

T.D. M51. Emmanu DUCLOS.

(R₁) E, F des ens.

(D) Une applic^{ation} f de E vers F , notée $f: E \rightarrow F$, c'est la donnée pour tt él^e $x \in E$, d'un él^e $f(x) \in F$.

→ E est appelé ens de définitio de f

→ F est appelé ens d'arrivée

(D) Soit $A \subseteq E$, $B \subseteq F$, l'image de A par f , notée $f(A)$, est $f(A) = \{f(a) \text{ pour } a \in A\}$.

L'image réciproque de B par f , notée $f^{-1}(B)$ est

$$f^{-1}(B) = \{x \in E, f(x) \in B\}.$$

avec le antécédé

(D) La restrictio de f à A , notée $f|_A$ est l'applicat

$$f|_A : A \rightarrow F$$

$$a \mapsto f(a)$$

(D) La corestrictio de f à B , notée $f|_B$ est l'applicat $f|_B : f(B) \rightarrow B$

$$z \mapsto f(z)$$

$$A \subseteq E, C \subseteq F$$

$$B \subseteq E, D \subseteq F.$$

Ex 1: Soit $f: E \rightarrow F$ une applicat. $A \subseteq E, C \subseteq F$.

a) Mq $A \subseteq f^{-1}(f(A))$ (puisque f est injective).

→ Soit $x \in A$, alors $f(x) \in f(A)$ dc $x \in f^{-1}(f(A))$.

On a bien mqé $A \subseteq f^{-1}(f(A))$.

supposons f injective, → Soit $x \in f^{-1}(f(A))$, $\exists y \in A$ tq $f(x) = f(y)$.

→ f est injective, on a $x = y$.

D'où $x \in A$, dc $f^{-1}(f(A)) \subseteq A$.

Par double inclusion : $A = f^{-1}(f(A))$.

b) Mq $f(f^{-1}(C)) \subseteq C$ ($\begin{array}{l} \text{de l'égalité basque} \\ f \text{ est surjective} \end{array}$) c) Mq $f(A \cup B) = f(A) \cup f(B)$.
 Soit $y \in f(f^{-1}(C))$ alors $\exists x \in f^{-1}(C)$
 tq $y = f(x)$.
 Comme $x \in f^{-1}(C)$, on a $f(x) \in C$, de $y \in C$.
et $f(f^{-1}(C)) \subseteq C$.

$y \in f(A \cup B) \Leftrightarrow \exists x \in A \cup B$ tq $y = f(x)$
 $\Leftrightarrow (\exists x \in A \mid y = f(x)) \text{ ou } (\exists x \in B \mid y = f(x))$
 $\Leftrightarrow y \in f(A) \text{ ou } y \in f(B)$
 $\Leftrightarrow y \in f(A) \cup f(B)$.

Donc $f(A \cup B) = f(A) \cup f(B)$.

Supposons f est surjective, soit $y \in C$,
 alors comme f est surjective, $\exists x \in E \mid y = f(x)$.
 Puisque $y \in C$, on a $x \in f^{-1}(C)$ & de
 $y \in f(f^{-1}(C))$.

On a dc mqé lorsque f est surjective,
 $C \subseteq f(f^{-1}(C))$.

& p double-inclusion: $C = f(f^{-1}(C))$.

d) Mq $f(A \cap B) \subseteq f(A) \cap f(B)$ ($\begin{array}{l} \text{de l'égalité basque} \\ f \text{ est injective} \end{array}$)
 Soit $y \in f(A \cap B) \Rightarrow \exists x \in A \cap B \mid y = f(x)$
 Comme x est à la fois dans A et B , on a
 $y = f(x) \in f(A)$ et $y \in f(B)$.

Donc $y \in f(A) \cap f(B)$; d'où $f(A \cap B) \subseteq f(A) \cap f(B)$

Supp f injective, soit $y \in f(A) \cap f(B)$ alors

$y \in f(A)$, de $\exists x \in A$ tq $y = f(x)$
 $y \in f(B)$, de $\exists x' \in B$ tq $y = f(x')$

$\exists f$ est injective & $f(x) = f(x')$; on a $x = x'$.

(e) $x \in A \cap B$; d'où $y \in f(A \cap B)$, & dc
 $f(A) \cap f(B) \subseteq f(A \cap B)$ Par double inclusion,
 $f(A \cap B) = f(A) \cap f(B)$

$$e) \text{ Mq } f^{-1}(C \cup D) = f^{-1}(C) \cup f^{-1}(D)$$

$$x \in f^{-1}(C \cup D) \Leftrightarrow f(x) \in C \cup D$$

$$\Leftrightarrow f(x) \in C \text{ ou } f(x) \in D$$

$$\Leftrightarrow x \in f^{-1}(C) \text{ ou } x \in f^{-1}(D)$$

$$\Leftrightarrow x \in f^{-1}(C) \cup f^{-1}(D)$$

$$\text{D'où } f^{-1}(C \cup D) = f^{-1}(C) \cup f^{-1}(D).$$

$$f) \text{ Mq } f^{-1}(C \cap D) = f^{-1}(C) \cap f^{-1}(D)$$

$$x \in f^{-1}(C \cap D) \Leftrightarrow f(x) \in C \cap D$$

$$\Leftrightarrow f(x) \in C \text{ et } f(x) \in D$$

$$\Leftrightarrow x \in f^{-1}(C) \text{ et } x \in f^{-1}(D)$$

$$\Leftrightarrow x \in f^{-1}(C) \cap f^{-1}(D)$$

$$\text{D'où } f^{-1}(C \cap D) = f^{-1}(C) \cap f^{-1}(D)$$

voir ex 2 ③

e) Mq $f^{-1}(C \cup D) = f^{-1}(C) \cup f^{-1}(D)$.

$$x \in f^{-1}(C \cup D) \Leftrightarrow f(x) \in C \cup D$$

$$\Leftrightarrow f(x) \in C \text{ ou } f(x) \in D$$

$$\Leftrightarrow x \in f^{-1}(C) \text{ ou } x \in f^{-1}(D)$$

$$\Leftrightarrow x \in f^{-1}(C) \cup f^{-1}(D)$$

D'où $f^{-1}(C \cup D) = f^{-1}(C) \cup f^{-1}(D)$.

f) Mq $f^{-1}(C \cap D) = f^{-1}(C) \cap f^{-1}(D)$

$$x \in f^{-1}(C \cap D) \Leftrightarrow f(x) \in C \cap D$$

$$\Leftrightarrow f(x) \in C \text{ et } f(x) \in D$$

$$\Leftrightarrow x \in f^{-1}(C) \text{ et } x \in f^{-1}(D)$$

$$\Leftrightarrow x \in f^{-1}(C) \cap f^{-1}(D)$$

D'où $f^{-1}(C \cap D) = f^{-1}(C) \cap f^{-1}(D)$

Ex2: Que dire de l'ens $F(E, F)$ lorsque $E = \emptyset$ ou $F = \emptyset$?

• $E \neq \emptyset$ mais $F = \emptyset$

$\boxed{\text{H1}} |F(E, F)| = |F|^{|E|} = 0^{|E|} = 0 \text{ et } F(E, F) = \emptyset$
 $\text{card}(\cdot) := 1 \cdot 1$

$\boxed{\text{H2}}$ soit $f \in F(E, F)$, soit $x \in E$, alors $f(x) \in F = \emptyset$

Donc $f(x) \notin F$, $F(E, F) = \emptyset$.

• $E = \emptyset$

$$(|F(E, F)| = |F|^{|E|} = |F|^0 = 1)$$

• $f(x) = \frac{1}{\sqrt{1-x^2}} \rightarrow \mathcal{D}_f = \emptyset$. (on n'impose q^e f)

Définir une applica $\emptyset \rightarrow F$, c'est donner $\forall x \in \emptyset$, une image $f(x)$. Comme le \emptyset ne contient pas d'elt, on peut faire le faire de une seule façon. $F(\emptyset, F)$ ne contient de qu'un sol elt.

voir ex2 ③

Ex 4 si E un ens. TH Cantor.

Mq \exists appl surjective $f: E \rightarrow \mathcal{P}(E)$

Indic^o: considérez $X = \{x \in E \mid x \notin f(x)\}$.

Sups p l'absurde qu'il existe $f: E \rightarrow \mathcal{P}(E)$ surjective.

Considérons $X = \{x \in E \mid x \notin f(x)\}$

Puisq f est surjective, $\exists x \in E$ tq $x = f(a)$.

Est-ce que $x \in X$?

\rightarrow supp $x \in X$ alors $x \in f(a)$. de $x \notin X$. $\textcircled{1}$)

\rightarrow supp $x \notin X$ alors $x \notin f(a)$ dc $x \in X$. $\textcircled{0}$)

On a donc les 2 cas une absurdité.

dc f ne pt pas être surjective.

Ex 5: TH Cantor-Bernstein

a) $G: \mathcal{P}(E) \rightarrow \mathcal{P}(E)$ f croissante.

$M = \bigcup_{A \in S} A$ où $S = \{A \in \mathcal{P}(E) \mid A \subset G(A)\}$

Mq $M \subset G(M)$, soit $x \in M$ alors $\exists A \in S$ tq $x \in A$.

Donc $A \subset G(A)$, et $x \in G(A)$.

dc $x \in \bigcup_{A \in S} G(A) = G(M)$ d'où $M \subset G(M)$.

Mq $G(M) \subset M$:

soit $G(x) \in G(A)$ $\forall A \in S$.

on sait que $A \subset G(A)$, dc comme G est croissante $G(A) \subset G^2(A) = G(G(A))$.

Donc $G(A) \in S$. Donc $G(x) \in \bigcup_{A \in S} A = M$

D'où $G(M) \subset M$.

Par double inclusion :

$M = G(M)$ | c'est bien un point fixe.

suite Thm Cantor-Bernstein

On va montrer Thm Cantor-Bernstein.

On a déjà montré si $G: \mathcal{P}(E) \rightarrow \mathcal{P}(F)$ est un morphisme alors elle a un point fixe M .

b) $f: E \rightarrow F$, $g: F \rightarrow E$ 2 injections.

Considérons $G: \mathcal{P}(E) \rightarrow \mathcal{P}(E)$ $\xrightarrow{\text{M}} \text{et } \xrightarrow{G}$
 $A \mapsto E \setminus g(F \setminus f(A))$.

soit $A \subset B \subset E \Rightarrow f(A) \subset f(B)$.

$$F \setminus f(A) \supset F \setminus f(B)$$

$$g(F \setminus f(A)) \supset g(F \setminus f(B))$$

$$E \setminus g(F \setminus f(A)) \subset E \setminus g(F \setminus f(B))$$

$$G(A) \subset G(B)$$

Donc f est surjective.

D'après @, G possède un point fixe $M \in \mathcal{P}(E)$.

$$M = E \setminus g(F \setminus f(M))$$

$$\text{ou encore } E \setminus M = g(F \setminus f(M))$$

$g: F \setminus f(M) \rightarrow E$ est une injection & son image est $E \setminus M$, c'est donc une bijection $F \setminus f(M) \rightarrow E \setminus M$.

On peut alors définir

$$h: E \longrightarrow F$$

 $x \longmapsto \begin{cases} f(x) & \text{si } x \in M \\ (g|_{E \setminus M})^{-1}(x) & \text{si } x \notin M \end{cases}$

h est injective.

h est injective par hypothèse.

$(g|_{F \setminus f(M)})^{-1}$ est bijective, donc en injective.

si $x \in M$ & $y \in E \setminus M$ alors $h(x) = f(x) \in M$,

$$h(y) = (g|_{E \setminus M})^{-1}(y) \in F \setminus F(M).$$

Donc $h(x) \neq h(y)$. h est bien injective

h est surjective:

$$\begin{aligned} h(E) &= h(M \cup E \setminus M) = h(M) \cup h(E \setminus M) \\ &= f(M) \cup (g|_{E \setminus M})^{-1}(M) \\ &= f(M) \cup (F \setminus f(M)) \end{aligned}$$

$$\boxed{h(E) = F}$$

h est bien surjective.

Ex PT soit $f: \mathbb{N} \times \mathbb{N} \rightarrow \mathbb{N}^*$ l'appl
 $f(k, n) = (2k+1)2^n \forall (k, n) \in \mathbb{N} \times \mathbb{N}$.

(R*) Ens dénombrable = Ens de m° cardinal que \mathbb{N} ,
i.e. un ens en biject° à \mathbb{N} .

Ens au plus dénombrable = ens dénombr au fond.

a) Mg f est bijective.

$$f: \mathbb{N} \times \mathbb{N} \rightarrow \mathbb{N}^*$$

$$(k, n) \mapsto (2k+1)2^n$$

sait $m \in \mathbb{N}^*$, d'après le (TH) de décomp°
 en facteurs premiers, $\exists!$ décomp°

$$m = \prod_{p \text{ premier}} p^{2p}$$

$$m = 2^{2e} \times \prod_{\substack{p \text{ premier} \\ p \neq 2}} p^{2p}$$

impair

$$m = f\left(\frac{\prod_{p \text{ premier}, p \neq 2} p^{2p} - 1}{2}, e_2\right)$$

comme la décomp° en facteurs premiers
 de m est uniq, c'est son uniq antécédent.

Donc $f: \mathbb{N} \times \mathbb{N} \rightarrow \mathbb{N}^*$ est bijective.

$$\text{cas Tplo: } 2k = \prod_{p \text{ premier}} p^{2p-1} \Leftrightarrow k = \frac{\prod_{p \text{ premier}} p^{2p-1}}{2}$$

b) et $\mathbb{N} \times \mathbb{N}$ est dénombr

$$\text{On a la biject° } \mathbb{N}^* \xrightarrow{m \mapsto m-1} \mathbb{N}$$

dc $\mathbb{N} \times \mathbb{N}$ est de m° card que \mathbb{N}^* &
 de de \mathbb{N} , dc $\mathbb{N} \times \mathbb{N}$ est dénombr.

c) Mg (PR) \mathbb{N}^m est dénombr.

On sait que \mathbb{N} et \mathbb{N}^2 est dénombr.

On appelle $m \geq 3$ & \mathbb{N}^{m-1} dénombr.

$$\mathbb{N}^m = \mathbb{N}^2 \times \mathbb{N}^{m-2} \xrightarrow{\text{bijec}} \mathbb{N} \times \mathbb{N}^{m-2} = \mathbb{N}^{m-1}$$

De \mathbb{N}^m est dénombr.

soit $f: \mathbb{Z} \rightarrow \mathbb{N}$ biject°.

alors on a la biject°

$$f^m: \mathbb{Z}^m \rightarrow \mathbb{N}^m$$

$$(k_1, \dots, k_m) \mapsto (f(k_1), \dots, f(k_m))$$

et \mathbb{Z}^m est, tout comme \mathbb{N}^m , dénombr.

