23

Structures algébriques : Groupes.

1.1.5 :

$$\cancel{a} * x = \cancel{a} * y \qquad \cancel{0}.x = \cancel{0}.y$$

1.1.6 elt symétrisable "ou inversible"

x^{-1} sym de x pour la loi $\square$ (autre not $-x$ sym de x pour la loi $\square$)

1.2.1

Def : $(G, *)$ groupe ssi $*$ lci

(G1) $*$ associative.

(G2) neutre. (e) (ou 1 si $\times$, 0 si $+$)

(G3) symétrique :

$(\forall x \in G)(\exists y \in G)\ x * y = y * x = e$

[(G4) ? commutatif ou abélien)

Tout élément est symplifiable.

$$a * x = a * y$$

a^{-1} $\qquad$ a^{-1}

$$\underbrace{a * \cancel{a^{-1}}}_{e} * x = \underbrace{a * \cancel{a^{-1}}}_{e} * y$$

1.2.23 groupe produit.

(G,T) $\quad G\times H=\{(g,h)\ /\ g\in G,\ h\in H\}$

$(H,\perp)$

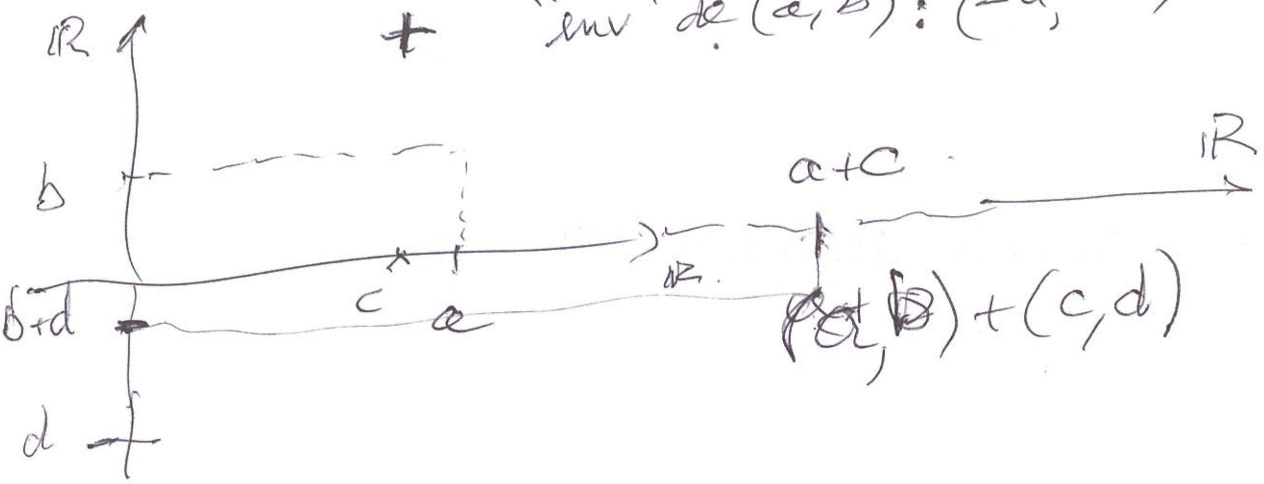
$(g_1,h_1) * (g_2,h_2) = (g_1 T g_2, h_1 \perp h_2)$

neutre : (e_G, e_H)

symétrique de (g,h) : $(g^{-1(T)}, h^{-1(\perp)})$

ex : $(\mathbb{R}^2,+)$ $\quad (a,b) \underset{+}{*} (c,d) = (a+c, b+d)$

"inv" de (a,b) : $(-a,-b)$



1.2.2 H ss gpe de G $\quad (G,*)$

H1 • $H\neq\emptyset$ (facile).

H2 • $\forall(x,y)\in H$ $\quad x*y\in H$ stabilité par $*$

H3 • $\forall x\in H$ $\quad x^{-1}\in H$ stabilité par inv

NB : $e\in H$ (dans la pratique on vérifie $e\in H$ DONC $H\neq\emptyset$)

explication : $H\neq\emptyset$ soit $x\in H$.

