03/04/2007

II Groupes

1 Définitions et exemples.

def un groupe est $(G,*)$ un ensemble G muni d'une loi $*$ t.q.

(1) $*$ est associative (2) $*$ a un élément neutre $e \in G$ $[\forall g \in G \; g*e = g = e*g]$

(3) tout $g \in G$ a un symétrique $g' \in G$ $[g*g' = e = g'*g]$

Souvent on note $* = \cdot$ multiplicativement $e = 1$, $g' = g^{-1}$

Si $*$ est claire par le contexte on dit le groupe G au lieu de $(G,*)$

un groupe est commutatif ou Abélien si sa loi est commutative

En ce cas [et en ce cas seulement] on peut noter sa loi $* = +$ additivement,
$e = 0$ et $g' = -g$

Exemples a) $(\mathbb{Z},+)$; $(\mathbb{Q},+)$; $(\mathbb{R},+)$; si $0 \neq N \in \mathbb{N}$, $\mathbb{N}/_{\text{mod } N}$

$(\{-1,+1\}, \times)$; $(\mathbb{Q}\setminus\{0\} = \mathbb{Q}^*, \times)$; $(\mathbb{R}\setminus\{0\} = \mathbb{R}^*, \times)$ sont des groupes abéliens

Exercice $1 < N \in \mathbb{N}$ $(\{\bar{n} \in \mathbb{N}/_{\text{mod } N} \mid n \text{ premier à } N\}, \times)$ est un groupe abélien.

b) $GL_2(\mathbb{R}) = \left(\left\{\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in M_2(\mathbb{R}) \;\middle|\; ad-bc \neq 0\right\}, \circ\right)$ est un groupe

$\circ$ produit des matrices

$$e = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = 1 \; ; \; \begin{pmatrix} a & b \\ c & d \end{pmatrix}^{-1} = \frac{1}{ad-bc} \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}$$

Rmq $\begin{pmatrix} a & b \\ c & d \end{pmatrix}^{-1} \mathcal{L} \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}$

relation de colinéarité $M \mathcal{L} M'$ ssi $\exists \lambda \in \mathbb{R}\setminus\{0\}$ $M' = \lambda M$
ds $M_2(\mathbb{R})\setminus\{0\}$

b'] $PGL_2(\mathbb{R}) = \left(GL_2(\mathbb{R})/_{\mathcal{R}} \,,\, \underset{\substack{\uparrow \\ \text{loi induite par } \circ}}{\bar{\circ}} \right)$ est un groupe :

$$e = \overline{\begin{pmatrix}1&0\\0&1\end{pmatrix}} \quad \left[= \left\{ \begin{pmatrix}\lambda&0\\0&\lambda\end{pmatrix} \mid \lambda\in\mathbb{R}\setminus\{0\} \right\} \right], \quad \overline{\begin{pmatrix}a&b\\c&d\end{pmatrix}} = \overline{\begin{pmatrix}d&-b\\-c&a\end{pmatrix}}$$

[les calculs dans $PGL_2(\mathbb{R})$ sont plus simples que dans $GL_2(\mathbb{R})$!]

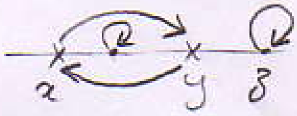
Ces groupes ne sont pas abeliens :

$$\begin{pmatrix}1&1\\0&1\end{pmatrix}\begin{pmatrix}1&0\\1&1\end{pmatrix} = \begin{pmatrix}2&1\\1&1\end{pmatrix} \neq \begin{pmatrix}1&1\\1&2\end{pmatrix} = \begin{pmatrix}1&0\\1&1\end{pmatrix}\begin{pmatrix}1&1\\0&1\end{pmatrix}$$

d] Soit X un ensemble $(\mathfrak{S}(X), \underset{\substack{\uparrow \\ \text{composition des bijections}}}{\circ})$ est un groupe

Si X a au moins deux éléments $x \neq y \in X$ la transposition de x et y est $(x,y) \in \mathfrak{S}(X)$ si $z \in X\setminus\{x,y\}$ $(x,y)(z) = z$

$$(x,y)(x) = y \,;\, (x,y)(y) = x$$



Proposition (i) Si $X = \emptyset$ ou $X = \{x\}$ a un seul élément $\mathfrak{S}(X) = \{Id_X\}$ n'a
(X a au plus un él^t)

qu'un élement et est isomorphe à $(\mathbb{N}/_{\text{mod } 1}, +) = (\{\bar{0}\}, +)$ $[$et à $(\underset{\substack{\cap\\ \mathbb{Z}\\ \cap\\ \mathbb{R}}}{\{0\}}, +), (\underset{\substack{\cap\\ \mathbb{Q}^*_+\\ \cap\\ \mathbb{R}\setminus\{0\}}}{\{1\}}, \times)]$