NB $f: \mathbb{Z} \rightarrow \mathbb{N}$

$$k \mapsto \begin{cases} 2k & \text{si } k \geq 0 \\ -2k-1 & \text{si } k < 0. \end{cases}$$

B&B Mg ens \mathbb{Q} des rationnels est dénombrable.

→ On va construire l'inject° $\mathbb{Q} \hookrightarrow \mathbb{N}$
 & $\mathbb{N} \hookrightarrow \mathbb{Q}$.

• $f: \mathbb{N} \rightarrow \mathbb{Q}$ l'inject° naturelle $n \mapsto n$

• i chg rationnels, on pl \Leftrightarrow une unq écriture
 fractionn° p/q &

• p & q premiers entre eux

• $q > 0$.

On pl définir $g: \mathbb{Q} \hookrightarrow \mathbb{Z}$

$$\frac{p}{q} \mapsto (p, q)$$

g est bien injective.

Comme \mathbb{Z}^2 est dénombrable (ex 17), \exists une biject°

$$h: \mathbb{Z}^2 \rightarrow \mathbb{N}$$

et de hog $\hookrightarrow \mathbb{N}$ est injective.

D'après le (TH) Cantor-Bernstein, \exists une biject°
 $\mathbb{N} \rightarrow \mathbb{Q}$.

Donc \mathbb{Q} est dénombrable. (on en tyco + \mathbb{N}).

E.61 But Mq \exists injct^e entre $P(\mathbb{N}) \times \mathbb{R}$

a) Mq tte pte de \mathbb{R} contenant un intervalle ouvert non vide est un bijct^e \mathbb{R} .

stat $A \subset \mathbb{R}$ une pte contenant $\exists a, b \in \mathbb{C}$
On a une inject^e $A \hookrightarrow \mathbb{R}$ naturelle
 $x \mapsto x$

On a la bijct^e:

$$\text{arctan}: \mathbb{R} \rightarrow]-\frac{\pi}{2}, \frac{\pi}{2}[$$

\exists bijct^e affine $f:]-\frac{\pi}{2}, \frac{\pi}{2}[\rightarrow]0, b[$

Donc $f \circ \text{arctan}: \mathbb{R} \rightarrow A$ est injective.

On a 2 injct^es $A \rightarrow \mathbb{R}$ & $\mathbb{R} \rightarrow A$,
de p^e le TM de Cantor-Bernstein:
on a une bijct^e.

6) Mq $\phi: P(\mathbb{N}) \rightarrow \mathbb{R}$, $\phi(A) = \sum_{n=0}^{\infty} \frac{\chi_A(n)}{3^n}$
est χ_A f^e const de $P(\mathbb{N})$ bien d^f & injective

$\phi: P(\mathbb{N}) \rightarrow \mathbb{R}$

$$A \mapsto \sum_{n=0}^{\infty} \frac{\chi_A(n)}{3^n}$$

$$\forall n, \left| \frac{\chi_A(n)}{3^n} \right| \leq \frac{1}{3^n}$$

$$\text{Qd } \sum_{n=0}^{\infty} \left| \frac{\chi_A(n)}{3^n} \right| \leq \sum_{n=0}^{\infty} \frac{1}{3^n} = \frac{1}{1-\frac{1}{3}} = \frac{3}{2}$$

La s^erie est abs. CV, de ϕ est bien d^f.

Sups $A \neq B$.

soit n_0 l^e + petit entier tq $\chi_A(n_0) \neq \chi_B(n_0)$
quitte à permute A & B, on pt m^e supposer
 $n_0 \in A$, $n_0 \notin B$.

$$\phi(A) - \phi(B) = \sum_{n=0}^{\infty} \frac{\chi_A(n) - \chi_B(n)}{3^n}$$

$$\begin{aligned} \phi(A) - \phi(B) &= \sum_{n=0}^{\infty} \frac{\chi_A(n) - \chi_B(n)}{3^n} \\ &= \frac{1}{3^{n_0}} + \sum_{n=n_0+1}^{\infty} \frac{\chi_A(n) - \chi_B(n)}{3^n} \\ &\geq \frac{1}{3^{n_0}} - \sum_{n=n_0+1}^{\infty} \frac{1}{3^n} \geq \frac{1}{3^{n_0}} - \frac{1}{3^{n_0+2}} \sum_{n=0}^{\infty} \frac{1}{3^n} \\ &\geq \frac{1}{3^{n_0}} - \frac{1}{3^{n_0+1}} \times \frac{3}{2} \geq \frac{1}{2 \times 3^{n_0}} > 0. \end{aligned}$$

Donc $\phi(A) \neq \phi(B)$.

ϕ est bien une injct^e de $P(\mathbb{N})$ dans \mathbb{R} .

CV $\phi: P(\mathbb{N}) \hookrightarrow \mathbb{R}$.

7) tr d^r dyadiq $(x_n)_{n \in \mathbb{N}}$ d^o un n^e tel
 $x \in [0, 1]$ et d^f r^uurant p^e

$$x_0 = \lfloor 2x \rfloor \quad x_{m+1} = \left\lfloor 2^{m+1} \left(2x - \sum_{k=0}^m \frac{x_k}{2^k} \right) \right\rfloor$$

Mq c^est une suite de 0 & 1 tq

$$x = \sum_{n=0}^{\infty} \frac{x_n}{2^n}$$

et $[0, 1] \hookrightarrow P(\mathbb{N})$. est injct^e

$$x \mapsto \{n \in \mathbb{N}, x_n = 1\}$$

soit $x \in [0, 1]$, on d^f. (x_n) p^e

$$\begin{cases} x_0 = \lfloor 2x \rfloor \\ x_{m+1} = \lfloor 2^{m+1} \left(2x - \sum_{k=0}^m \frac{x_k}{2^k} \right) \rfloor \end{cases}$$

On va mg PR:

$$P_m: x_m \in \{0, 1\} \quad \& \quad x'_m = x_m - \sum_{k=0}^m \frac{x_k}{2^{k+1}} \in [0, \frac{1}{2^{m+1}}]$$

① $x \in [0, 1]$; $\exists n \in \mathbb{N}$ de $x_0 = \lfloor 2x \rfloor \in \{0, 1\}$.

$$x'_0 = x_0 - \frac{\lfloor 2x \rfloor}{2} = \frac{2x - \lfloor 2x \rfloor}{2} \in [0, \frac{1}{2}]$$

De P_0 est v*é*rfi*c*é.

② Pr P_n & mg P_{n+1} .

$$2x - \sum_{k=0}^n \frac{x_k}{2^k} = x'_{n+1} \in [0, \frac{1}{2^{n+1}}] \quad \& \quad \text{UDR}.$$

$$\text{Dme } 2^{n+1} \left(2x - \sum_{k=0}^n \frac{x_k}{2^k} \right) \in [0, 1].$$

$$\text{de } x_{n+1} = \left\lfloor 2^{n+1} \left(2x - \sum_{k=0}^n \frac{x_k}{2^k} \right) \right\rfloor \in \{0, 1\}$$

$$x'_{n+1} = x_n - \sum_{k=0}^{m+1} \frac{x_k}{2^{k+1}} = x'_n - \frac{x_{m+1}}{2^{m+2}}$$

$$= x'_n - \left\lfloor \frac{2^{m+2} x'_n - \lfloor 2^{m+1} x'_n \rfloor}{2^{m+2}} \right\rfloor \in [0, \frac{1}{2^{m+2}}[$$

On a donc bien P_{m+1} .

D'où $(x_m)_{m \in \mathbb{N}}$ est une suite de 0 & de 1.

De plus, $x'_m \in [0, \frac{1}{2^{m+1}}[$ de $x'_m \xrightarrow[m \rightarrow \infty]{} 0$

$$\text{de } n - \sum_{k=0}^m \frac{x_k}{2^{k+1}} \xrightarrow[m \rightarrow \infty]{} 0, \text{ i.e. } \boxed{n = \sum_{k=0}^m \frac{x_k}{2^{k+1}}}$$

et $\Psi: [0,1] \rightarrow \mathcal{P}(\mathbb{N})$

$$x \mapsto \{n \in \mathbb{N}, x_n = 1\}$$

alors $x = \Psi(x) = \Psi(y)$ implique $x_n = 1 \Leftrightarrow y_n = 1$.

Comme $(x_n), (y_n)$ est à l'IN de $\{0,1\}$, cela signifie que les 2 suites ont la même valeur. $\textcircled{2}$

$$\text{Donc } x = \sum_{m=0}^{\infty} \frac{x_m}{2^{m+1}} = \sum_{m=0}^{\infty} \frac{y_m}{2^{m+1}} = y.$$

Donc $\Psi: [0,1] \hookrightarrow \mathcal{P}(\mathbb{N})$ est injective.

d) On a une injec $\phi: \mathcal{P}(\mathbb{N}) \hookrightarrow \mathbb{R}$.

On a aussi l'injco $\psi: [0,1] \hookrightarrow \mathcal{P}(\mathbb{N})$ & on a mqé en a) que $[0,1]$ est un bijct w \mathbb{R} .

On peut de appliquer le Th de Cantor-Bernstein pr déclire qu'il existe un bijct entre $\mathcal{P}(\mathbb{N})$ & \mathbb{R} .

e) D'après ex4, il n'y a pas de bijct entre \mathbb{N} & $\mathcal{P}(\mathbb{N})$. Il n'y a pas non plus de bijct entre \mathbb{N} & \mathbb{R} .

\mathbb{R} est indénombrable.

T.D 2 - Groupes

* Un \textcircled{g} monogène est un groupe G engendré par un seul élé, i.e. $\exists g \in G$ tq

$$G = \{g^k, k \in \mathbb{Z}\}$$

* s'il est fini, on dit que c'est un groupe cyclique. \exists alors $m \in \mathbb{N}^*$ tq G est isomorphe à $\mathbb{Z}/m\mathbb{Z}$.

* s'il est infini, $\mathbb{Z} \rightarrow G$ est un isomorphisme. $k \mapsto g^k$ (isomorphie bijective)

* par ex: $g \neq 1, g^2 \neq 1, g^3 \neq 1, g^4 = 1$,

$$g^{4k+1} = g^1 ; g^{4k+2} = g^2$$

On a un isomorphisme: $\mathbb{Z}/4\mathbb{Z} \rightarrow G$

$$k \mapsto g^k$$

Elle munie: on cherche $(a,b) \in \mathbb{R}_+^* \times \mathbb{R}$ tq

$$(a,b)(c,d) = (a,c)$$

$$\text{Donc } \begin{cases} ac = a \\ ad + b = c \end{cases} \Leftrightarrow \begin{cases} c = 1 \\ d = 0 \end{cases} \text{ car } a \in \mathbb{R}_+^*$$

Ex1 Mg $\mathbb{R}_+^* \times \mathbb{R}$ munie de la loi

$$(a,b)(c,d) = (ac, ad+b)$$
 est un groupe.

Stabilité: soit $(a,b), (c,d) \in \mathbb{R}_+^* \times \mathbb{R}$

$$\begin{aligned} \text{On a } a,c > 0 \text{ dc } ac \in \mathbb{R}_+^*. \\ \text{de } (a,b)(c,d) \in \mathbb{R}_+^* \times \mathbb{R}. \\ ((a,b)(c,d))(e,f) &= (ac, ad+b)(e,f) \\ &= (ace, ace + ad + b) \\ &= (ace, ace + ad + b) \end{aligned}$$

$$\begin{aligned} ((a,b)(c,d))(e,f) &= (a,b)(ce, cf + d) \\ &= (ace, acf + ad + b) \\ &= (ace, acf + ad + b) \\ &= ((a,b)(c,d))(e,f) \end{aligned}$$

$$\text{On a dc } (a,b)(1,0) = (a,b)$$

De plus,

$$(1,0) \cdot (a,b) = (1 \cdot a, 1 \cdot b + 0) = (a,b)$$

Donc $(1,0)$ est bien un élément neutre.

\rightarrow Symétricité:

soit $(a,b) \in \mathbb{R}_+^* \times \mathbb{R}$,

on cherche $(c,d) \in \mathbb{R}_+^* \times \mathbb{R}$ tq

$$(a,b) \cdot (c,d) = (1,0)$$

$$(ac, ad+b) = (1,0).$$

$$\begin{cases} ac = 1 \\ ad + b = 0 \end{cases} \Leftrightarrow \begin{cases} c = \frac{1}{a} \\ d = -\frac{b}{a} \end{cases}.$$

$$\text{Donc } (a,b) \cdot \left(\frac{1}{a}, -\frac{b}{a}\right) = (1,0).$$

$$\text{Df, } \left(\frac{1}{a}, -\frac{b}{a}\right) \cdot (a,b) = \left(\frac{1}{a} \cdot a, \frac{1}{a} \cdot b + \left(-\frac{b}{a}\right)\right) \\ = (1,0)$$

$$\text{Donc } (a,b)^{-1} = \left(\frac{1}{a}, -\frac{b}{a}\right).$$

al $\mathbb{R}_+^* \times \mathbb{R}$ muni de cette loi est bien un groupe d'élément neutre $(1,0)$.

Ex 2 Mg on tt est d'un groupe G est involutif (i.e.: $\forall g \in G, g^2 = 1$) alors G est commutatif.

$$\begin{aligned} \Leftrightarrow G \text{ est commutatif} &\Leftrightarrow \forall g, h \in G \Rightarrow gh = hg \\ &\Leftrightarrow \forall g, h \in G \Rightarrow ghg^{-1}h^{-1} = 1 \end{aligned}$$

Or puisque g & h st involutifs, $g^{-1}=g$ et $h^{-1}=h$

De $ghg^{-1}h^{-1} = (gh)(gh) = 1$ car gh est involutif

al G est bien commutatif.

Ex 3 Mg tt groupe de cardinal un nombre premier est cyclique.

indic : Th de Lagrange.

Th de Lagrange:

soit G un g de cardinal n , soit $H \subset G$ un

g alors le cardinal de H divise n .

et, pr $g \in G$, \exists l'ordre de g est $1 \{g^n, n \in \mathbb{Z}\}$,

alors l'ordre de g divise n .

Suite ex 3 Mg tt gpe de cardinal un

mbr premier est cycliq.

soit G un gpe de cardinal p premier
alors $p \geq 2$ dc on pt choisir $g \in G \setminus \{1\}$.

Le sous-groupe $\langle g \rangle$ engendré par g possède
un cardinal q divise celui de G (d'après le
Th de Lagrange).

Donc $|\langle g \rangle| = 1$ ou p .

Car $\langle g \rangle$ contient au moins 1 & g .

Donc $|\langle g \rangle| = p$, $\langle g \rangle = G$.

Donc G est monogène, de cardinal fini,
c'est de un gpe cycliq.

Ex 4 Mg si G est un gpe de cardinal
 ≤ 5 alors G est commutatif.

Qu'en est-il pour gpe de cardinal 6?

• si $m=2, 3$ ou 5 : Alors comme m est premier,
un gpe de cardinal m est cyclique.