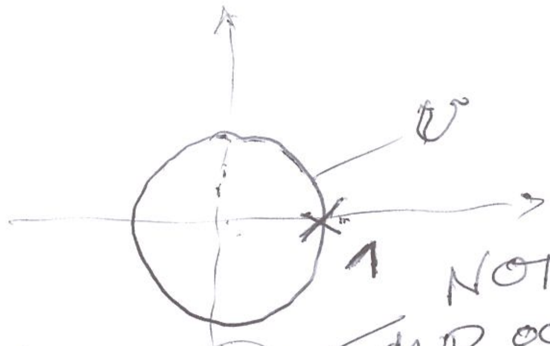
d'après H_3 : $x^{-1}\in H$ d'après H_2 $\underbrace{x*x^{-1}}_{e}\in H$

Caractérisation stable par inv et prod

1.2.29

ex $\mathbb{U} = \{z \in \mathbb{C} \,/\, |z| = 1\}$

$(\mathbb{U}, \times)$ sous groupe de $(\mathbb{C}^*, \times)$

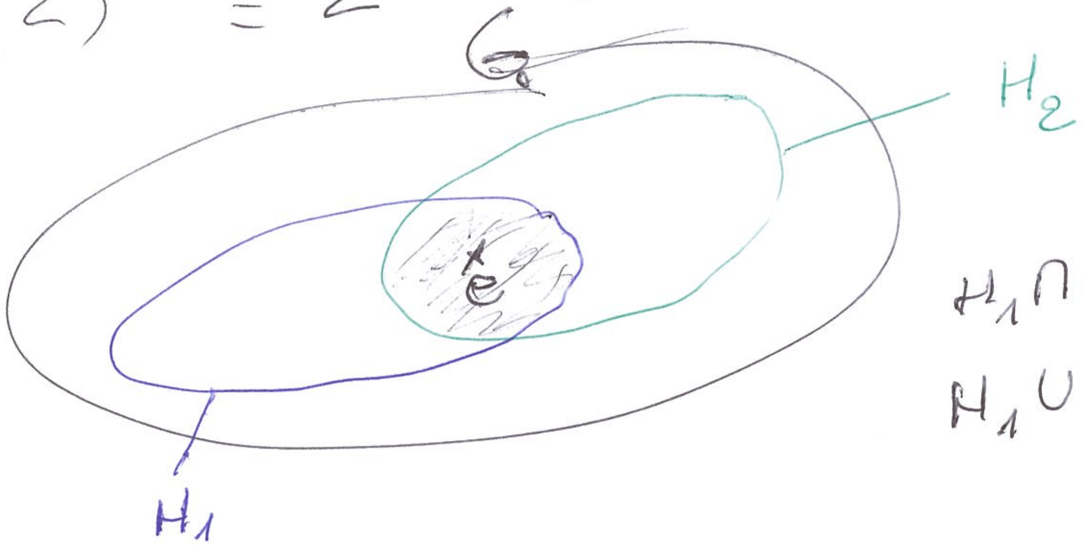


z, z' dans $\mathbb{U}$ ~~$z * z'$~~ $z \times \frac{1}{z'} \in$? NOT ds $\mathbb{R}$ ou $\mathbb{C}$

$$\left|z \times \frac{1}{z'}\right| = |z| \times \frac{1}{|z'|} = 1 \times \frac{1}{1} = 1$$

$z \in \mathbb{U}$ a un inverse : $\frac{1}{z} = \frac{\bar{z}}{z\bar{z}} = \frac{\bar{z}}{|z|^2} = \bar{z}$

"$(z)^{-1}$" $= \bar{z}$ $\quad z.\bar{z} = 1$.



$H_1 \cap H_2$?