(ii) Si $X = \{x,y\}$ a deux éléments $\mathfrak{S}(X) = \{Id_X, (x,y)\}$ a deux élements et est isomorphe à $(\mathbb{N}/_{\text{mod } 2}, +) = (\{\bar{0},\bar{1}\}, +)$ $[$et à $(\{-1,1\}, \times)]$

(iii) Si X a au moins trois éléments $x \neq y \neq z \neq x$ distincts $(\mathfrak{S}(X), \circ)$ n'est pas abélien : $(x,y)\circ(y,z) \neq (y,z)\circ(x,y)$

pv de (iii) $(x,y)\circ(y,z)(z) = (x,y)((y,z)(z)) = (x,y)(y) = x$

$$\neq$$

$(y,z)\circ(x,y)(z) = (y,z)((x,y)(z)) = (y,z)(z) \quad y$ ☐

Exercice prouver (i) et (ii) ∎

2 Sous-groupes et morphismes de groupe.

def un sous-groupe H d'un groupe G est une partie $H \subset G$ stable par la loi de G et t.q., muni de la loi induite, H est un groupe

on note $H < G$

Lemme Si H est un sous-groupe de G $e_H = e_G$ et $\forall h \in H$, $h^{-1_H} = h^{-1}$ ← inverse de H

pv $e_H = e_H \cdot e_H \Rightarrow e_G = e_H \cdot e_H^{-1} = (e_H \cdot e_H) \cdot e_H^{-1} = e_H \cdot (e_H \cdot e_H^{-1}) = e_H \cdot e_G = e_H$

$e_G = h \cdot h^{-1} \Rightarrow h^{-1_H} = h^{-1_H} \cdot e_G = h^{-1_H}(h \cdot h^{-1}) = (h^{-1_H} h) \cdot h^{-1} = e_H \cdot h^{-1} = e_G \cdot h^{-1} = h^{-1}$ ∎

Exemples a) $\mathbb{Z}$ $(=(\mathbb{Z},+))$ est un sous groupe de $\mathbb{Q}$ $(=(\mathbb{Q},+))$

b) $\left(\left\{\begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} \in M_2(\mathbb{R})\right\}, \circ\right)$; $\left\{\begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix} \in M_2(\mathbb{R}) \mid a \neq 0\right\}, \circ)$

sont des sous-groupes de $GL_2(\mathbb{R})$ $\left[\begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix}^{-1} = \begin{pmatrix} 1 & -b \\ 0 & 1 \end{pmatrix}; \begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix}^{-1} = \begin{pmatrix} a^{-1} & -ba^{-1} \\ 0 & 1 \end{pmatrix}\right]$

Exercice vérifier la stabilité.

Proposition (Exercice) une partie $H \subset G$ d'un groupe G est un sous-groupe ssi

(1) $H \neq \emptyset$ $(\Leftarrow (1')\ e_G \in H)$ et (2) $\forall h, k \in H$ $h \cdot k^{-1} \in H$

def un morphisme d'un groupe G vers un groupe K est

$f : G \to K$ un morphisme de leur lois

Exemple a) $\exp : (\mathbb{R},+) \to (\mathbb{R}^*, \times)$ $t \mapsto e^t$; $\exp : (\mathbb{C},+) \to (\mathbb{C}^*, \times)$ $t \mapsto e^t$ (avec $\mathbb{R}^* = \mathbb{R} \setminus \{0\}$, $\mathbb{C}^* = \mathbb{C} \setminus \{0\}$)

b) Si $H < G$ est $\mathrm{incl}_H^G : H \to G$, $h \mapsto h$

def et prop l'image et le noyau d'un morphisme $f : G \to H$ de groupes sont

$$\mathrm{Im} f = \{f(g) \mid g \in G\} (\subset K) \quad \text{et} \quad \ker f = \{g \in G \mid f(g) = e_K\} (\subset G)$$

sont des sous-groupes de H et G respectivement.