Donc $G \cong \mathbb{Z}/m\mathbb{Z}$, dc G est commutatif.

• si $m=1$: Alors un gpe de card 1 est $G=\{1\}$.
C'est bien un gpe commutatif.

• si $m=4$: soit G un gpe de cardinal 4, $g \in G$.

D'après le Th de Lagrange, l'ordre de g divise 4,
dc ordre(g) = 1, 2 ou 4.

\rightarrow si g est d'ordre 4: alors $1, g, g^2, g^3$ st éts $\neq b$,
dc $G = \{1, g, g^2, g^3\} \cong \mathbb{Z}/4\mathbb{Z}$ (car cycliq
& de card 4)

Preuve gpe cycliq est commutatif:

soit G cycliq, soit $g \in G$ q engendre G alors si $h, k \in G$
alors $\exists n, m \in \mathbb{N}$ tq $h = g^n$, $k = g^m$.

$h \cdot k = g^n \cdot g^m = g^{n+m} = g^m \cdot g^n = kh$ dc le gpe est commutatif.

\rightarrow si G est cyclique, alors $G \cong \mathbb{Z}/m\mathbb{Z}$

isomorphe commutatif

→ si g est d'ordre 4: alors $1, g, g^2, g^3$ st
éts \neq de $G = \{1, g, g^2, g^3\} \cong \mathbb{Z}/4\mathbb{Z}$

Qu'en est-il pour groupe de cardinal 6?

Pr $n \geq 6$, ce n'est plus vrai.

Donc G est groupe commutatif.

→ si tous les g éts st d'ordre 1 ou 2.

Alors $\forall g \in G, g^2 = 1$. Dc d'après
l'¹ en 2, G est commutatif.

al **R**

si G est de cardinal ≤ 5 ,

L G est commutatif.

@ Groupe de cardinal dt b b éts st
d'ordre 1 ou 2.

$$G \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} = \{(0,0), (0,\bar{1}), \\ (\bar{1},0), (\bar{1},\bar{1}), \\ (a,b) + (c,d) = (a+c, b+d)\}$$

$|S_3| = 6$ & S_3 n'est pas commutatif.

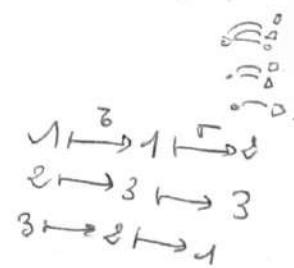
$$|S_3| = 3! = 6.$$

$$\tau = (1\ 2) \quad \text{et} \quad \sigma = (2\ 3)$$

$$\text{alors } \tau \circ \sigma = (1\ 2\ 3)$$

$$\text{De m } \sigma \circ \tau = (1\ 3\ 2).$$

Donc $\tau \sigma \neq \sigma \tau$, S_3 ne commute pas.



Ex6 Mg $(\mathbb{Q}, +)$ & (\mathbb{Q}_+^*, \times) ne
sont pas isomorphes. (indic : $\sqrt{2}$)

Supposons par l'absurde qu'il y ait
un isomorphisme.

$$\varphi: (\mathbb{Q}, +) \longrightarrow (\mathbb{Q}_+^*, \times)$$

alors φ est bijective &

$$\varphi(0) = 1$$

$$\varphi(a+b) = \varphi(a) \varphi(b)$$

$$\varphi(-a) = \frac{1}{\varphi(a)}$$

Idee : $\vartheta \in \mathbb{Q}_+^*$, $\sqrt{2} \notin \mathbb{Q}_+^*$.

Comme φ est bijective, $\exists a \in \mathbb{Q}$ tq
 $\varphi(a) = \vartheta$

Alors $(\varphi(\frac{a}{2}))^2 = \varphi(a) = \vartheta$. { Donc les groupes ne

Mais $\sqrt{2}$ n'est pas rationnel. { et pas
 $\varphi(\frac{a}{2})$ n'est pas défini. (c!c) { isomorphes.

Ex7 a) Mg groupe quotient \mathbb{R}/\mathbb{Z} est isomorphe
au groupe multiplicatif $S^1 = \{z \in \mathbb{C}, |z|=1\}$.

b) Mg groupe quotient \mathbb{C}/\mathbb{R} est isomorphe à \mathbb{R} .

(A)

Ex 9 a) Montrer que le groupe quotient \mathbb{R}/\mathbb{Z} est isomorphe au groupe multip.

$$\mathbb{S}^1 = \{z \in \mathbb{C}, |z|=1\}$$

On va construire un isomorphisme

$$\varphi: \mathbb{R}/\mathbb{Z} \rightarrow \mathbb{S}^1.$$

Pour cela il suffit trouver un morphisme

$$\psi: \mathbb{R} \rightarrow \mathbb{S}^1 \text{ surjectif et tel que } \text{at } \mathbb{Z}.$$

$$\psi: t \mapsto e^{2i\pi t}$$

- Morphisme: soit $t, u \in \mathbb{R}$,

$$\begin{aligned}\psi(t-u) &= e^{2i\pi(t-u)} = e^{2i\pi t - 2i\pi u} \\ &= e^{2i\pi t} \cdot (e^{-2i\pi u})^{-1}\end{aligned}$$

$$\psi(t-u) = \psi(t) \cdot \psi(u)^{-1}$$

- Définir \mathbb{R}/\mathbb{Z} : si $\bar{t} = \bar{u}$ dans \mathbb{R}/\mathbb{Z} ,
ie si $t = u + k$ et $k \in \mathbb{Z}$ alors

$$\begin{aligned}\psi(t) &= \psi(u+k) = e^{2i\pi u} \cdot e^{2i\pi k} = \psi(u). \\ \psi(t) &= \psi(u)\end{aligned}$$

On peut définir $\bar{\psi}: \mathbb{R}/\mathbb{Z} \rightarrow \mathbb{S}^1$

- $\bar{\psi}$ est injectif

Si $\bar{t} = \bar{u}$ dans \mathbb{R}/\mathbb{Z} , ie si $t = u + k$, $k \in \mathbb{Z}$
alors $\psi(t) = \psi(u+k) = e^{2i\pi u} \cdot e^{2i\pi k} = \psi(u)$

$$\begin{aligned}\text{soit } \bar{\psi}(t) &= \bar{\psi}(u), \text{ ie } \psi(t) = \psi(u), \\ e^{2i\pi t} &= e^{2i\pi u} \Leftrightarrow e^{2i\pi(t-u)} = 1\end{aligned}$$

dc $t-u \in \mathbb{Z}$, ie $\bar{t} = \bar{u}$.

- $\bar{\psi}$ est surjective (il s'agit de \mathbb{S}^1 possédant bien un antécédent).

Soit $z \in \mathbb{S}^1$, pt écrire $z = e^{i\theta}$ on a $|z| = 1$ & dc $z = e^{i\theta} = \psi\left(\frac{\theta}{2\pi}\right) = \bar{\psi}\left(\frac{\theta}{2\pi}\right)$

cl $\bar{\psi}: \mathbb{R}/\mathbb{Z} \rightarrow \mathbb{S}^1$ est isomorphisme de groupes.

Prop en + soit $\varphi: G \rightarrow H$ tq
 $\forall a, b: \varphi(a b^{-1}) = \varphi(a) \cdot \varphi(b)^{-1}$

Alors φ MDG.

Dm

• soit $a \in G$, $\varphi(1_G) = \varphi(a a^{-1})$
 $= \varphi(a) \cdot \varphi(a)^{-1} = 1$

• soit $a \in G$, $\varphi(a^{-1}) = \varphi(1_G \cdot a^{-1})$
 $= \varphi(1_G) \cdot \varphi(a)^{-1} = \varphi(a)^{-1}$

soit $a, b \in G$,

$$\varphi(ab) = \varphi(a(b^{-1})^{-1}) = \varphi(a) \varphi(b^{-1})^{-1} = \varphi(a) \varphi(b)$$

e) Mg le groupe quotient \mathbb{C}/\mathbb{R}
est isomorphe à \mathbb{R} .

M1 $\mathbb{C} \cong \mathbb{R} \times \mathbb{R}$

\downarrow quotient

$$\mathbb{C}/\mathbb{R} \cong (\mathbb{R} \times \mathbb{R})/\mathbb{R} \cong \mathbb{R}.$$

| M2 $f_m: \mathbb{C} \rightarrow \mathbb{R}$

• Morphisme: $a+ib, c+id \in \mathbb{C}$, alors

$$\begin{aligned} f_m((a+ib) - (c+id)) &= f_m((a-c) + i(b-d)) \\ &= b-d = f_m(a+ib) - f_m(c+id) \end{aligned}$$

• Ker(f_m) = \mathbb{R}

$$f_m(z) = 0 \Leftrightarrow z \in \mathbb{R}.$$

Donc $f_m: \mathbb{C}/\mathbb{R} \rightarrow \mathbb{R}$ est defined & injective.

• Surjectif: soit $n \in \mathbb{R}$, $x \in f_m(\mathbb{R})$.

al On a bien un isomorphisme de groupes
 $f_m: \mathbb{C}/\mathbb{R} \rightarrow \mathbb{R}$.

Ex 14

Soit $H, K \subsetneq \text{sg}$ d'un g de G .

a) Montrons que HUK est sg de G si $HCK = KCH$.

(\Leftarrow) si HCK alors $HUK = K$

si KCH alors $HUK = H$

Dès lors dans les 2 cas, HUK est sg de G .

(\Rightarrow) Supposons $H \not\subset K$ et $K \not\subset H$

alors $\exists h \in H$ tq $h \notin K$.

$\exists k \in K$ tq $k \notin H$.

Montrons que $hk \notin HUK$

• si $hk \in H$, alors $h = h(hk)h^{-1} \in H$.

Contd $\text{do } \text{?}$

• si $hk \in K$, alors $h = (hk)k^{-1} \in K$.

Contd $\text{do } \text{?}$

Donc $hk \notin HUK$.

HUK n'est donc pas stable par la loi de G , ce qui montre que HUK n'est pas un sg de G .

Par contre, si HUK est un sg de G , alors $HCK = KCH$.

b) Si $A, B \subsetneq \text{g}$ de G , on note

$$AB = \{ab \mid a \in A, b \in B\}.$$

Montrons que HK est sg de G si $HK = KH$.

(\Leftarrow) \triangleleft $HK = KH$ ne signifie pas que les éléments commutent.

Cela signifie seulement $hk \in HK \Rightarrow \exists h' \in H, k' \in K$ tq $hk = h'k'$.

Supposons $HK = KH$, soit $hk \in HK$, $h'k' \in HK$.

$$\text{alors } (hk)(h'k')^{-1} = \underbrace{hk}_{\in K} \underbrace{k'^{-1}h'^{-1}}_{\in H}$$

Donc $hk^{-1}h'^{-1} \in KH = HK$, $\exists h'' \in H, k'' \in K$ tq $hk^{-1}h'^{-1} = h''k''$.

Donc $(hk)(h'k')^{-1} = \underbrace{h h'' k''}_{\in H} \in HK$

Donc HK est bien un sg de G .

\Leftrightarrow Suppos HK $\neq KH$,

alors soit $\exists hk \in HK$ tq $hk \notin KH$.
soit $\exists kh \in KH$ tq $kh \notin HK$.

Quitte à échanger les rôles de H & K,
Suppos qu'on est du b 2° cas.

On a $hk = 1 \cdot k \in HK$
 $h = h \cdot 1 \in HK$.

Mais $hk \notin HK$.

De HK n'est pas un \textcircled{sg} de G.

Pour contraposée, si HK est un \textcircled{sg} de G,
alors $HK = KH$.

E+t

soit $G \textcircled{sg}$, le centre $Z(G) = \{g \in G, gx = xg, \forall x \in G\}$

a) Mg $Z(G)$ est \textcircled{sg} distingué commutatif de G

b) Mg G est commutatif $\Leftrightarrow Z(G) = G \Leftrightarrow \%_{Z(G)}$ monog.

~~*~~ \textcircled{sg} de G :

$\forall n \in G, n \cdot 1 = 1 \cdot n = n$ dc $1 \in Z(G)$

soit $g, h \in Z(G)$, alors $\forall n \in G$,

$(gh)n = gnh = n(gh)$, dc $gh \in Z(G)$.

soit $g \in Z(G)$ alors $\forall n \in G$,

$$(g^{-1}n)g = g^{-1}gn = n = (ng^{-1})g \Leftrightarrow g^{-1}n = ng^{-1}$$

dc $g^{-1} \in Z(G)$.

Donc $Z(G)$ est bien un \textcircled{sg} de G.

~~*~~ \textcircled{sg} distingué

soit $h \in Z(G), g \in G$, mg $ghg^{-1} \in Z(G)$

(alors $(ghg^{-1})x = gg^{-1}hx = xhgg^{-1} = x(ghg^{-1})$)

De $ghg^{-1} \in Z(G)$ d'où $Z(G) \triangleleft G$

alors $ghg^{-1} = hgg^{-1} = h \in Z(G)$ dc $Z(G) \triangleleft G$

\textcircled{sg} commutativité :

soit $g, h \in Z(G)$, alors $gh = hg$
car $g \in Z(G)$.

Donc $Z(G)$ est commutatif

Groupe quotient

G un \textcircled{g} , $H \textcircled{g}$

$G/H = \{gH, g \in G\} =$ classes d'équivalences pr
la relation $g Rh$ si $gh = hg$.

$H\backslash G = \{Hg, g \in G\}$: en général $H\backslash G \neq G/H$.

Supposons à présent que H est un \textcircled{g} distingué de G . En effet, cela signifie que

$$hg \in H, \quad gHg^{-1} = H$$

$$\Leftrightarrow hg \in H, \quad gh = hg.$$

On a alors $H\backslash G = G/H$.

On peut munir alors G/H de la loi

$$gH \cdot g'H = (gg')H$$

$\rightarrow G/H$ est alors de groupe, de neutre $H = \textcircled{H=1}$.
& l'inverse de gH est $g^{-1}H$.

$$\text{si } gH = \{gh \text{ pr } h \in H\}$$

Pour simplifier les manipulations, on peut écrire :

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

où $\bar{g} = gH$ est la classe de g par la relation $gRh \Leftrightarrow gh^{-1} \in H$.