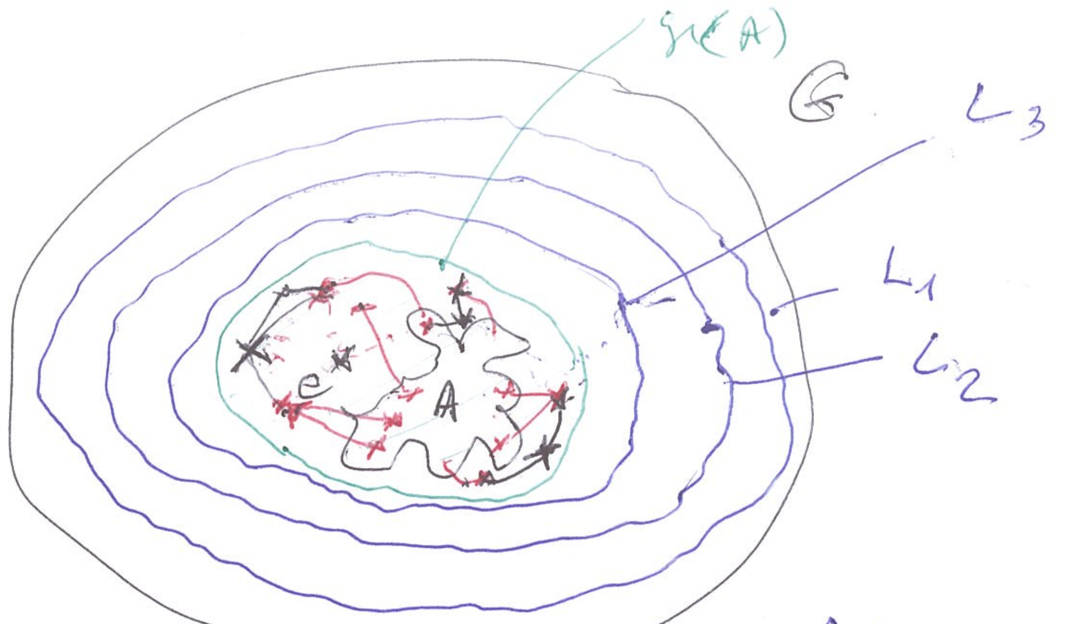
$H_1 \cup H_2$?

Th. 1.2.30 : $(H_i)_{i \in I}$ famille de sous groupe

$H = \bigcap_{i \in I} H_i$ but mq H ss gpe de G.

- $e \in H_i \ \forall i \in I$: $e \in H$ $\quad (H \neq \emptyset)$
- x, y ds H $\underline{\forall i \in I}$ $x, y \in H_i$ donc $x * y \in H_i$ $\quad x * y \in H$.
- $x \in H$ $\quad x^{-1} \in H_i \ \forall i \in I$ $\quad x^{-1} \in H$.

1.2.32
33



Par l'exterieur

$$gr(A) = (A) = \bigcap_{L \in \mathcal{E}} L \qquad \mathcal{E} = \{ L \text{ ss gpe de } G \,/\, A \subset L \}$$

non vide $G \in \mathcal{E}$.

↳ c'est un sous groupe de G

c'est le plus petit ! (pour $\subset$)

Par l'interieur : Prop 1.2.34.

$$H = \left\{ a_1^{\varepsilon_1} a_2^{\varepsilon_2} \cdots a_n^{\varepsilon_n} \,/\, \begin{matrix} n \in \mathbb{N} \\ a_i \in A \end{matrix} \right\} \quad \varepsilon_i \in \{+1, -1\}$$

déjà : $A \subset H$ ($n = 1$ $\varepsilon_1 = 1$)

Montrons que H le + petit sous groupe contenant A
si L ss gpe contenant A, forcement $a_1^{\varepsilon_1} a_2^{\varepsilon_2}$ avec
$a_i \in A$ sont dans L donc $H \subset L$ ("L + grand")

Groupe monogène $g \in G$.

$$(g) = \{ g^p \,/\, p \in \mathbb{Z} \}$$

$g, g^{-1}, g \circ g = g^2, g^3, \ldots$

↳ $g^{-1} \times g^{-1} = g^{-2} = (g^{-1})^2$

↳ $g^{-3}, \ldots$

1.2.4 Les sous groupes de $(\mathbb{Z}, +)$

H sous gpe. $\exists n \in \mathbb{N}$ $H = n\mathbb{Z}$

dem: Division euclidienne.

$H^+ = H \cap \mathbb{Z}_+^* = \{ h \in H \,/\, h > 0 \}$

1er cas $H^+ = \emptyset$ $H = \{0\} = 0\mathbb{Z}$

2ème cas: on note $n = \min H^+$ (non vide, minorée)

donc $n > 0$. Deja $n \in H$.

donc $(\forall k \in \mathbb{Z})$ $n.k \in H$. $n\mathbb{Z} \subset H$

$k > 0$ $\underbrace{n + n \cdots + n}_{k\text{ fois}} \in H$

$k < 0$ $-n - n \cdots - n \in H$.

soit $a \in H$ (Quitte à changer le signe on suppose $a > 0$)

$\begin{cases} a = nq + r \\ 0 \leq r < n \end{cases}$ $r = \underset{\in H}{a} - \underset{\in H}{nq} \in H$

