$$

$$\ker \varphi = \{y \in \mathbb{Z}/p\mathbb{Z}, y^2 = 1\}$$

$\ker \varphi$ contient 1 & -1 . $(1 \neq -1)^{\frac{p-1}{2}}$ est impair & ce sont les seuls élts car $y^2 = 1$ est une équation de degré 2 n l' \textcircled{int} égrer

B) Soit $x \in C(p)^*$, écrivons $x = y^2$, Ex R: soit $P(x) = x^2 + 1 \in K[x]$
où $K = \mathbb{Z}/3\mathbb{Z}$.

alors $x^{\frac{p-1}{2}} = y^{p-1} = 1$ par le Th de Lagrange,
puisq $|(\mathbb{Z}/p\mathbb{Z})^*| = p-1$.

Le polynôme $X^{\frac{p-1}{2}} = 1$ admet au plus $\frac{p-1}{2}$ racines
de $\mathbb{Z}/p\mathbb{Z}$. On sait que les $\frac{p-1}{2}$ élts de $C(p)^*$
sont des racines de ce polynôme. Ce et de les seuls:
 $x^{\frac{p-1}{2}} = 1 \iff x \in C(p)^*$.

c) Cl: -1 est un carré de $\mathbb{Z}/p\mathbb{Z}$

$$\iff -1 \in C(p)^*$$

$$\iff (-1)^{\frac{p-1}{2}} = 1$$

$\iff \frac{p-1}{2}$ est paire.

$\iff p-1$ est multiple de 4 .

$$\iff p \equiv 1 \pmod{4}$$

- a) Mg P est irréductible
- b) Mg $K[x]/(P)$ est un corps à g élts.

Sous pr ?! $P(x)$ est réductible
 $\Rightarrow P(x) = A(x)B(x)$ si $0 < \deg A < 2$.
 donc $\deg A = 1$ ie $A(x) = X - \lambda$,

et $\lambda \in \mathbb{Z}/3\mathbb{Z}$. Donc λ est une racine de ?!

Contradict: car P n'a pas de racine:

x	$x^2 + 1$
$\bar{0}$	$\bar{1}$
$\bar{1}$	$\bar{2}$
$\bar{2}$	$\bar{2}$

Par l'absurde,
 P est irréductible.

b) Comme P est irréductible & $K[X]$

est un anneau principal, alors (P) est
un idéal premier, de maximal.

$K[X]/(P)$ est un corps.

et chaque polynôme de $K[X]$, on peut
associer à sa classe dans $K[X]/(P)$
le reste de sa division euclidienne par P .

Donc $|K[X]/(P)|$ est le nbr de restes
possibles, i.e le nbr de polynômes de degré
inférieur ST à 2. Un tel polynôme est de la
forme $a+bX$ & $(a, b) \in (\mathbb{Z}/3\mathbb{Z})^2$.

Donc $|K[X]/(P)| = |\mathbb{Z}/3\mathbb{Z}|^2 = 9$.

- - - - -
Séance Révisions M^{me} : 22/12

14^h45. → Zoom.

DS 2021