La f $G \rightarrow G/H$ est un MDG

$$g \mapsto gH$$

Ex. \bullet $G = (\mathbb{Z}, +)$; $H = n\mathbb{Z}$ pr $n \in \mathbb{N}^*$.

$$H \triangleleft G, \quad G/H = \mathbb{Z}/n\mathbb{Z}.$$

\bullet $G = GL_n(\mathbb{R})$, $H = SL_n(\mathbb{R})$

$$= \{A \in GL_n(\mathbb{R}), \det(A) = 1\}$$

$$SL_n(\mathbb{R}) \triangleleft GL_n(\mathbb{R})$$

En effet, si $A \in SL_n(\mathbb{R})$, $P \in GL_n(\mathbb{R})$

$$\det(PAP^{-1}) = \det(P) \cdot \det(A) \cdot \det(P^{-1}) = 1$$

De $PAP^{-1} \in SL_n(\mathbb{R})$,

$SL_n(\mathbb{R})$ bien distingué.

soit $A, B \in GL_n(\mathbb{R})$

$$A SL_m(\mathbb{R}) = B SL_m(\mathbb{R}) \Leftrightarrow AB^{-1} \in SL_m(\mathbb{R})$$

$$\Leftrightarrow \det(AB^{-1}) = 1$$

$$\Leftrightarrow \det(A) \cdot \det(B^{-1}) = 1$$

$$\Leftrightarrow \det(A) = \det(B)$$

Donc $GL_n(\mathbb{R}) / SL_m(\mathbb{R})$ est l'ensemble de tous les déterminants, dc \mathbb{R}^* .

$\det: GL_n(\mathbb{R}) \rightarrow (\mathbb{R}^*)$ est un morphisme.

$\det: GL_n(\mathbb{R}) / SL_m(\mathbb{R}) \xrightarrow{\sim} (\mathbb{R}^*)$ est un isomorphisme

$$\text{tq } \ker(\det) = SL_m(\mathbb{R})$$

* Injectif? soit $x \in \mathbb{R}^*$, $x = \det \begin{pmatrix} x_1 & x \\ 0 & 1 \end{pmatrix}$ $\Leftrightarrow G/Z(G)$ est monog.

* injectif? soit A tq $\det(A) = 1$.

$$\text{tq } A \in SL_m(\mathbb{R})$$

$$\bar{A} = A SL_m(\mathbb{R}) = SL_m(\mathbb{R})$$

$$\bar{A} = 1_{GL_n(\mathbb{R}) / SL_m(\mathbb{R})}$$

Donc $\ker(\det) = \{1_{GL_n(\mathbb{R}) / SL_m(\mathbb{R})}\}$

mq $\boxed{\text{MDG}}$ est injectif, il suffit de mq le moyen est égal à 1.

Ex (f) Mg ASSE

G est commutatif $\Leftrightarrow Z(G) = G \Leftrightarrow G/Z(G)$ est monog.

(i) \Rightarrow (ii):

$Z(G) = \{g \in G, gn = ng, \forall n \in \mathbb{Z}\} = G$
car comme G est commutatif, tt est vérifié cela

(ii) \Rightarrow (iii) supposons $Z(G) = G$,
alors $G/Z(G) = G/G = \{gG, g \in G\} = \{G\}$
d'où $G/Z(G) \cong \{1\}$.

(iii) \Rightarrow (i) sps $G/Z(G) = \langle \bar{g} \rangle = \langle gZ(G) \rangle$

cela signifie que si $\bar{g} \in G$ alors $\exists m \in \mathbb{Z}$
tq $\bar{g} \in Z(G) = g^m Z(G)$

(iii) \Rightarrow (i) opps $\mathbb{Z}(G) = \langle \bar{g} \rangle = \langle g \mathbb{Z}(G) \rangle$

ce qui signifie que si $g' \in G$

alors $\exists m \in \mathbb{Z}$ tq $g' \mathbb{Z}(G) = g^m \mathbb{Z}(G)$

i.e., tt elt $g' \in G$ s'écrit

$$g' = g^m h \quad \forall m \in \mathbb{Z}, h \in \mathbb{Z}(G)$$

soit $g', g'' \in G$,

$$\text{on écrit } g' = g^m h \quad \text{et } m, n \in \mathbb{Z} \\ g'' = g^n k \quad h, k \in \mathbb{Z}(G)$$

$$\text{alors } g'g'' = g^m h g^n k = g^m g^n h k = g^m g^n k h \\ = g^{m+n} h k \Rightarrow g'g'' = g''g'$$

Donc G est commutatif.

Ex 18 Groupe dérivé

soit G un \mathbb{G} , le groupe dérivé de G est le \mathbb{G}

de G engendré par les commutateurs :

$$\mathcal{D}(G) = \langle ghg^{-1}h^{-1} \mid g, h \in G \rangle$$

Mq $\mathcal{D}(G)$ est le plus petit \mathbb{G} distingué de G pour lequel le \mathbb{G} quotient $G/\mathcal{D}(G)$ est commutatif.

$\mathcal{D}(G)$ \mathbb{G} distingué ?

soit $c = ghg^{-1}h^{-1}$ un commutateur,

$$\text{soit } a \in G, \text{ alors } acca^{-1} = agh g^{-1} h^{-1} a^{-1} \\ = [(ag)h(a g)^{-1} h^{-1}] [h a h^{-1} a^{-1}] \in \mathcal{D}(G)$$

comme $(ghg^{-1}h^{-1})^{-1} = hgh^{-1}g^{-1}$, tout elt de $\mathcal{D}(G)$ se écrit $c_1 \dots c_n$ + c_i des commutateurs.

$$\text{si } a \in G, \text{ on a } a(c_1 \dots c_n)a^{-1} = \\ (a \cdot c_1 a^{-1}) \dots (a c_n a^{-1}) \in \mathcal{D}(G).$$

Donc $aD(G)a^{-1} \subset D(G) \quad \forall a \in G.$

D'où $D(G) \triangleleft G.$

• $G/D(G)$ est commutatif

soit $g, h \in G.$

On a $ghg^{-1}h^{-1} \in D(G)$

Donc dans $G/D(G), \quad ghg^{-1}h^{-1} = \underline{1} \stackrel{G/D(G)}{=} D(G) = D(G)$

$$ghg^{-1}h^{-1} = \underline{1} = ghg^{-1}h^{-1}D(G) = D(G)$$

$$\overline{g} \overline{h} = \overline{h} \overline{g}$$

Donc $G/D(G)$ est commutatif.

• $D(G)$ minimal par cette prop'

soit $H \triangleleft G$ tq G/H est commutatif.

soit $\overline{g}, \overline{h} \in G$, alors ds G/H ,

$$\overline{g} \overline{h} \overline{g}^{-1} \overline{h}^{-1} = \underline{1}$$

$$\text{de } ghg^{-1}h^{-1} \in H.$$

H contient tous les commutateurs.

• Donc H contient $D(G).$

$D(G)$ est bien le + petit \circledcirc distingué de G tq $G/D(G)$ commute.

(+ petit : il est contenu de n'importe quel \circledcirc)

Ex 20 soit $G \circledcirc$, $\forall g \in G, \varphi_g: G \rightarrow G$

a) Vérifier φ_g est automorphisme de G . $x \mapsto g x g^{-1}$ une op

b) Vérifier que $\text{Aut}(G)$ des automorphismes de G est un groupe (par la loi de composition).

c) Montrer l'appli $\psi: G \rightarrow \text{Aut}(G), g \mapsto \varphi_g$ est un M.D.G

d) Déterminer le Im de ψ

e) Montrer l'image de ψ est \circledcirc distingué de $\text{Aut}(G)$.

Résultat Exo $g \in G$, $\psi_g : G \rightarrow G$,

$$\psi_g(x) = g x g^{-1} \quad \forall x \in G.$$

a) Vérifions ψ_g est automorphisme de G .

$$\psi_g : \begin{array}{ccc} G & \longrightarrow & G \\ x & \longmapsto & g x g^{-1} \end{array}$$

ψ_g est un morphisme $\forall x, y \in G$.

$$\begin{aligned} \psi_g(xy) &= g(xg^{-1})g^{-1} = g x g^{-1} g g^{-1} \\ &= (gxg^{-1})gyg^{-1} \end{aligned}$$

$$\psi_g(xy) = \psi_g(x) \cdot \psi_g(y)$$

ψ_g est une bijection

$$\begin{aligned} \psi_g(x) = y &\Leftrightarrow g x g^{-1} = y \\ &\Leftrightarrow x = g^{-1} y g \\ &\Leftrightarrow x = \psi_{g^{-1}}(y) \end{aligned}$$

ψ_g est bien bijective et l'inverse ψ_g^{-1} .

Donc $\psi_g : G \rightarrow G$ est bien automorphisme. (26)

b) Vérifier $\text{Aut}(G)$ est un (G).

$\text{Aut}(G)$ est associatif.

$a, b, c \in \text{Aut}(G), x \in G$,

$$\begin{aligned} (a \circ b) \circ c(x) &= (a \circ b)(c(x)) = a(b(c(x))) \\ &= a(b \circ c(x)) = a \circ (b \circ c)(x) \end{aligned}$$

Donc $(a \circ b) \circ c = a \circ (b \circ c)$.

$\text{Aut}(G)$ est stable par composition

si $\varphi, \psi \in \text{Aut}(G)$; $\varphi \circ \psi$ est toujours bijective
& $\forall x, y \in G$,

$$(\varphi \circ \psi)(xy) = \varphi(\psi(x)\psi(y)) = (\varphi \circ \psi)(x)(\varphi \circ \psi)(y)$$

Donc $\varphi \circ \psi$ est encore un automorphisme

Neutre

On cherche un neutre $\varepsilon \in \text{Aut}(G)$ alors

$$\forall \varphi \in \text{Aut}(G), \varepsilon \circ \varphi = \varphi \circ \varepsilon = \varphi \text{ i.e. } \forall x \in G$$

$$\varepsilon(\varphi(x)) = \varphi(\varepsilon(x)) = \varphi(x)$$

Possible si $\varepsilon = \text{Id}_G$. Donc Id_G est le neutre de $\text{Aut}(G)$

Inverse soit $\varphi \in \text{Aut}(G)$,

de φ possède une réciproque $\varphi^{-1}: G \rightarrow G$

$$\text{tq } \varphi \circ \varphi^{-1} = \varphi^{-1} \circ \varphi = \text{Id}_G$$

φ^{-1} est-il un automorphisme ?

On sait déjà que c'est une bijection.

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

De plus $\varphi \circ \varphi^{-1} = \text{Id}_G$ et bien $\varphi: G \rightarrow \text{Aut}(G)$

Donc φ^{-1} est bien un morphisme, de plus un automorphisme,

$\Rightarrow (\text{Aut}(G), \circ)$ est bien un \textcircled{g} .

$$\begin{aligned} \text{B}^* &= \varphi(\varphi^{-1}(x) \varphi^{-1}(y)) \\ &= \varphi(\varphi^{-1}(x) \varphi^{-1}(y)) \quad \downarrow \varphi \text{ injectif} \\ \varphi^{-1}(xy) &= \varphi^{-1}(x) \varphi^{-1}(y). \end{aligned}$$

c) $M_\varphi: \varphi: G \rightarrow \text{Aut}(G)$ et $M.D.G$

soit $g, h \in G$, on a $\varphi(gh) = \varphi(g)\varphi(h)$

soit $x \in G$,

$$\begin{aligned} \varphi_{gh}(x) &= (gh)x(gh)^{-1} = ghxh^{-1}g^{-1} = g(hxh^{-1})g^{-1} \\ &= \varphi_g \circ \varphi_h(x) \end{aligned}$$

et bien $\varphi: G \rightarrow \text{Aut}(G)$

d) Déterminer le noyau de φ .

$$\begin{aligned} \text{ker } \varphi &= \{g \in G, \varphi_g = \text{Id}_G\} \\ &= \{g \in G, \forall x \in G, gxg^{-1} = x\} \\ &= \{g \in G, \forall x \in G, gx = xg\} = Z(G). \end{aligned}$$

e) M_φ l'image de φ est \textcircled{g} distinguée de $\text{Aut}(G)$.

$$\begin{aligned} \text{soit } \varphi_g &\in \text{Im } \varphi, \text{ soit } \varphi \in \text{Aut}(G), \\ \text{alors } \forall x &\in G, \varphi \circ \varphi_g \circ \varphi^{-1}(x) = (\varphi \circ \varphi_g)(\varphi^{-1}(x)) \\ &= \varphi(g \varphi^{-1}(x) g^{-1}) = \varphi_g \circ \varphi \varphi^{-1}(x) \circ \varphi(g^{-1}) \\ &= \varphi(g) x (\varphi(g))^{-1} = \varphi_{\varphi(g)}(x) \in \text{Im } \varphi \end{aligned}$$

$\textcircled{27} \Rightarrow \text{Im } \varphi \subset \text{Aut}(G)$

Actions de Groupes

- Une **action** de groupe G sur l'ens A , c'est une application $G \times A \rightarrow A$

$$(g, a) \mapsto g \cdot a$$

Vérifiant:

$$\textcircled{1} \quad \forall a \in A, 1_G \cdot a = a$$

$$\textcircled{2} \quad \forall g, h \in G, \forall a \in A, g \cdot (h \cdot a) = (gh) \cdot a$$

- RQ** Une action de groupe, c'est la donnée d'un morphisme $\theta \rightarrow S(A)$ permétais des élts de A .



1. Le stabilisateur d'un élét de A , c'est

$$\text{Stab}_a = \{g \in G, g \cdot a = a\}$$

Stab_a est un sg de G .

Ex 29 Déterminer les orbites de l'action de $GL_n(\mathbb{R})$ sur \mathbb{R}^n .

L'action de $GL_n(\mathbb{R})$ sur \mathbb{R}^n . Prendre $A \cdot x = g(x)$ où $g \in GL(\mathbb{R}^n)$ est l'isomorphisme associé à A de la base canoniq ue voir les élts de \mathbb{R}^n à des matrices colonnes $1 \times n$ telles $A \cdot X = AX$.

$GL_n(\mathbb{R}) \curvearrowright \mathbb{R}^n$ (opér)

On va voir \mathbb{R}^n à l'ens des vect^{rs} colonnes $\mathbb{C}^{1 \times n}(\mathbb{R})$ L'action est $A \cdot x = AX$.

Vérifions c'est bien une act de groupe.

1) soit $x \in \mathbb{R}^n$, $I_n \cdot x = x$

2) soit $A, B \in GL_n(\mathbb{R})$, $x \in \mathbb{R}^n$

$$A \cdot (B \cdot x) = A \cdot (BX) = ABX = (AB)X.$$

soit $X \in \mathbb{R}^n$, l'orbite de X est

$$\mathcal{O}_X = \{A \cdot X \text{ pour } A \in GL_n(\mathbb{R})\}$$

$$\mathcal{O}_X = \{Y \in \mathbb{R}^n \text{ tq } Y = AX\}.$$

On cherche à déterminer à X fixé tous les $Y \in \mathbb{R}^n$ qui peuvent être obtenus par multiplication de X par une matrice de $GL_n(\mathbb{R})$.

Il faudra faire une distinction de cas entre le cas où $X=0$ & le cas où $X \in \mathbb{R}^n \setminus \{0\}$.

cas $X=0$:

Pour la matrice $g \in GL_n(\mathbb{R})$, $g \cdot 0 = g(0) = 0$.

$$\text{Donc } \mathcal{O}_0 = \{0\}.$$

en $X \in \mathbb{R}^n \setminus \{0\}$:

soit $y \in \mathbb{R}^n \setminus \{0\}$,

→ soit B_1 une base de \mathbb{R}^n dont le 1^{er} vecteur est x .