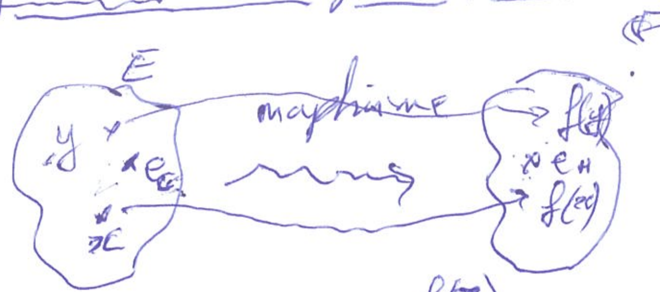
$\begin{cases} 0 \leq r < n = \min H^+ \\ r \in H \end{cases}$

Donc $r = 0$ $a = nq \in n\mathbb{Z}$

donc $H \subset n\mathbb{Z}$ donc $H = n\mathbb{Z}$

Chapitre 23 (suite)

1.3 Morphisme de groupes :



$$\overbrace{x * y}^{z} \qquad \overbrace{f(x) \top f(y)}^{f(z)}$$

$$f(x*y) = f(x) \top f(y)$$

$G \neq \emptyset \quad x \in G \qquad x * e_G = x$

f morphisme de G sur H :

$$\cancel{f(x)} \top f(e_G) = \cancel{f(x)}$$

$$\boxed{f(e_G) = e_H}$$

inv ds H

$y = x^{-1} \in G \qquad x * y = e_G$

$$f(x) \top f(y) = e_H$$

donc $f(y) = f(x)^{-1}$.

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

exemple :

$f(x) = e^x \qquad G = (\mathbb{R}, +) \qquad e^{a+b} = e^a e^b$

$$f(a+b) = f(a) \times f(b)$$

$(\mathbb{R}, +) \xrightarrow{f} (\mathbb{R}_+^*, \times) \longrightarrow$ sous groupe de $(\mathbb{R}^*, \times)$

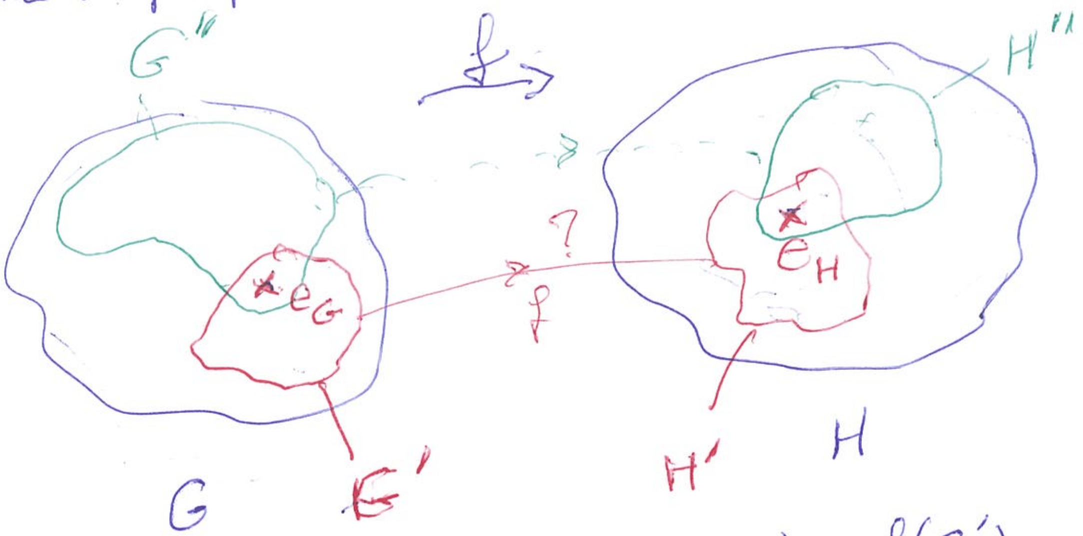
f morphisme du groupe $(\mathbb{R}, +)$ vers le groupe $(\mathbb{R}_+^*, \times)$

ex : $(\mathbb{R}, +)$ groupe $\quad \mathbb{U} = \{z \in \mathbb{C} \;/\; |z| = 1\}$ $(\mathbb{U}, \times)$ groupe.

$$f : \mathbb{R} \to \mathbb{U}, \quad t \mapsto e^{it} \qquad f(t+s) = e^{i(t+s)} = e^{it} e^{is} = f(t) \times f(s)$$

f morphisme de groupe $(\mathbb{R}, +)$ vers $(\mathbb{U}, \times)$

1.3.44



dem : . G' groupe $\quad K = f(G')$ $\quad$ deja $e_H = f(e_G) \in f(G')$

Th car : y_1, y_2 dans K $\quad x_1, x_2$ tq $y_i = f(x_i)$

$$y_1 \top y_2^{-1} = f(x_1) \top f(x_2)^{-1} = f(x_1) \top f(x_2^{-1}) = f(\underbrace{x_1 * x_2^{-1}}_{\in G'}) \in f(G')$$