pr pour $\mathrm{Im} f$ $\forall f(g_1), f(g_2) \in \mathrm{Im} f$ $\; f(g_1)\cdot f(g_2) = f(g_1 g_2) \in \mathrm{Im}(f)$

$f(g_1)\cdot f(e_G) = f(g_1 \cdot e_G) = f(g_1) = f(e_G \cdot g_1) = f(e_G)\cdot f(g_1)$ donc $f(e_G)$ neutre

$f(g_1)\cdot f(g_1^{-1}) = f(g_1 \cdot g_1^{-1}) = f(e_G) = f(g_1^{-1}\cdot g_1) = f(g_1^{-1})\cdot f(g_1)$ donc $f(g_1)^{-1} = f(g_1^{-1}) \in \mathrm{Im} f$ ■

(on a montré lemme Si $f : G \to K$ morphisme $f(e_G) = e_G$ et $f(g^{-1}) = f(g)^{-1}$)

o pour $\ker f$: $\forall g_1, g_2 \in \ker f$ $\; f(g_1 g_2) = f(g_1)\cdot f(g_2) = e_H \cdot e_H$ donc $g_1 g_2 \in \ker f$

on a vu $f(e_G) = e_H$ donc $e_G \in \ker f$ et $f(g_1^{-1}) = f(g_1)^{-1} = e_K^{-1} = e_K$ donc $g_1 \in \ker f$ ■

Théorème un morphisme $f : G \to K$ est injectif ssi ~~$\ker f = \{e\}$~~

son noyau $\ker f = \{e_G\}$ est réduit à l'élément neutre de G.

pr $\Rightarrow$ $\forall g \in \ker f$ $\; f(g) = e_K = f(e_G) \underset{f \text{ injectif}}{\Rightarrow} g = e_G$

$\Leftarrow$ $\forall g, g' \in G$ t.q. $f(g) = f(g')$, $e_K = f(g)^{-1}\cdot f(g') = f(g^{-1} g')$ donc $g^{-1} g' \in \ker g$

et (Hypothèse $\ker g = \{e_G\}$) $e_G = g^{-1}\cdot g' \Rightarrow g = g \cdot e_G = g \cdot g^{-1} g' = g'$ ◻

on a donc $(f(g) = f(g')) \Rightarrow g = g'$ c.a.d. f est injective. ■

Exercices ① Si G et H sont deux groupes alors leur produit $G \times H$, muni de la loi produit est un groupe.

② Si $0 < N \in \mathbb{N}$, $p, q \in \mathbb{N}$ tq $N = pq$ alors (voir contrôle)

$\pi : \mathbb{N}/_{\mathrm{mod}\,N} \to \mathbb{N}/_{\mathrm{mod}\,p} \times \mathbb{N}/_{\mathrm{mod}\,q}$ $\quad \bar{n}_{\mathrm{mod}\,N} \mapsto (\bar{n}_{\mathrm{mod}\,p}, \bar{n}_{\mathrm{mod}\,q})$ est morphisme de groupe

<u>Lemme</u> Si $N = pq$ le noyau de $\pi : \mathbb{N}/_{\mathrm{mod}\,N} \to \mathbb{N}/_{\mathrm{mod}\,p} \times \mathbb{N}/_{\mathrm{mod}\,q}$

$\{\bar{n} \in \mathbb{N}/_{\mathrm{mod}\,pq} \mid p|n \text{ et } q|n\}$ est $\{\bar{0}\}$ ssi p et q sont premiers entre eux.

pv

$\Rightarrow$ si $1 < d$, avec $d|p$ et $d|q$ il y a $k, l \in \mathbb{N}$ t.q. $p = dk$ et $q = dl$ alors

$1 < dkl = \frac{pq}{d} < N$ et $p | dkl$, $q | dlk = dkl$ donc $\bar{0} \neq \overline{dkl} \in \ker \pi$ □