→ soit B_2 une base de \mathbb{R}^n dont le 1^{er} vecteur est y .

soit $g \in GL_n(\mathbb{R})$ la mat de passage de B_1 à B_2 .
Alors $g \cdot x = y$.

$$\text{Donc si } n \neq 0, \mathcal{O}_x = \mathbb{R}^n \setminus \{0\}.$$

Ex 30

Vérifier \mathbb{R} agit sur \mathbb{C} par $(\theta, z) \in \mathbb{R} \times \mathbb{C}$

→ $\theta \cdot z = e^{i\theta} z$. Décrire les orbites de cette action.

$\mathbb{R} \curvearrowright \mathbb{C}$, $\theta \cdot z = e^{i\theta} z$, soit $z \in \mathbb{C}$ alors $\forall \theta \in \mathbb{R}$

$$|\theta \cdot z| = |e^{i\theta} z| = |e^{i\theta}| \cdot |z| = |z|$$

Réiproquement, si $|z| = |z'| \neq 0$ alors $|\frac{z'}{z}| = \frac{|z'|}{|z|} = 1$

de $\exists \theta \in \mathbb{R}$ tq $\frac{z'}{z} = e^{i\theta}$ i.e. $z' = z \cdot e^{i\theta} = \theta \cdot z$.

$$\text{Or: } \mathcal{O}_z = S^1(0, 1).$$

Les orbites sont les cercles de centre 0.

Prop^m Soit $G \curvearrowright X$, $\forall x \in X$,
l' n est un bijo $\varphi: G/\text{stab}(n) \rightarrow \Omega_n$.

TH (Équations formelles aux classes)

Soit $G \curvearrowright X$, X fini

soit x_1, \dots, x_n des représentants des orbites

alors $|X| = \sum_{i=1}^n [G : \text{stab}(x_i)] = \frac{|G|}{|\text{stab}(x_i)|}$

Démonstration $|X| = \sum_{i=1}^n |\Omega_{x_i}| = \sum_{i=1}^n |G/\text{stab}(x_i)|$
 $= \sum_{i=1}^n [G : \text{stab}(x_i)]$

Ex 33 FF de Burnside

Soit G fini agissant sur un X fini. Pq $g \in G$,
on note $\chi(g)$ le nbr de pts de X fixés par g .

Mg

N = $\frac{1}{|G|} \sum_{g \in G} (\chi(g))$ — nbr pts X fixés par g
 nbr orbites de l'act.

On dénombre $S = \{(g, n) \in G \times X, g \cdot n = n\}$.
de 2 manières différentes.

M.1 $S = \bigcup_{g \in G} \{(g, n), \exists n \in X \text{ tq } g \cdot n = n\}$.

$$|S| = \sum_{g \in G} \chi(g)$$

M.2 $S = \bigcup_{n \in X} \{(g, n) \text{ tq } g \in G \text{ tq } g \cdot n = n\}$.

$$S = \bigcup_{x \in X} \{(g, n) \text{ tq } g \in \text{stab}(n)\}.$$

$$|S| = \sum_{x \in X} |\text{stab}(n)|$$

soit x_1, \dots, x_N des représentants des orbites.

$$\begin{aligned} |S| &= \sum_{i=1}^N \sum_{n \in \Omega_{x_i}} |\text{stab}(n)| \\ &= \sum_{i=1}^N |\Omega_{x_i}| \times |\text{stab}(x_i)| \\ &= \sum_{i=1}^N \frac{|G|}{|\text{stab}(x_i)|} \times |\text{stab}(x_i)| = N \cdot |G| = |S| \end{aligned}$$

(30)

cl

$$N \times |G| = \sum_{g \in G} \chi(g)$$

$$\Rightarrow N = \frac{1}{|G|} \sum_{g \in G} \chi(g)$$



Bonus

On a des perles de 3 couleurs différentes.
Combien de bracelets différents peut-on faire de 5 perles?

$$\text{cl}R = \{R, V, B\}$$

Appliquer
 Bonnadoise.

$$\begin{matrix} R & R \\ R & V \\ R & B \end{matrix} \quad \begin{matrix} V & V \\ V & B \\ V & R \end{matrix} = \begin{matrix} R & B \\ B & R \end{matrix} \quad \text{Rotat.}$$

Ex 35 (Normalisateur d'un sg)

soit G gr , H sg de G . Le normalisateur de H de G est

$$N_G(H) = \{g \in G \mid gHg^{-1} = H\}$$

a) Montrer que $N_G(H)$ est le plus petit sg de G contenant H
Il est sg distingué.

b) Montrer que le nombre de sg distincts conjugués de H de G est égal $[G : N_G(H)]$

a) $N_G(H) = \{g \in G, gHg^{-1} = H\}$

Montrer c'est sg

montrer $1H1^{-1} = H$ de $1 \in N_G(H)$.

montrer $g \in N_G(H)$, $g^{-1}Hg = g^{-1}(gHg^{-1})g = H$ de $g^{-1} \in N_G(H)$

stabilité $g, h \in N_G(H)$, $(gh)^{-1}H(gh) = ghHh^{-1}g^{-1} = gHg^{-1} = H$,
 $gh \in N_G(H)$.

Donc $N_G(H)$ est sg de G .

soit $h \in H$, $hHh^{-1} = H$ de $h \in N_G(H)$, $H \subset N_G(H)$

soit $g \in N_G(H)$, $gHg^{-1} = H$ par définition, d'où $H \subset N_G(H)$.

le + grad :

soit $K \triangleleft G$ contenant H & tq $H \triangleleft K$.

si $g \in K$, $\hat{e} H$ est distingué de K ,

$$gHg^{-1} = H.$$

De $K \subset N_G(H)$.

$N_G(H)$ est de bien le + grad \triangleleft .

b) Nombre de distincts conjugués de H de G est égal à $[G : N_G(H)]$.

On prend l'ordre suivante de G sur les \triangleleft de G def p $g \cdot K = gKg^{-1}$

Alors \mathcal{Q}_H est l'ensemble des \triangleleft conjugués à H .

$N_G(H) = \text{Stab}(H)$. $\triangleleft \triangleleft^{\text{voir}}$

Donc \mathcal{Q}_H est en bijection de $G/\text{Stab}(H)$.

ie l'ensemble des \triangleleft de G conjugués à H est en bijection avec $G/N_G(H)$. (32)

Le nombre de \triangleleft de G conjugués à H est de $|G/N_G(H)| = [G : N_G(H)]$.

$$\{gHg^{-1}, g \in G\}; N_G(H) = \{g \in G, gHg^{-1} = H\}.$$

Ex 36 Th de Cayley.

Mq \triangleleft s'injecte dans $\text{Bij}(G)$

indic: faire agir G sur lui-même par translation à gauche

Comme toute action, elle définit un morphisme: $\pi: G \rightarrow \text{Bij}(G)$

$$g \mapsto \pi_g$$

$$\text{où } \pi_g(n) = g \cdot n = gn.$$

soit $g \in \ker \varphi$ alors $\varphi_g = \text{Id}_G$

$$\varphi_g(1) = 1$$

$$g \cdot 1 = 1$$

$$g = 1$$

Donc $\ker \varphi = \{1\}$, φ est bien une injection $G \hookrightarrow \text{Bij}(G)$.

Eo37 Mg \mathfrak{G} fini G d'ordre pair possède un élé d'ordre 2.

indic $\varepsilon \cdot n = n^2$, considère act $\{1, -1\} \times G$.
Considérons l'act $\{1, -1\} \times G$,
def p. $\varepsilon \cdot g = g^\varepsilon$

Vérifions que c'est bien une act :

- $1 \cdot g = g^{-1} = g$
- $1 \cdot (1 \cdot g) = g = (1 \times 1)g$
- $-1 \cdot (1 \cdot g) = (1 \cdot (-1 \cdot g)) = g^{-1} = (-1 \times 1)g$
- $-1 \cdot (-1 \cdot g) = -1 \cdot g^{-1} = g = (-1 \times -1)g$

\Rightarrow c'est bien une act de groupe.

On peut de appliquer l'équation aux classes (formule des classes)
soit x_1, \dots, x_r une sélect des représentants
des orbites, alors $|G| = \sum_{i=1}^r |\Omega_{x_i}|$

$|G|$ est pair.

- $\Omega_{x_i} = \{1 \cdot x_i, -1 \cdot x_i\} = \{x_i, x_i^{-1}\}$
- Donc $|\Omega_{x_i}| = 1$ ou 2.
- $|\Omega_{x_i}| = 1 \Leftrightarrow x_i^{-1} = x_i \Leftrightarrow x_i^2 = 1$.

De sh x_i est l'natte ou d'ordre 2.

Qd étant donné que $|\Omega_1| = 1$, si on veut que la somme $\sum_{i=1}^r |\Omega_{x_i}|$ soit bien paire,
il faut qu' $\exists i$ $x_i \neq 1$ tq $|\Omega_{x_i}| = 2$.

Un tel x_i est bien un élé d'ordre 2.

Ex 22 Lemme de Cauchy

soit $G \neq \emptyset$ fini, p fact^e premier de $|G|$.

Mo G possède est d'ordre p .

Indic considérons p -cycle $\sigma = (12\cdots p) \in S_p$

Q l'ac^e du \emptyset cycliq $\langle \sigma \rangle$ si t'ens

$$X = \{(g_1, \dots, g_p) \in G^P \mid g_1 \cdots g_p = 1\}$$

def f $\tau \cdot (g_1, \dots, g_p) = (g_{\tau(1)}, \dots, g_{\tau(p)})$.

G \emptyset fini, $p \nmid |G|$, considérons $\sigma = (1\cdots p) \in S_p$. $X = \{(g_1, \dots, g_p) \text{ tq } g_1 \cdots g_p = 1\}$

$$\langle \sigma \rangle \subset S_p.$$

$$\langle \sigma \rangle = \{(12\cdots p), (135\cdots p+2), \dots, \sigma^p = \text{id}\}$$

$$\cdot |\langle \sigma \rangle| = p$$

$$\text{soit } X = \{(g_1, \dots, g_p) \text{ tq } g_1 \cdots g_p = 1\}.$$

$$\langle \sigma \rangle \cap X$$

$$\sigma(g_1, \dots, g_p) = (g_{\sigma(1)}, \dots, g_{\sigma(p)})$$

$$\text{id. } (g_1, \dots, g_p) = (g_1, \dots, g_p)$$

$$\sigma(g_1, \dots, g_p) = (g_2, g_3, \dots, g_p)$$

$$\tau^e(g_1, \dots, g_p) = (g_3, g_1, \dots, g_2)$$

$$\tau^p(g_1, \dots, g_p) = (g_4, \dots, g_p)$$

$$\underline{\text{Équat aux classes}}: |X| = \sum_{i=1}^n |\Omega_{x_i}|$$

$$\rightarrow |X| = ?$$

$\rightarrow Q^u$ et v^u possibles pr $|\Omega_{x_i}|$, do quel cas
 $|\Omega_{x_i}|$ vaut une valeur donnée.
 $(\Leftrightarrow x_i = (g_1^i, \dots, g_p^i))$

$$X = \{(g_1, \dots, g_p) \text{ tq } g_1 \cdots g_p = 1\}$$

$$\text{si } g_1 \cdots g_p = 1 \Leftrightarrow g_p = g_{p-1}^{-1} \cdots g_1^{-1}.$$

i.e., on a une bijecto $G^{P-1} \rightarrow X$

$$(g_1, \dots, g_{p-1}) \mapsto (g_1, \dots, g_{p-1}, g_p^{-1}, \dots, g_1^{-1})$$

$$\text{Done } |X| = |G^{P-1}| = |G|^{p-1}$$

$$\mathcal{R}(g_1, \dots, g_p) = \left\{ (g_1, \dots, g_p), (g_2, g_3, \dots, g_p, g_1), \right. \\ \left. (g_3, g_4, \dots, g_p), \dots, (g_p, g_1, \dots, g_{p-1}) \right\}$$

$\circ (g_1, \dots, g_p) = (g_2, g_3, \dots, g_p)$.
(R^o p est premier)

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

10/20

Ex 1: 4/6

OK!

a) Soit $I_1 = \int_0^\infty t^3 \sin(t) e^{-t} dt$, I_1 est généralisée en $+\infty$,
soit $X > 0$ tel que $X \rightarrow +\infty$. La fonction $t \mapsto t^3 \sin(t) e^{-t}$
est bien définie et continue sur $[0, \infty]$ donc localement
intégrable sur $[0, \infty]$.

0,5

Puis $0 \leq |t^3 \sin(t) e^{-t}| \leq t^3 e^{-t} \leq 1$ pourquoi?

Gr $\int_{\frac{X}{2}}^{X \rightarrow \infty} \frac{1}{X^3} dX$ est une intégrable ok Riemann convergente.
(Donc $\int_0^\infty \frac{1}{t^3} dt$ converge aussi)

Comme I_1 et $\int_0^\infty \frac{1}{t^3} dt$ sont de mêmes signes,
 I_1 converge aussi.

A Votre raison
1 montre séries
que $\int_0^{+\infty} e^{-t} dt$ de cr.

b) Soit $I_2 = \int_0^1 \frac{t^2}{1 - \cos^2(t)} dt$ suivant $\lambda \in \mathbb{R}$.

1,5

La fonction $t \mapsto \frac{t^2}{1 - \cos^2(t)}$ est bien définie et continue

sur $[0, 1]$, donc localement intégrable sur $[0, 1]$.

Il y a un problème en 0 car $1 - \cos^2(0) = 1 - 1 = 0$!

1

$\alpha \in \mathbb{R}$ $I_2 = \int_1^{\infty} \frac{t^2}{1-\cos^2(t)} dt$, $\cos(t) \underset{t \rightarrow 0}{\sim} 1 - \frac{t^2}{2} + o(t^2)$
 $\cos^2(t) \underset{t \rightarrow 0}{\sim} (1 - \frac{t^2}{2})(1 - \frac{t^2}{2}) = 1 - t^2 + o(t^4)$

D'où $1 - \cos^2(t) \underset{t \rightarrow 0}{\sim} t^2$. En voisinage de 0 : $\frac{t^2}{1-\cos^2(t)} \underset{t \rightarrow 0}{\sim} \frac{t^2}{t^2} = 1$

En cette intégrale converge si $2-\alpha < 1$ si $1 < \alpha$. B

En voisinage de 1 : $\frac{t^2}{1-\cos^2(t)} \underset{t \rightarrow 1}{\sim} +\infty$. En cette intégrale converge
si $-\alpha > 2$
 $\alpha < -2$

D'où I_2 converge si $\alpha \in]-\infty, -2] \cup [1, \infty[$

En 1, il n'y a aucun problème, fonction continue!

c) Soit $I_3 = \int_1^{\infty} \left(1+t^2 \ln\left(\frac{t^2}{t^2+1}\right)\right) dt$, la fonction

$t \mapsto 1+t^2 \ln\left(\frac{t^2}{t^2+1}\right)$ est une fonction continue sur $[1, \infty[$
et définie sur \mathbb{R} car $\forall t \in [1, \infty[; \frac{t^2}{t^2+1} > 0$. Donc la fonction est localement

intégrable sur $(1, \infty[$. I_3 est généralisée en ∞ .