. idem pour $f^{-1}(H'')$ (à faire)

def : 2 cas particuliers : $G' = G$ .. (ss gpe de G)

: $H' = \{e_H\}$ (——— H)

ex : $\operatorname{sgn} : (\mathbb{R}^*, \times) \longrightarrow (\{-1, +1\}, \times)$ morphisme de groupe.

$x \longmapsto \operatorname{sgn}(x)$

$\operatorname{sgn}(a \times b) = \operatorname{sgn}(a) \times \operatorname{sgn} b.$ $\quad (\{-1, +1\}, \times$ groupe$)$

$+ \longleftarrow + \; +$
$- \longleftarrow + \; -$
$- \longleftarrow - \; +$
$+ \longleftarrow - \; -$

$\times$	1	-1
1	1	-1
-1	-1	1

ex (suite) $f : (\mathbb{R}, +) \longrightarrow (\mathbb{U}, \times)$

$t \longmapsto e^{it}$

$\mathrm{Im} f = \mathbb{U}$ sous groupe de $\mathbb{U}$.

$\mathrm{Ker} f = f^{-1}(1) = \{ t \in \mathbb{R} / e^{it} = 1 \}$

$= \{ 2k\pi \ / \ k \in \mathbb{Z} \}$

$= 2\pi\mathbb{Z}$ (notation)

$(2\pi\mathbb{Z}, +)$ sous groupe de $(\mathbb{R}, +)$

exercice : Soit $(G, *)$ groupe et $f : G \to G$

définie par $f(x) = x^2$ $(= x * x)$

Montrer que si $(G,*)$ commutatif, alors f morphisme de groupe.

- Réciproque : si f morphisme de groupe, $(G,*)$ commutatif

- $f(e) = e^2 = e$ $\quad x, y$ dans G $\quad f(x*y) = (x*y)^2$

$f(x) * f(y) = x^2 * y^2$

$f(x*y) = (x*y)^2 = (x*y) * (x*y)$

commutat $\Rightarrow$ $= x^2 * y^2 = f(x) * f(y)$

[$\mathrm{Ker} f = \{ y / \exists x \in G \ y = x^2 \}$ sous groupe de G]

- si f morphisme $\quad f(x*y) = f(x) * f(y)$

$\cancel{x} * y * x * \cancel{y} = x^{\cancel{2}} * y^{\cancel{2}}$

$\forall x \in G \ \forall y \in G \quad y * x = x * y$

G commutatif.

Th 1.3.47.

2. ok.

1. $\Rightarrow$ si f inj l'unique antécédent de e_H est e_G.

$$\ker f = \{e_G\}.$$

$\Leftarrow$ on suppose $\ker f = \{e_G\}$

$\boxed{\text{STOP}}$

x, y dans G tels que $f(x) = f(y)$

$$f(x) \times f(y)^{-1} = e_H$$

$$f(x \times y^{-1}) = e_H \quad \text{donc } xy^{-1} = e_G \quad x = y.$$

Jamais on dem l'inj en commençant par

$f(x) = f(y) \ldots$

On CALCULE TOUJOURS $\underline{\ker f}$

$$\boxed{f(x) = e_H \Rightarrow x = e_G}$$

Types de morphismes de groupes :

morphisme : $\rightarrow$ vocabulaire.

<u>endo</u> morphisme : $G \to G$

iso ———— $G \to H$ bij.

auto = endo + iso $G \longrightarrow G$ bij.

ex. ln isomorphisme $(\mathbb{R}_+^*, \times) \to (\mathbb{R}, +)$.

$\ln^{-1} = \exp : (\mathbb{R}, +) \longrightarrow (\mathbb{R}_+^*, \times)$.

1,4 Groupe monogène, groupe cyclique,

$(\mathbb{Z}/n\mathbb{Z}, +) \leftarrow$ groupe.

1.4.1 relation d'equivalence.

$x \mathcal{R} y$.

E ens R relation d'equi. $x, y \in E$ soit $x \not\mathcal{R} y$.