$\Leftarrow$ si $\bar{n} \in \ker \pi$ $\; p|n$ donc $\exists\, k \in \mathbb{N}$ tq $n = pk$

et $q | n = pk \Rightarrow q | k$ donc $\exists\, l \in \mathbb{N}$ tq $k = ql$ et $n = pql$ c.a.d $pq | n$
car p et q premiers entre eux

et $\bar{n} = \{\bar{0}\}$ ■

<u>Corollaire</u> (thm des restes chinois) Soit $p, q \in \mathbb{N}$ des entiers premiers entre eux

alors $\pi : \mathbb{N}/_{\mathrm{mod}\,(pq)} \to \mathbb{N}/_{\mathrm{mod}\,p} \times \mathbb{N}/_{\mathrm{mod}\,q}$

est un isomorphisme de groupe

pv c'est un morphisme par l'exercice, injectif par Lemme et thm

et $\mathrm{Card}(\mathbb{N}/_{\mathrm{mod}\,pq}) = pq = \mathrm{Card}(\mathbb{N}/_{\mathrm{mod}\,p}) \times \mathrm{Card}(\mathbb{N}/_{\mathrm{mod}\,q}) = \mathrm{Card}(\mathbb{N}/_{\mathrm{mod}\,p} \times \mathbb{N}/_{\mathrm{mod}\,q})$

donc π est bijectif donc isomorphisme. ■

3 Congruence modulo un sous-groupe et groupe quotient (cas abélien)

<u>Prop et def</u> Soit H un sous-groupe d'un groupe G. Deux éléments $g, g' \in G$ sont congrus modulo H noté $g' \equiv g \mod H$ si $g^{-1}g' \in H$

La congruence modulo H est une relation d'équivalence sur G l'ensemble quotient est le quotient $G/_H$ de G par H

pv (i) réfl. $e \in H \Rightarrow g^{-1}g = e \in H$ donc $g \equiv g \mod H$

(ii) symé. $g' \equiv g \mod H \Rightarrow g^{-1}g' \in H \Rightarrow (g')^{-1} \cdot g = (g')^{-1}(g^{-1})^{-1} \in H \Rightarrow g \equiv g' \mod H$

(iii) trans. $\begin{cases} g' \equiv g \mod H \\ g'' \equiv g' \mod H \end{cases} \Rightarrow \begin{rcases} g^{-1}g' \in H \\ (g')^{-1}g'' \in H \end{rcases} \Rightarrow g^{-1}g'' = g^{-1} e_G g'' = g^{-1} \cdot (g' \cdot (g')^{-1}) \cdot g$

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

donc $g'' \equiv g \mod H$ ■

<u>Exemple</u> [Exercice] $G = GL_2(\mathbb{R})$ alors $H = \left\{ \begin{pmatrix} 1 & b \\ 0 & d \end{pmatrix} \in M_2(\mathbb{R}) \,\middle|\, d \neq 0 \right\}$ et

$K = \left\{ \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \in M_2(\mathbb{R}) \,\middle|\, ad \neq 0 \right\}$ sont des sous groupes

$M' \equiv M \mod H$ ssi $M' \begin{bmatrix} 1 \\ 0 \end{bmatrix} = M \begin{bmatrix} 1 \\ 0 \end{bmatrix}$ (m̃ première colonne)

$M' \equiv M \mod K$ ssi $M' \begin{bmatrix} 1 \\ 0 \end{bmatrix} \mathcal{L}\, M \begin{bmatrix} 1 \\ 0 \end{bmatrix}$ ((des premières colonnes) colinéaires

<u>Remarque générale</u> $g' \equiv g \mod H$ ssi $\exists h \in H$ tq $g' = g \cdot h$

pv $\Rightarrow$ $g^{-1}g' = h \in H \Rightarrow g \cdot h = g(g^{-1}g') = (gg^{-1})g' = eg' = g'$

$\Leftarrow$ $g' = g \cdot h \Rightarrow g^{-1}g' = g^{-1}(g \cdot h) = (g^{-1}g)h = e \cdot h$

<u>Théorème et définition</u> Soit G un groupe abélien et H un sous-groupe de G.

Alors la congruence modulo H est compatible à la loi de G.

Le <u>groupe quotient</u> de G par le sous-groupe H est $G/_H$ muni de la loi quotient.