Soit $x > 0$ tel que $x \rightarrow \infty$.

Si $\ln\left(\frac{t^2}{t^2+1}\right) = -\ln\left(1+\frac{1}{t^2}\right)$ et $\ln(1+u) \underset{u \rightarrow 0}{\sim} u - \frac{u^2}{2} + o(u^2)$

D'où $-t^2 \ln\left(1+\frac{1}{t^2}\right) \underset{t \rightarrow \infty}{\sim} -1 + \frac{1}{2t^2} + o\left(\frac{1}{t^2}\right)$

Puis $1+t^2 \ln\left(\frac{t^2}{t^2+1}\right) \underset{t \rightarrow \infty}{\sim} 1 + \frac{1}{2t^2} + o\left(\frac{1}{t^2}\right)$

on $1+t^2 \ln\left(\frac{t^2}{t^2+1}\right)$ et $\frac{1}{2t^2}$ sont de mêmes signes.

De plus $\int_1^{\infty} \frac{1}{2t^2} dt$ est une intégrale de Riemann convergente TB

Donc I_3 est aussi une intégrale qui converge.

Ex 2 : Posons $x > 0$: $F(x) = \int_0^{x/2} \ln(x^2 + \sin^2(t)) dt$ (e2)

(6/15)

a) Montrons que F est bien définie et continue sur $]0, \infty[$.
soit $(x, t) \mapsto \ln(x^2 + \sin^2(t))$ est bien définie si $x^2 + \sin^2(t) > 0$
Théorème ! avec $x > 0$, la condition est vérifiée donc F est bien définie et continue sur $]0, \infty[$.

b) soit $f:]0, \infty[\times [0, \frac{\pi}{2}] \rightarrow \mathbb{R}$

$$(x, t) \mapsto \ln(x^2 + \sin^2(t))$$

f est bien définie et continue sur $]0, \infty[$.

Calculons $\frac{\partial f}{\partial x}(x, t) = \frac{2x}{x^2 + \sin^2(t)}$, la dérivée partielle en x existe et est bien continue

sur $]0, \infty[$. Donc F est de classe C^1 sur $]0, \infty[$.

Pour $x > 0$, $F'(x) = \int_0^{x/2} \frac{\partial f}{\partial x}(x, t) dt$ 3

$$F'(x) = \int_0^{x/2} \frac{2x}{x^2 + \sin^2(t)} dt$$

\triangle $\frac{\partial f}{\partial x}$ est une fonction de 2 variables.

(3)

c) Montrons que $\forall t \in [0, \frac{\pi}{2}]$, on a :

$$\sin^2(t) = \frac{\tan^2(t)}{1 + \tan^2(t)} \quad \text{et} \quad \tan'(t) = 1 + \tan^2(t)$$

Le qui équivaut à montrer $\sin^2(t) = \frac{\tan^2(t)}{1 + \tan^2(t)} = \frac{\tan^2(t)}{(\tan(t))'}$
ie : $\tan^2(t) = (\tan(t))' \cdot \sin^2(t)$. (en posant $t = \arctan(u)$)

$$\text{Calculons } \tan^2(t) = \left(\frac{\sin^2(t)}{\cos^2(t)} \right)' = \frac{1}{\cos^2(t)} \times \sin^2(t) = (\tan(t))' \cdot \sin^2(t)$$

d) Soit $x > 0$, on pose $u = \tan(t)$ et $\sin^2(t) = \frac{u^2}{1+u^2}$
et on a $dt = \frac{du}{1+u^2}$.

0.5

$$F'(x) = \int_0^\infty \frac{2x}{x^2 + \frac{u^2}{1+u^2}} \frac{1}{1+u^2} du = 2x \int_0^\infty \frac{1}{x^2(1+u^2) + u^2} du$$

$$= \frac{2x}{x^2} \int_0^\infty \frac{1}{x^2 + \left(\frac{u}{\sqrt{1+u^2}}\right)^2} du = 2x \left[\frac{\sqrt{1+u^2}}{u} \arctan\left(\frac{x\sqrt{1+u^2}}{u}\right) \right]_0^\infty$$

$$= \frac{2x}{\sqrt{1+x^2}} \left[\arctan\left(\frac{x\sqrt{1+u^2}}{u}\right) \right]_0^\infty = \frac{e}{\sqrt{1+x^2}} \frac{\pi}{2} = \frac{\pi}{\sqrt{1+x^2}}$$

Après calcul, on obtient d'après l'énoncé $F'(x) = \frac{\pi}{\sqrt{1+x^2}}$, $x > 0$.

4

Définition
Monotonie $(\ln(u))'$ $= \frac{1}{u} \ln(u) \frac{u}{u} = \frac{1}{u}$

e) On a $G(x) = \pi \ln(x + \sqrt{1+x^2})$, $x > 0$.

Montrons qu'il existe $A \in \mathbb{R}$ tq $\forall x > 0$:

$$F(x) = G(x) + A$$

Le qui revient à montrer que $F'(x) = G'(x)$

$$G'(x) = \pi \ln\left(x + \frac{x}{\sqrt{1+x^2}}\right) \left(x + \sqrt{1+x^2}\right) = \pi x + \sqrt{1+x^2}$$

f) Montrons que $\forall x > 0$: on a $F(x) - \pi \ln(x) = \int_0^{\pi/2} \ln\left(1 + \frac{\sin^2(t)}{x^2}\right) dt$

$$\text{on sait que } F(x) - F(0) = \int_0^x F'(t) dt$$

5

g) On veut en déduire que $\forall n > 0$,

$$0 \leq F(x) - \pi \ln(n) \leq \frac{\pi}{2n^2}$$

$$0 \leq F(x) - \pi \ln(n) = \int_0^{\pi/2} \ln\left(1 + \frac{\sin^2(t)}{x^2}\right) dt \quad \text{d'après g)}$$

$$\leq \int_0^{\pi/2} \frac{\sin^2(t)}{x^2} dt = \frac{1}{x^2} \int_0^{\pi/2} \sin^2(t) dt = \frac{1}{x^2} \int_0^{\pi/2} \frac{1 - \cos(2t)}{2} dt$$

$$= \frac{1}{2x^2} \int_0^{\pi/2} 1 - \cos(2t) dt = \frac{1}{2x^2} \left(\int_0^{\pi/2} dt - \int_0^{\pi/2} \cos(2t) dt \right)$$

$$= \frac{1}{2x^2} \left[t \right]_0^{\pi/2} - \frac{1}{2x^2} \left[\frac{1}{2} \sin(2t) \right]_0^{\pi/2}$$

$$= \frac{\pi}{4x^2} + \frac{\pi}{8x^2} = \frac{\pi}{2x^2}.$$

$$\text{Donc } \forall n > 0, 0 \leq F(n) - \pi \ln(n) \leq \frac{\pi}{2n^2}.$$

h) D'après g) on a $0 \leq F(n) - \pi \ln(n) \leq \frac{\pi}{2n^2}$.

Or $\lim_{n \rightarrow \infty} \frac{\pi}{2n^2} = 0$, donc par le théorème des gendarmes :

$$\lim_{n \rightarrow \infty} F(n) - \pi \ln(n) = 0$$

$$\text{NON ! Ainsi } F(n) = \pi \ln(n).$$

D'après c) $F(a) = G(a) + A$

$$\Leftrightarrow A = F(x) - G(x)$$

$$A = \pi \ln(n) - \pi \ln\left(x + \sqrt{1+x^2}\right), x > 0$$

$$A = \pi \ln\left(\frac{x}{x + \sqrt{1+x^2}}\right)$$

$$\mathcal{R}(g_1, \dots, g_p) = \left\{ (g_1, \dots, g_p), (g_2, g_3, \dots, g_p, g_1), \dots, (g_3, g_4, \dots, g_1), \dots, (g_p, g_1, \dots, g_{p-1}) \right\}$$

V k ∈ ℕV, $\tau^k \cdot x = (g_1, \dots, g_k)$ = x
Donc $\mathcal{L}_x = \{x\}$, $|\mathcal{L}_x| = 1$.

Ex $(g_1, \dots, g_p) = (g_4, g_5, \dots, g_3)$.
(Rq p est premier)

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

$$|X| = |G^{p-1}| = |G|^{p-1}$$

$$|\mathcal{L}_{x_i}| = ?$$

$$x = (g_1, \dots, g_p) \in X,$$

$$\mathcal{L}_x = \{ \tau \cdot x, \tau \in \langle \tau \rangle \}$$

$$\mathcal{L}_x = \{ \text{Id} \cdot (g_1, \dots, g_p); \tau \cdot (g_1, \dots, g_p), \dots, \tau^{p-1} \cdot (g_1, \dots, g_p) \}$$

$$\mathcal{L}_x = \{(g_1, \dots, g_p), (g_2, g_3, \dots, g_p, g_1), \dots, (g_p, g_1, \dots, g_{p-1})\}$$

~~Supposons que tous les g_i sont différents~~

→ tous les g_i sont égaux, i.e. $x = (g, \dots, g)$

→ Réciproquement, supposons $|\mathcal{L}_x| < p$:

Alors $\exists k \in \{1, \dots, p-1\}$ tq $\tau^k \cdot x = x$.

$$(g \tau^k(p), \dots, g \tau^k(1)) = (g_1, \dots, g_p)$$

Donc $g \tau^k(1) = g_1, g \tau^k(2) = g_2, \dots, g \tau^k(p) = g_p$.

Ce, τ^k est d'ordre p dc c'est un cycle qui permute les élts de $\{1, \dots, p\}$ dc $g_1 = g_5 \tau^k(1) = g_5 \tau^{2k}(1) = \dots = g_p$
 $\Rightarrow g_1 = g_2 = \dots = g_p$.

On a donc 2 possibilités:

|| → soit $g_1 = \dots = g_p$ & $|\mathcal{L}_x| = 1$.

|| → soit $|\mathcal{L}_x| = p$.

$$\text{Revenons à } |X| = \sum_{i=1}^n |\mathcal{L}_{x_i}|$$

→ $|X| = |G|^{p-1}$ est un multiple de p.

$$\rightarrow |\mathcal{L}_{(1, \dots, 1)}| = 1$$

$$\text{Modulo } p, 0 \equiv \sum_{\substack{i \\ m_i = (g, \dots, g)}} [Q_{x,i}] \equiv \sum_{\substack{i \\ m_i = (g, \dots, g)}} 1 \cdot [P]^i$$

et $\exists g \neq 1 \text{ tq } |Q_{(g, \dots, g)}| = 1$

comme $(g, \dots, g) \in X$, $g \cdots g = g^p = 1$

L'ordre de g divise p & n'est pas 1,
 g est donc bien un élé d'ordre p .

Retour sur ~~FF~~ de Burnside

$G \rtimes X$, X fini, $\chi(g)$ = nbr pts fixés par g tq $g \cdot x = x$
 chts le nbr d'orbites de $P \rtimes G$ est

$$N = \frac{1}{|G|} \sum_{g \in G} \chi(g)$$

On a des perles de 5 contours éts.

nb de colliers \neq pt-on faire de 5 perles?

X = ens des suites de 5 perles \mathcal{S}

G = rotat du collier $\cong \mathbb{Z}/5\mathbb{Z}$

Deux colliers sont identq si l'on obtient l'un à partir de l'autre par rotation, dc s'ils sont dans la m^e orbite.

N = nbr de colliers

$$N = \frac{1}{|G|} \sum_{g \in G} \chi(g) = \frac{1}{5} (\chi(\text{id}) + \dots + \chi(a_1) \cdot \chi(id))$$

- $\chi(a_i) = 2$ car seuls les colliers monochromes sont stabilisés par une rotation.

- $\chi(id) = 2^5 = 32$ car tous les colliers sont stabilisés par l'identité

$$N = \frac{1}{5} (2 + 2 + 2 + 2 + 32) = 8.$$

\Rightarrow Il y a 8 colliers différents.

Avec 3 couleurs, il faut aussi prendre en compte les réflexions.

$G = D_5$, le groupe des symétries du pentagone,

\rightarrow 1 Id

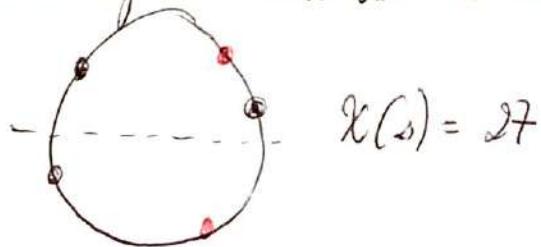
\rightarrow 4 rotations

\rightarrow 5 réflexions.

→ L'identité stabilise tous les colliers $3^5 = 243$

→ Une rotation stabilise uniquement les colliers monocromes
 $\chi(n) = 3$.

→ Une réflexion stabilise les colliers symétriques

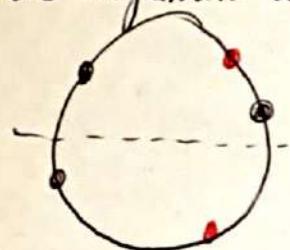


$$\chi(s) = 27$$

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

\rightsquigarrow L'identité stabilise tous les colliers $3^5 = 243$
 \rightarrow Une rotat. stabilise unq les colliers monochromes
 $X(n) = 3.$

\rightarrow Une réflexion stabilise les colliers symétriques



$$X(s) = 27$$

$$N = \frac{1 \times 243 + 4 \times 3 + 5 \times 27}{16} = 10 = \frac{243 + 12 + 135}{16} = 39$$

Groupe Symétrie

$$\text{Ex 23} \quad \sigma_1 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 1 & 4 & 3 & 2 & 7 & 8 & 6 & 5 \end{pmatrix}, \quad \sigma_2 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 5 & 6 & 4 & 7 & 3 & 2 & 1 \end{pmatrix}$$

a) Decompose σ_1 & σ_2 en \prod cycles à signe droit

$$\sigma_1 = (24)(5768), \quad \sigma_2 = (15347)(26)$$

b) et ordre & signature de σ_1 & σ_2 .