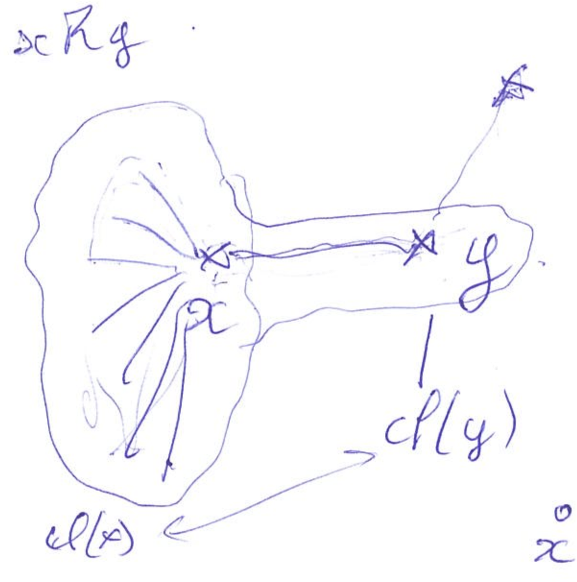
- reflexive
- symétrique
- transitive.

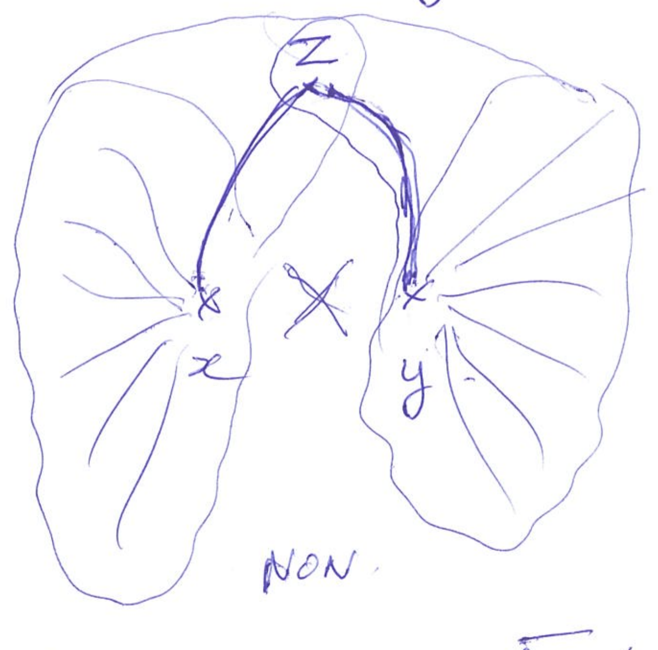
on def pour $x \in E$ $\quad \mathring{x} = cl(x) = \bar{x} = \{y \in E / x \mathcal{R} y\}$

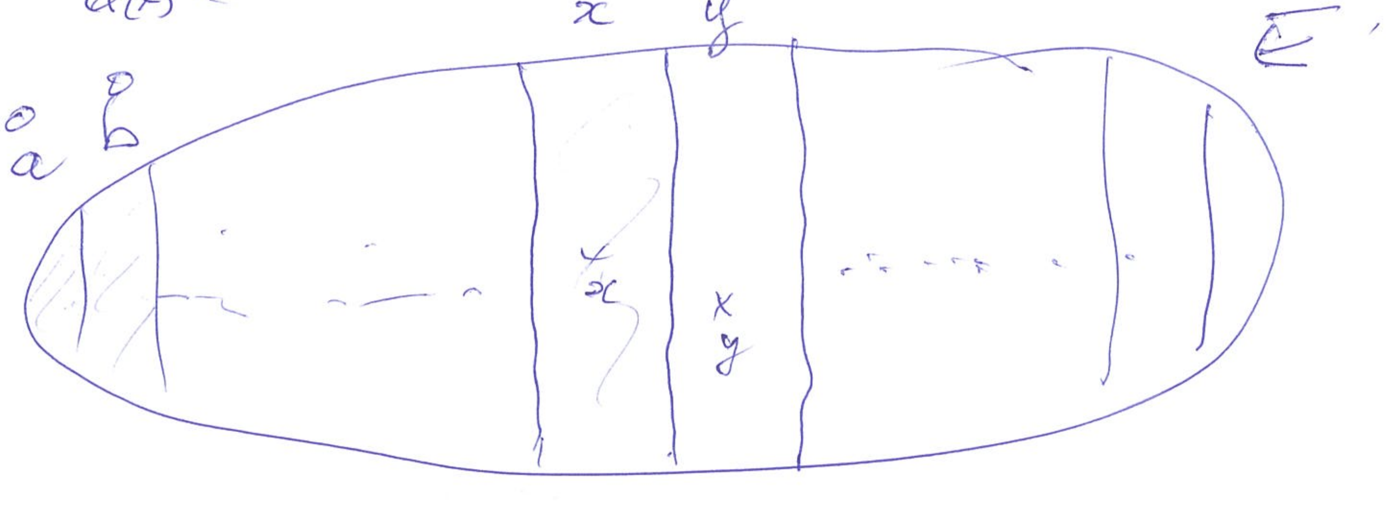
dans ce cas x représentant de $cl(x)$.