pv. Comme la loi de G est commutative il suffit de vérifier

$$\forall g, g', g'' \in G \text{ avec } g' \equiv g'' \bmod H \quad gg' \equiv gg'' \bmod H$$

$$g' \equiv g'' \bmod H \Rightarrow (g')^{-1} g'' = h \in H \quad \text{donc}$$

$$gg' \cdot h = (gg')(g')^{-1} \cdot g'' = g(g' \cdot (g')^{-1}) \cdot g'' = g \cdot e \cdot g'' = gg''$$

et, par la remarque, $gg'' \equiv gg' \bmod H$ et $gg' \equiv gg'' \bmod H$ ∎

<u>Exercice</u> faire une autre pv en calculant $(gg')^{-1} \cdot (gg'')$ □

<u>Exemples</u> Si $N \in \mathbb{Z}$ alors (exercice) $N\mathbb{Z} \overset{\text{def}}{=} \{Nk \mid k \in \mathbb{Z}\}$ est un sous-groupe de $\mathbb{Z}$

$$m, n \in \mathbb{Z} \quad m \equiv n \bmod N\mathbb{Z} \text{ ssi } -m+n \in N\mathbb{Z}$$
$$\Leftrightarrow \exists k \in \mathbb{Z} \text{ tq } n-m = -m+n = Nk$$

on note $\mathbb{Z}/_{N\mathbb{Z}}$ le groupe quotient

<u>Exercice</u> Si $N \in \mathbb{N}$ tq l'inclusion $\mathbb{N} \hookrightarrow \mathbb{Z}$ passe au quotient

en $\mathbb{N}/_{\bmod N} \to \mathbb{Z}/_{N\mathbb{Z}}$ qui est un isomorphisme. si $N \neq 0$

<u>Remarque</u> le passage au quotient est aussi vrai si $N = 0 \in \mathbb{N}$,

mais en ce cas $(\mathbb{N}/_{\bmod \mathbb{N}}, +)$ isomorphe à $(\mathbb{N}, +)$ n'est pas un groupe

• $\mathbb{N}/_{\bmod 0} \to \mathbb{Z}/_{0\mathbb{Z}}$ reste injectif mais n'est pas surjectif.

8

b) (contre-exemple) $G = GL_2(\mathbb{R}) > H = \left\{ \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \in M_2(\mathbb{R}) \mid ad \neq 0 \right\}$

la congruence mod H n'est pas compatible ā $\circ$

pv $M = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$ $M' = \begin{pmatrix} 2 & 1 \\ 1 & 1 \end{pmatrix}$, $M'' = \begin{pmatrix} 2 & -1 \\ 1 & 0 \end{pmatrix}$ $M' \equiv M'' \bmod H$ (m̃ premiere colonne)

mais $M'M = \begin{pmatrix} 3 & 1 \\ 2 & 1 \end{pmatrix} \not\equiv \begin{pmatrix} 1 & -1 \\ 1 & 0 \end{pmatrix} = M''M \bmod H$

fin 03/12/2007

c) Si $f : G \to K$ est un morphisme de groupe alors

f passe au quotient en une application injective $G/_{\ker f} \to K$ d'image $\mathrm{Im} f$

pv: $g, g' \in G$ $g \equiv g' \bmod \ker f$ soit $h \in \ker f$ tq $g = g'h$

$$f(g) = f(g'h) = f(g') \cdot f(h) = f(g') \cdot e_K = f(g') \quad \square$$

injectivité: $\bar{f}(\bar{g}) = \bar{f}(\bar{g'}) \Rightarrow f(g) = f(g') \Rightarrow f(g^{-1}g') = f(g)^{-1} \cdot f(g') = e_K$ donc $g^{-1}g' \in \ker f$ et $g \equiv g' \bmod \ker f$ c.a.d $\bar{g} = \bar{g'}$ ■

En ce cas la congruence mod $\ker f$ est compatible avec $\circ$,

$G/_{\ker f}$ muni de la loi quotient est un groupe isomorphe, par $\bar{f}$ ā $\mathrm{Im} f$.

c') $f = \exp : \mathbb{C} \to \mathbb{C}^*$ morphisme de noyau $\mathbb{Z}2\pi i = \{k2\pi i \mid k \in \mathbb{Z}\}$,

comme f surjectif $\mathrm{Im} f = \mathbb{C}^*$ et $(\mathbb{C}^*, \times)$ est isomorphe,

par le passage au quotient de exp, à $(\mathbb{C}, +)/_{\mathbb{Z}2\pi i}$.

c'') $f : (\mathbb{R}, +) \to (\{z \in \mathbb{C} \mid |z| = 1\}, \times)$ morphisme surjectif
$t \mapsto \exp(it)$

de noyau $\mathbb{Z}2\pi = \{k2\pi \mid k \in \mathbb{Z}\}$ donc $(\mathbb{R}/_{2\pi\mathbb{Z}}, +)$ isomorphe à $(\{z \in \mathbb{C} \mid |z| = 1\}, \times)$