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

$$\begin{aligned} \text{ordre } (\sigma_1) &= \text{ppcm}(\text{ordre } (24), \text{ordre } (5768)) \\ &= \text{ppcm}(2, 4) = 4. \end{aligned}$$

$$\begin{aligned} \text{ordre } (\sigma_2) &= \text{ppcm}(\text{ordre } (15347), \text{ordre } (26)) \\ &= \text{ppcm}(5, 2) = 10. \end{aligned}$$

signature (σ) = $\varepsilon(\sigma)$?

$$\varepsilon(\sigma_1) = \varepsilon((24)) \times \varepsilon((5768)) = (-1)^4 \times (-1)^3 = 1$$

$$\varepsilon(\sigma_2) = \varepsilon((15347)) \times \varepsilon((26)) = (-1)^9 \times (-1)^1 = -1$$

c) calculer σ_1^{175} & σ_2^{1999}

$$\sigma_1^{175} = \sigma_1^{175} [4]$$

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

$$= (\sigma_1^4)^{43} \times \sigma_1^3 = (\text{Id})^{43} \times \sigma_1^3 = \sigma_1^3$$

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

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

$$\sigma_1^{175} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 1 & 4 & 3 & 2 & 8 & 7 & 5 & 6 \end{pmatrix}$$

on regarde de
à son

$$\sigma_2^{1999} = ?$$

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

$$\sigma_2^{1999} = (\sigma_2^{10})^{200} \times \sigma_2^{-4} = \sigma_2^{-4} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 7 & 6 & 5 & 3 & 1 & 2 & 4 \end{pmatrix}$$

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 $(1,2), (1,3), \dots, (1,n)$

$$\boxed{m=0} \quad S_2 = \{ \text{id}, (1,2) \} = \langle (1,2) \rangle$$

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

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

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

Raisonnement Par Recurrence

Supposons $m \geq 3$:

$$T = (m-1, n) \cdots (\sigma(m)+1, \sigma(m)+2) (\sigma(m), \sigma(m)+1) \sigma$$

soit $\sigma \in S_{m-1}$ et on prendra $\rho (1,2), \dots, (1,m-1)$ pour $T \in S_m$:

\vdash

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

$$\sigma = T(m)$$

$$\text{et alors } T(m) = (1,m) \circ (1, \sigma(m)) \circ (\sigma(m))$$

$$T(m) = (1,m)(1) = m$$

$$\text{Dc } T \in S_{m-1} = \langle (1,2), \dots, (1,n-1) \rangle$$

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

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

$$\text{Dc } \textcircled{PR} \quad S_m \text{ est engendré par } (1,2), \dots, (1,n)$$

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

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

$$\text{b) } Mq \quad S_n \text{ est engendré par } n-1 \text{ transpositions } (1,2), (2,3), \dots, (n-1,n)$$

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

$$\text{Dc } \textcircled{PR}, \quad T \in \langle (1,2), \dots, (n-1,n) \rangle$$

soit $\sigma \in S_{n-1}$, considérons

$$T(m) = (m-1, n) \cdots (\sigma(m)+1, \sigma(m)+2) (\sigma(m), \sigma(m)+1) \sigma$$

$$\text{alors } T(m) = (m-1, n) \circ \cdots \circ (\sigma(m)+1, \sigma(m)+2) \circ (\sigma(m), \sigma(m)+1) \sigma$$

$$= (m-1, n) \circ \cdots \circ (\sigma(m)+1, \sigma(m)+2) \circ (\sigma(m), \sigma(m)+1).$$

$$\vdash \dots$$

$$\sigma = T(m)$$

$$\sigma = T(m)$$

On peut alors prendre $m-1$ premiers éléments $1, \dots, m-1$

$$\text{de } \textcircled{HDR}, \quad T \in \langle (1,2), \dots, (n-1,n) \rangle$$

Dc \textcircled{PR} , S_n est bien engendré par les

$$\text{transpositions } (1,2), \dots, (n-1,n).$$

$$(p,q) = (1,p) (1,q) (1,p) \quad : \eta = p \circ q \quad (p \circ q) \circ r = (1,p) (1,p+1) (1,r)$$

38

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

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

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

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

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

Ensuite, 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{H} de G . Ds chq $g \in G$, vérifier si H agit bien d'une act^o, déterminer les stabilisat^o, les orbites, & élire $\frac{|G|}{|H|}$ égalité.

a) G agit sur lui-m^{ême} par translation à gauche : $g \cdot x = gx$.

► **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^o de \textcircled{G} de G à lui-même.

• Stabilisat^o

Soit $x \in G$,

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

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

• Orbites:

soit $x \in G$,

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

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

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

• Equal aux classes:

$$\text{hyp: } \frac{|G|}{|H|} \times \text{joli. } |X| = \sum_{i=1}^n |\text{Or}_{x_i}| - \sum_{i=1}^n |\text{Stab}_{x_i}|$$

$$\hookrightarrow |G| = |G| = |G/H|$$

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

Action

neutre
associativité

- $1_G \cdot n = 1_G n 1_G^{-1} = n$

- $g \cdot (h \cdot n) = g \cdot (hn h^{-1}) = ghnh^{-1}g^{-1}$
 $= (gh)n(gh)^{-1}$
 $= (gh) \cdot n.$

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

Stabilité

Soit $x \in G$,

$$\text{Stab}_n = \{g \in G, g \cdot n = n\}$$

$$= \{g \in G, gng^{-1} = n\} =$$

$$\boxed{\text{Stab}_n = \{g \in G, gn = ng\}}$$

$= Z_G(n)$: le centralisateur de n .

Orbites Soit $n \in G$

$$\mathcal{O}_n = \{g \cdot n \mid g \in G\} = \{gng^{-1} \mid g \in G\}$$

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

Égaux aux classes

$$|X| = \sum_{i=1}^n |\mathcal{O}_{n_i}| = \sum_{i=1}^n |G/\text{Stab}_{n_i}|$$

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

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

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

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

Act θ

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

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

- $g \cdot (g \cdot (g^1 H g^{1-1})) = g(g^1(g^1 H g^{1-1})g^{1-1})g^{-1}$
 $= (gg^1)(g^1 H g^{1-1})(gg^1)^{-1}$
 $= (gg^1), (g^1 H g^{1-1}).$

Stabilisateur

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

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

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

$$= N_G(gHg^{-1}) \text{ normale.}$$

④ Normalisatrice $N_G(H) = \{ g \in G, gHg^{-1} = Hg \}$.

Orbites:

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

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

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

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

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:

$$|X| = \sum_{i=1}^n |Q_{x_i}| = \sum_{i=1}^n |G/Stab_{x_i}|$$

$$\text{nb: } |\mathcal{O}_H| \text{ de conjugués de } H = |G/Stab(H)| = [G : N_G(H)]$$

⑤ soit $\varphi: G \rightarrow H$ M.D.G

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

⑥ $\bar{\varphi}$ est bien défini

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

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

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

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.G.

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

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

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

$\bar{\varphi}$ bien injective

$\bar{\varphi} = \varphi \text{ sur } \ker \varphi$

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 .

A/ (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.

$$\text{Q: } G \xrightarrow{\varphi} G', \quad \forall g \in G \quad \text{dans } \exists' \text{ isom}$$
$$q = \varphi \circ p \quad \overline{\varphi}: G/H \rightarrow H \varphi$$

$$G/H \cong H \varphi$$

$$\varphi: G \rightarrow G', \quad \text{(groupes), } \forall K \text{ sous-groupe de } G, \quad \varphi(K) \cong \varphi(K)$$

$$G/H \cong G'/\varphi(H)$$

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

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.

$\Delta 6$
 Hsg
 $\text{H} \subset Z(G)$
 dc
 $2(6) + \text{grd}$
 n

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

$\langle \mathcal{S} \rangle = \{a^{2k}, k \in \mathbb{Z}\}$
 $\langle \mathcal{S} \rangle = \{a^{2n}, n \in \mathbb{N}\}$ $\Rightarrow G \text{ commutatif}$

$$[G:H] \cdot |H| = |G|$$

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

$|G|=2k$
 \mathcal{S} ordre 2
 $G/\langle a^2 \rangle \cong \text{Imp. } \text{ST}^{2,0}$
 $a^2 = e$
 $G/\langle 2(6) \rangle \cong G$
 stabil.

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

$$G/$$

$$\langle a^2 \rangle$$

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

$g \cdot x = x$
 $\forall a \in G \quad \varphi(ab^{-1}) = \varphi(a) \varphi(b)^{-1}$
 $\varphi(a) = \varphi(b)$

$x^2 = x$
 $x^2 = x^m$
 $x^2 = 6x$

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 fs) 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'additif sur A est l'additif sur \mathbb{R} point par point. Comme $(\mathbb{R}, +)$ est associatif et commutatif, c'est aussi le 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 $-f : x \mapsto -f(x)$.

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

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 $1_A : x \mapsto 1$, ant & $1_A(0) = 1_A(1) = 1$

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

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

• \times est distributive sur $+$

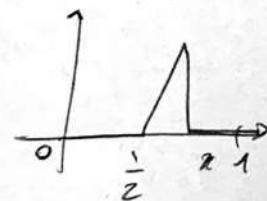
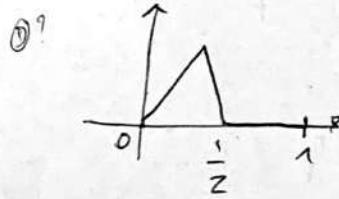
$$\begin{aligned}(f(g+h))(x) &= f(x)(g(x) + h(x)) \\&= f(x)g(x) + f(x)h(x) \\&= (fg + fh)(x).\end{aligned}$$

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

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

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

DC en chq x , une des 2 fs est nulle,
mais pr chacun, \exists point où elle ne
s'annule pas.



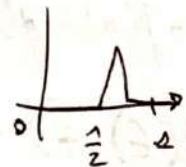
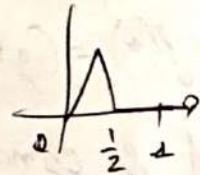
DC A pas intégre.

$$\begin{aligned} \text{• } X \text{ est distributive sur } + \\ (f(g+h))(n) &= f(n)(g(n) + h(n)) = f(n)g(n) + f(n)h(n) \\ &= (fg + fh)(n) \end{aligned}$$

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

②) Construisons $f, g \in A \setminus \{0\}$ tq $fg = 0$,
 $\forall n \in [0, 1], f(n)g(n) = 0$.

De ce chq n , une des 2 fs est nulle,
mais pr chacune, \exists point où elle n'annule
pas.



De A pas intègre.

$$I : \text{idéal de } A \text{ si } \left\{ \begin{array}{l} (I, +) \text{ est } (A, +) \\ \forall a \in A, \forall i \in I, ai \in I \end{array} \right.$$

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

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

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

Donc $f+g \in I$.

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

Donc $f \cdot g \in I$.

⇒ cl I est un idéal de A.

sit $f \in I$, montrons que f n'engendre pas I.

Mg $\sqrt{|f|}$ est do I et pas dans (f)

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

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

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

Sppos qu' $\exists g \in A$ 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 $(G, +)$ \mathbb{G} commutatif.

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

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

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

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

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

En effet,

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

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

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

Mq $(\text{End}(G), +)$ est un \mathbb{G} 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
 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 $f, g, h \in \text{End}(G), x \in G,$

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

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

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

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

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

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

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

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

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

Ex 4 Anneau de Boole

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

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

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

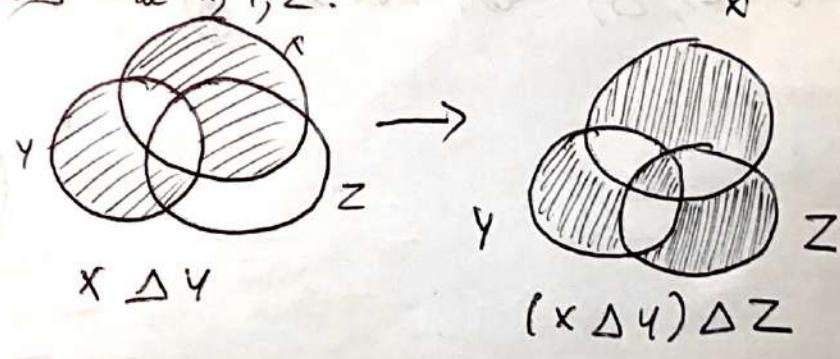
→ gabarit & addi
→ (⊗) distri, associ, e neutre
→ ici commutativity.

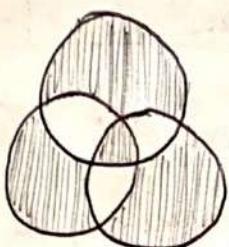
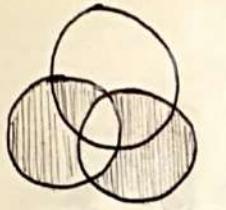
(i) Mq $(\mathcal{P}(E), \Delta)$ est \oplus abélien.

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

Cela démontre que le diag de Venn est aussi accepté.

Pour mq l'associativité, on va utiliser un diag de Venn. Cela 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.

\rightarrow 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 opposé:

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

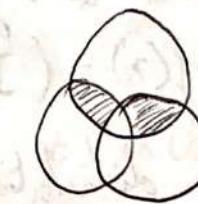
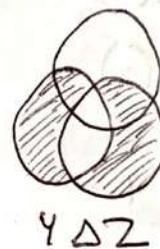
2) $(P(E), \cap)$ est un monoïde (i.e associative + neutre)
Commutatif

(trivial mg \cap est associative & commutative).

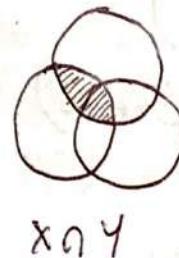
E est le neutre : soit $X \in P(E)$, $X \cap E = X$

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

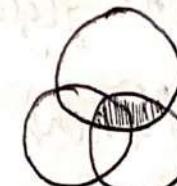
3) \cap est distributive sur Δ



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



&



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

ccp

$(P(E), \Delta, \cap)$ 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 $|E|=1$:

$P(E) = \{\emptyset, E\} \simeq \frac{\mathbb{Z}}{2\mathbb{Z}}$ \hookrightarrow 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 $P(x) \subset I$.

• $x, y \in I$,

• $x \Delta y \in I$

• $x \cap y \in I$.

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

c) Mg si E est fini alors les idéaux de $P(E)$ sont exactement les $P(F)$ tels que $F \subseteq E$.

analyse / synthèse

soit I un idéal de $P(E)$,

soit $F \subseteq E$ de cardinal maximal.

D'après a), $P(F) \subset I$.

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 : de $A \cap X \in P(F)$.

• 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 $P(E)$.

A/5:
 A/1 si supp dgt J.
 A/2: mg qd pfin dgt J.

49

• Rés: mg qd pfin dgt J.

• Rés: mg qd pfin dgt J.

<u>Idéal</u>
• stable par \oplus
• $P \oplus$
• (I, \cap) qd de $(A, +)$.

d) Supposons $E \neq \emptyset$. Si $I = \{ \text{pièces finies de } E \}$ est un idéal de $\mathcal{P}(E)$ qui n'est pas de la forme $\mathcal{P}(F) \neq F \subset E$.