2 cas possibles. soit $x \mathcal{R} y$ alors $\mathring{x} = \mathring{y}$

sinon $x \not\mathcal{R} y$ alors $\mathring{x} \cap \mathring{y} = \emptyset$







Prop L'ens des classes d'équi est une partition de E

1.4.2 Congruences. $\mathbb{Z}$ $n \in \mathbb{N}^*$ fixé

Def : a "$\mathcal{R}$" b $\quad \mathcal{R}$ = congruence modulo n

ssi n divise $b-a$.

ie $\exists k \in \mathbb{Z}$ tq $b-a = kn$.

ie ——— $b = a + \underbrace{kn}_{\text{multiple de } n}$

Not : $a \equiv b\,[n]$, ou $a = b \mod n$

c'est une rel d'équivalence.

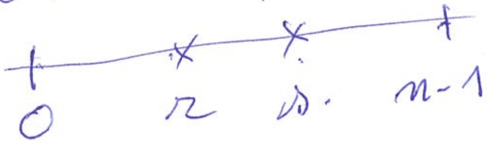
On s'intéresse aux classes d'équ ds $\mathbb{Z}$.

$a \in \mathbb{Z}$ on peut écrire (div euclidienne)

$a = qn + r$ avec $0 \leq r < n$

$a \,\mathcal{R}\, r$ donc $cl(a) = cl(r)$ $\quad \mathring{a} = \mathring{r}$

de + si r, s dans $[\![0, n-1]\!]$ $\quad |r-s| \leq n-1 < n$



donc n ne divise pas $r-s$ si $r \neq s$

Toutes les classes sont distinctes.

Def : On appelle $\mathbb{Z}/n\mathbb{Z}$ l'ens des classes d'équi.

$$\mathbb{Z}/n\mathbb{Z} = \{\underset{\overset{\|}{\underset{\|}{\mathring{n}}}\atop \mathring{2n}}{\mathring{0}}, \underset{\overset{\|}{\mathring{n+1}}}{\mathring{1}}, \dots, \mathring{n-1}\} \qquad \text{Card} = n$$

1.4.3 Le groupe $(\mathbb{Z}/n\mathbb{Z}, \dot{+})$

L'addition + de $\mathbb{Z}$ est compatible avec R "$\equiv$ mod n"

$\left.\begin{array}{l} a \equiv b\,[n] \\ c \equiv d\,[n] \end{array}\right\}$ alors $a+c \equiv b+d\,[n]$

$\left.\begin{array}{l} a = b+kn \\ c = d+ln \end{array}\right\}$ $\quad a+c = b+d+(k+l)n$

$\qquad a+c \equiv b+d\,[n]$.

On peut def une + sur $\mathbb{Z}/n\mathbb{Z}$ "$\dot{+}$"

C, D 2 classes de $\mathbb{Z}/n\mathbb{Z}$. $\quad C = \mathring{c} = \mathring{a}$

on def $C+D$ par ? $\quad D = \mathring{d} = \mathring{b}$

on pose $C \dot{+} D = \overset{\circ}{\overline{c+d}} = \overset{\circ}{\overline{a+b}}$

↳ indep du representant.

Th : L'ens $(\mathbb{Z}/n\mathbb{Z}, \dot{+})$ muni de cet addition est un groupe commutatif.

- neutre : $\mathring{0}$ $\quad \mathring{a} \dot{+} \mathring{0} = \overset{\circ}{\overline{a+0}} = \mathring{a}$
- "inverse" opposé $\quad \mathring{a} \dot{+} \overset{\circ}{\overline{(-a)}} = \overset{\circ}{\overline{a-a}} = \mathring{0}$

Par ex opposé $(\dot{1}) = \overset{\circ}{\overline{-1}} = \overset{\circ}{\overline{n-1}}$

ex ~~...~~ Table d'+ dans $\mathbb{Z}/6\mathbb{Z}$

$\overline{5} + \overline{3} = \overline{2}$

$gr(\overline{0}) = \{\overline{0}\}$.

(*) $gr(\overline{1}) = \{\overline{0}, \overline{1}, \dots \overline{5}\} = \mathbb{Z}/6\mathbb{Z}$

$gr(\overline{2}) = \{\overline{0}, \overline{2}, \overline{4}\}$ ss gpe de card 3

$gr(\overline{3}) = \{0, \overline{3}\}$ —— —— 2

$gr(\overline{4}) = \{\overline{0}, \overline{2}, \overline{4}\}$ —— 3.

(*) $gr(\overline{5}) = \{\overline{0}, \overline{1}, \overline{2}, \overline{3}, \overline{4}, \overline{5}\}$

$\quad \parallel$

$gr(\overline{-1})$ $\quad$ card 6.

Th 1.4.70

IMPORTANT

$\boxed{\text{Th : Les generateurs de } (\mathbb{Z}/n\mathbb{Z},+) \text{ ce sont exactement les classes } \mathring{k} \text{ avec } k \wedge n = 1}$

ie $gr(\mathring{k}) = \mathbb{Z}/n\mathbb{Z}$.

dem : • on suppose $gr(\mathring{k}) = \mathbb{Z}/n\mathbb{Z} \leftarrow \mathring{1}$

donc il existe $p \in \mathbb{Z}$ tel que $p.\mathring{k} = \mathring{1}$

ie $pk \equiv 1 [n]$ n divise $pk - 1$

$\exists q \in \mathbb{Z}$ $pk - 1 = qn$, $pk - qn = 1$

Bezout donc $\underline{k \wedge n = 1}$

• on suppose $k \wedge n = 1$ Bezout : $ku + nv = 1$

ie $k.u \equiv 1 [n]$ $\mathring{k} = \mathring{1}$

donc $\mathring{1} \in gr(\mathring{k})$ $\mathring{1} + \mathring{1} = \mathring{2} \in gr(\mathring{k})$

etc..... $gr(\mathring{k}) = \mathbb{Z}/n\mathbb{Z}$.

Application : $\mathbb{U}_n = \{$racines n^{ie} de l'unité$\}$.

$\varphi : (\mathbb{Z}/n\mathbb{Z},+) \longmapsto (\mathbb{U}_n, \times)$ $\underline{\text{iso}}$morphisme de groupes

$\mathring{k} \longmapsto e^{\frac{2ik\pi}{n}}$

si $\mathring{k} = \mathring{l}$ $l = k + nq$ $e^{\frac{2il\pi}{n}} = e^{\frac{2ik\pi}{n} + \frac{2inq\pi}{n}}$

$= e^{\frac{2ik\pi}{n}} \cancel{e^{2iq\pi}}_{1}$

$\alpha_k = e^{\frac{2ik\pi}{n}}$ engendre $\mathbb{U}_n$ ssi $k \wedge n = 1$ 14

φ isomorphisme. $\dot{\bar{k}}$ engendre $\mathbb{Z}/n\mathbb{Z} \iff \varphi(\dot{\bar{k}})$ engendre $\mathbb{U}_n$

1.4.5 Ordre d'un élément.

G groupe $\quad \varphi : \mathbb{Z} \longrightarrow G$

a fixé $\in G \quad k \longmapsto a^k$ (not $\times$)

$k.a$ (not $+$)

φ morphisme de groupe.

$\forall k, l \in \mathbb{Z} \quad a^{k+l} = a^k \times a^l$

Ker φ sous groupe de $\mathbb{Z}$ $\nearrow n\mathbb{Z} \quad n \in \mathbb{N}^*$, $\searrow 0\mathbb{Z} = \{0\}$.

• si $n = 0$, φ est injective. $gr(a)$ isomorphe à $\mathbb{Z}$

$gr(a) = \{\underbrace{\ldots a^{-p}, \ldots a^{-1}, e, a, a^2 \ldots a^p \ldots}_{\text{tous } \neq}\}$.

• $n \geq 1$: On dit que a est d'ordre n.

$a^k = e \iff k \in n\mathbb{Z} \quad$ n le + petit entier > 0

tq $\underline{a^n = e}$ (1er retour sur le neutre)

Ds ce cas $gr(a) = \{e, a, a^2 \ldots a^{n-1}\}$ Card n (tous $\neq$)

isomorphe à $(\mathbb{Z}/n\mathbb{Z}, +)$