Mais 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 que $I = \mathcal{P}(F) \neq F \subset E$.

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

• Donc $E \subset F$, 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 $\mathcal{P}(F)$ de $F \subset E$.

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) Mais aucun inverse de A n'est nulpotent.
 Soit $a \in A$ inversible, a n'est pas un diviseur de zéro, de sorte qu'il ne peut pas être nulpotent.

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

b) Mais 1 est l'unique élément idempotent inv. de A .
 Soit $a \in A$ idempotent & inversible

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

$$1 \cdot 1 = 1^2 = 1 \quad \text{Donc } 1 \text{ est inversible}$$

& 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 $a = 1$.

Cp : 0 & 1 st les seuls idempotents.

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

$$ax^2 + bx + c$$

$$\begin{array}{ccc} \Delta & & \left\{ \begin{array}{l} a, c \\ b, c \\ a, b \end{array} \right. \\ x_1 & x_2 & \\ ab = 0 & ab = 0 & ab = 0 \\ \Leftrightarrow x_1 = 0 & \text{ou} & \text{ou} \end{array} \quad \text{51}$$

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 ?

Demarche: Essayer de montrer le résultat
si si c'est bon et si l'une des hypothèses n'est pas vérifiée alors l'assertion sera 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 sg de $(B, +)$.

• soit $b \in B$, $f(a) \in f(I)$,

b. $f(a) = b = f(u)$? non possib.

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

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

• $f(\mathbb{R}) = \mathbb{R}$ et \mathbb{R} n'est pas un idéal de \mathbb{C}
(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 $f(a-a') = \underbrace{f(a)}_{\in J} - \underbrace{f(a')}_{\in J} \in J$

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

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

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

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

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

Ex 9: Existe-t-il un MDA de \mathbb{R} vers \mathbb{Q} . et $M_{a,b,c} - M_{d,e,f} \in A$.

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

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

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

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

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

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

Ex 10 soit $A = \{M_{a,b,c} \mid a, b, c \in \mathbb{C}\}$.

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

a) $M_I A$ est \textcircled{a} -commutatif de $M_3(\mathbb{C})$.

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

b) $M_I (A, +)$ \textcircled{a} -abélien de $M_3(\mathbb{C})$

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

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

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

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

$$(53) = M_{a-d, b-e, c-f}$$

Donc $(A, +) \rightleftharpoons (M_3(\mathbb{C}), +)$ (avec on est à \mathbb{Q})
 abélien et multiplicable

$\Rightarrow M_I$ neutre $\in A$

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

$\Rightarrow M_I A$ est stable par multiplication.

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

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

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

Done A est bien stable par multiplication.

De plus, cette \textcircled{a} permet de vérifier que

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

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

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

intuit: considérez que $M_{a,b,c} \in A \rightarrow a+b+c \in \mathbb{C}$.

$$\text{Idéal} = \left\{ \begin{array}{l} (I, +) \text{ sg } (A, +) \\ a_n \in I, \forall a \in A, \forall n \in I \end{array} \right.$$

► Mg $(I, +)$ sg de $(A, +)$ mv
stab p stabs

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

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

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 sg de $(A, +)$.

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

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

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

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

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

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

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

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

\Rightarrow 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

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

on écrit

Idéal maximal si A/I corps

Mg I maximal:

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

$$\text{On a déjà mg } \Psi(n-y) = \Psi(n) - \Psi(y)$$

$$\Psi(ny) = \Psi(n) \Psi(y).$$

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

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

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

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

On peut appliquer le théorème d'isomorphisme, i

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

car $z \in \mathbb{C}$ vérifie $z = \varphi(z \cdot I_3)$ ~~par conséquent~~

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

Anneaux d'entiers & Entiers de Gauss

Ex 21 (Anneau d'entiers)

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

soit 1'ens $\mathbb{Z}[w]$ & 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) Mq $\mathbb{Z}[w]$ est ~~sa~~ de \mathbb{C} .

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

$$\rightarrow \frac{\mathbb{Z}[w] \triangleleft \mathbb{C}}{\circ = 0 + 0w \in \mathbb{Z}[w]}$$

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

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

• Stable par \times

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

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

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

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

b) Mq $(1, w)$ 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'existence d'une telle décomposition provient de la définition de $\mathbb{Z}[w]$.

Sups $a + bw = c + dw$ alors $a - c = w(d - b)$

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

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

La décomp est de uniq.

c) $M_q \quad \Psi: \mathbb{Z}[\omega] \rightarrow \mathbb{Z}[\omega]$

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

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

M_q est MDA :

$$\begin{aligned} \circ \Psi(a + \omega b + c + \omega d) &= \Psi((a+c) + \omega(b+d)) \\ &= (a+c) - \omega(b+d) = a - \omega b + c - \omega d = \Psi(a + \omega b) + \Psi(c + \omega d). \end{aligned}$$

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

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

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

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

$$\bullet \Psi(1) = \Psi(1 + 0\omega) = 1 - 0\omega = 1.$$

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

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

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

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

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

e) $M_q \quad x \in \mathbb{Z}[\omega]$ 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.

10in op 22
 57

Ex 25: Entiers de Gauss
 L'anneau des entiers de Gauss est le sa
 $\mathbb{Z}[i] = \{a+ib, a, b \in \mathbb{Z}\}$ 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 $N(z) = a^2 + b^2 = 1$.

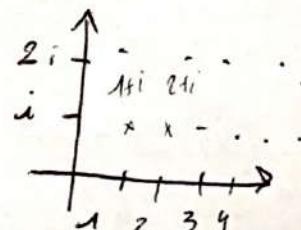
On a 4 possibilités: $(a, b) \in \{(\pm 1, 0), (0, \pm 1)\}$
 Les inversibles de $\mathbb{Z}[i]$ st dc $\{\pm 1, \pm i\}$.

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

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' indicatrice de l'ordre
 $\phi(p) = p-1$

(P30) 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 $\mathcal{G}_d \simeq \mathbb{Z}/d\mathbb{Z}$

alors \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

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

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

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

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

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 $m \times n$

Les entiers x ds $[1, p^x]$ premiers à p^x
sont les entiers entre 1 & p^x sauf
 p^{x-1} 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 qui a pour 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 $x \in \mathbb{N}, \dots ;$, $\text{pgcd}(n, p^x) = 1$

$$\Downarrow \\ p \nmid n$$

$$\begin{aligned} @ \Phi(12) &= \Phi(2^2 3) = \Phi(2^2) \Phi(3) \\ &= (2^2 - 2)(3 - 3^0) \\ &= 4. \end{aligned}$$

S3 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
($\mathbb{R}[x], \mathbb{C}[x], \mathbb{Z}/p\mathbb{Z}[x], (K[x], +, \cdot)$) et @ com @.

$\boxed{X^N}$ $\in \mathbb{Z}/p\mathbb{Z}[x]$ pas intz E.S = 0
coeff dominant $\neq 0$,

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

⑧6 $K \text{ corps} \Rightarrow$ 1) $\mathbb{K}[x]$ intègre
2) L'ens $(\mathbb{K}[x])^X$ sels inv = \mathbb{K}^*

van ⑧5, ⑧6

$$\textcircled{D} 7 \quad P = \sum_{n=0}^m a_n x^n, \quad Q = \sum_{n=0}^m b_n x^n, \quad \neq 0$$

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

$\deg(PQ) = \deg(P) + \deg(Q) = m+m$ & 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 $(\mathbb{K}[x])^X = \mathbb{K}^X$ pc \mathbb{K} @ intègre:

(c) évident

(c) soit $P \in (\mathbb{K}[x])^X$ ie $\exists Q \in \mathbb{K}[x]$ tq

⑧7 $P_x Q = 1$. Alors $\deg P + \deg Q = 0$

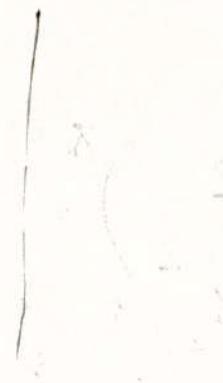
de $\deg P = \deg Q = 0$

ie $P, Q \in \mathbb{K}$ et ⑧7 dit que $P \in \mathbb{K}^X$.

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

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

⑧9 (2^e monômes).



2. Division Euclidienne

⑧10 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.

21 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^e cas: si $m < d$, on a :

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

2^e cas: si $m \geq d$

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

D NDR, $\exists Q_1, R_1 \in K[X]$ tq

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

de $\deg R_1 < \deg P$.

Cela donne:

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

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

(63)

(30) Spp $F = PQ_1 + R_1 = PQ_2 + R_2$
et $\deg R_1 < \deg P$, $\deg R_2 < \deg P$.

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 $R_1 = R_2$

□

(Ca) si K est un corps, $K[X]$ est un @ euclidien & dc principal.

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

3. Racines d'un polynôme

Si $a \in K$, K est un corps.

(D) Racine d'un polynôme

$P(x) = \underbrace{(x-a)}_{\text{diviseur}} Q + R \underset{x=a}{=} P(a)$

remplacer $x=a$

⑩ Multiplicité.

⑨ P ∈ K[X], K corps, app. a_1, \dots, a_m racines de P
de multiplicité respectives m_1, \dots, m_n
alors P est divisible par
 $(X-a_1)^{m_1} \cdot (X-a_2)^{m_2} \cdots (X-a_n)^{m_n}$

⑩ Si P ∈ K[X] est un polynôme non-nul alors le nbr de racines distinctes de P ds K est $\leq \deg P$.

⑪ Si a_1, \dots, a_m st les racines distinctes de P & m_1, \dots, m_n leurs multiplicités, ∃ Q ∈ K[X] tq $P = Q \times (X-a_1)^{m_1} \cdots (X-a_n)^{m_n}$

On obtient $\deg P \geq \deg Q + m_1 + \dots + m_n > 0 + \underbrace{1+ \dots + 1}_n$

⑪ P92, 93

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

voir 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.

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

⑫ P ∈ K[X] v. dit irréductible a.

∀ 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 $\deg G = 0$.

⑬ • $\deg P = 1 \Rightarrow P$ 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 $\mathbb{Q}[x]$ 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 $\mathbb{R} (\Leftrightarrow x^2+1)$.

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

• les polynômes de deg 1 st irréduct (trivs)

• soit $P \in \mathbb{C}[x]$ irréductible. D'après le

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

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

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

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

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

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

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

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

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

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

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

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

On a bien DG et N pr statme $\mathbb{Z}[i]$ est euclidien, cf PL.

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

+ résultat 21g) ; on calcule la norme de $3i$: $N(3) = 3^2$
les diviseurs de $N(3) \neq$ de ± 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 é ds 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 $N(3) = 9$ ds l'image de N st ± 1 & ± 3
en appliquant le résultat de 21g, on et que 3 est irréductible ds l'anneau $\mathbb{Z}[i]$.

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

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

Les résultats de 21.g. mg z est irréductible.

La réciproq est fausse & 8 me donne un ca MS il est irréductible ds $\mathbb{Z}[i]$ mais $N(3) = 9$ n'est pas 1.

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

$$(2+i)(2-i) = 2^2 - i^2 = 4+1 = 5 \quad \text{et} \quad (1+2i)(1-2i) = 1^2 - (2i)^2 = 1+4=5$$

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

⑤8 De ces 2 décompos st équivalentes, ce résultat ne contredit pas l'3e de la décomp on est irréductible.

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

$N(2) = 2^2 - 4$, l'un diviseur de 2 ≠ de ± 2 & ± 1 doit être de norme 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 irréductibles.

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 & $\bar{a}^{-1} = \bar{u}$.

§ Annexe $\mathbb{Z}/m\mathbb{Z}$

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

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

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

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

$$\Rightarrow 3 = 28 - 5 \times 5 = 28 - 5 \times (1 \times 705 - 25 \times 28) \\ = 126 \times 28 - 5 \times 705$$

• DÉ 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 $\bar{28}^{-1} = \bar{277}$ de $\mathbb{Z}/705\mathbb{Z}$.

Ex 18 Résoudre de \mathbb{Z} les systèmes suivants.
(E1) $\begin{cases} 3x \equiv 2 \quad [41] \\ 3x \equiv 4 \quad [47] \end{cases}$ (E2) $\begin{cases} x \equiv -3 \quad [99] \\ x \equiv 2 \quad [140] \end{cases}$ (E3) $\begin{cases} x \equiv 3 \quad [4] \\ x \equiv -2 \quad [3] \\ x \equiv 7 \quad [5] \end{cases}$

(E1) 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 $\mathbb{Z}/mn\mathbb{Z}$.

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

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

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

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

Donc $3^{-1} = \overline{26}$ 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.

$$1 = 29 \times 140 - 41 \times 99 \Leftarrow 140, 99 \text{ paa.}$$

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

Donc $-3 \times 29 \times 140 - 2 \times 41 \times 99 \equiv \begin{cases} -3 \pmod{99} \\ 2 \pmod{140} \end{cases}$
 $-20 \cdot 298$

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

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

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

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 :

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

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

$$3 \text{ et } 5 \times 3 = 15: \quad 1 = 3 \times 3 - 1 \times 15$$

$$5 \text{ et } 3 \times 5 = 15: \quad 1 = 5 \times 5 - 2 \times 12$$

$$\text{Donc } \begin{cases} 1 \equiv -1 \times 15 \pmod{4} \\ 1 \equiv -1 \times 80 \pmod{3} \\ 1 \equiv -2 \times 18 \pmod{5} \end{cases}$$

$$\text{Donc } -3 \times 15 + 2 \times 20 - 7 \times 84 = \begin{cases} 3 \\ -2 \\ 7 \end{cases} \quad \text{soit } \varphi: (\mathbb{Z}/p\mathbb{Z})^* \rightarrow (\mathbb{Z}/p\mathbb{Z})^* \\ y \mapsto y^2.$$

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

$$\Rightarrow \boxed{x \equiv 7 \pmod{60}} \quad \begin{array}{l} \text{en 3, 4, 5} \\ \text{par } 2 \tilde{=} 2 \end{array}$$

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

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

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

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

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{g} 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 à l' \textcircled{a} intégrée

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

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

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

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

$$\iff p-1 \text{ est multiple de } 2$$

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

- a) Mg P est irréductible
b) Mg $\mathbb{K}[x]/(P)$ est un corps à g stb.

Sppos par ?1 $P(x)$ est réductible
 $\Rightarrow P(x) = A(x)B(x)$ & $0 < \deg A < 2$
donc $\deg A = 1$ ie $A(x) = X - \lambda$,

& $\lambda \in \mathbb{Z}/3\mathbb{Z}$. Donc λ est une racine de ?1

Contradict: car P n'a pas de racine:

x	$x^2 + 1$
0	1
1	2
2	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 $|K[X]/(P)| = |\mathbb{Z}/3\mathbb{Z}|^2 = 9$.

Deancie Révisions M^{de}_R : 22/12

14^h45. → Zoom.

DS 2021

