Structure algèbre.

I Groupe.

(1) Loi de composition interne:

$$E \times E \to E$$
$$\perp : (x, y) \mapsto x \perp y.$$

une application

E est muni d'une loi de composition interne

Déf: E, s.t un ensemble et $\perp$ une loi de composition interne sur E

(2) Associativité:

- $\perp$ est associative $\Leftrightarrow \forall (x, y, z) \in E$

$$(x \perp y) \perp z = x \perp (y \perp z)$$

• $\cdot$ est commutative $\Leftrightarrow$

$\forall x, y \in E \quad x \cdot y = y \cdot x$.

• admet un élt neutre dans E.

$\exists e \in E \ \forall x \in E \quad x \cdot e = e \cdot x = x$.

Soit E un ens muni de 2 lois.

• et T

T est distributive % à •

$\Leftrightarrow \forall x, y, z \in E$

$$x T (y \bullet z) = (x T y) \bullet (x T z)$$

x à gauche

Distribution à gauche

$$(y \bullet z) T x = (y T x) \bullet (z T x)$$

Distribution à droite

E un ensemble muni •

soit $x \in E$: x admet un symétrique

$\Leftrightarrow \exists y \in E \quad x \cdot y = y \cdot x = e$

le symétrique — l'inverse de x.

$y = x^{-1}$

notation

$x \cdot x^{-1} = e = x^{-1} \cdot x = e$

$x \in E$: x est regulié :

$\forall y, z \in E \quad xy = xz \Rightarrow y = z$

régulier à gauche

$yx = zx \Rightarrow y = z$

régulier à droite

$(G, \circ)$ est un groupe

ssi

1. admet 1 élt neutre de G.
2. associative
3. $\forall x \in G$, x admet un inverse

$(G, \circ)$: groupe abélien

$\Leftrightarrow \forall x, y \in G \quad x \circ y = y \circ x$

Exemples :

$(\mathbb{C}, +)$; $(\mathbb{R}, +)$; $(\mathbb{Z}, +)$;

$(\mathbb{C}^*, \cdot)$; $(\mathbb{R}^*, \cdot)$; $(\mathbb{Q}^*, \cdot)$

$(\mathcal{U}_n, \cdot)$: $\mathcal{U}_n = \left\{ e^{\frac{2ik\pi}{n}} \mid k \in \{0, \dots, n-1\} \right\}$

$(\mathcal{M}_n(\mathbb{K}), +)$; $(GL_n(\mathbb{K}), \cdot)$

$(S_n, \circ)$ $S_n = \{\sigma : [\![1,n]\!] \to [\![1,n]\!] \mid \sigma \text{ est bijective}\}$

$k \to \sigma(k)$

est un groupe.

non commutatif en générale

si $n = 2$: $(S_2, \circ)$ est un groupe abélien

$n \geq 3$ non abélien

$A, B \in GL_n(\mathbb{K})$ $A \times B \neq B \times A$

Morphisme de Groupe :

$(G, \cdot) \to (E, T)$

$\varphi \quad x \to \varphi(x)$

φ est morphisme de Groupe

$\Leftrightarrow \forall x,y \in G_1 \cdot \varphi(x \cdot y) = \varphi(x) \top \varphi(y)$

- φ est un endomorphisme

$\Leftrightarrow G_1 = E$ et $\cdot = \top$

- φ est un isomorphisme $\Leftrightarrow$

φ est un morphisme bijectif

- φ est un automorphisme $\Leftrightarrow$

endomorphisme bijectif

$$\varphi : \begin{array}{ccc} G_1 & \to & E \\ x & \to & \varphi(x) \end{array} \quad e_{G_1} \; ; \; e_E$$

Si φ est un morphisme :

$$\varphi(e_{G_1}) = e_E$$

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

$\ker\varphi$ = le noyau de φ

$$= \{x \in G \mid \varphi(x) = e_H\}$$

$$\mathrm{Im}\varphi = \varphi(G) = \{\varphi(x) \mid x \in G\}$$

② Sous-groupe.

Déf : $(G, \cdot)$ un groupe et H une partie de G.

H sg de G $\Leftrightarrow$

$$\begin{cases} e \in H \\ \forall x, y \in H \quad xy^{-1} \in H \end{cases}$$

$\Leftrightarrow$

$$\begin{cases} \underline{H \neq \emptyset} \\ \forall x, y \in H \quad xy^{-1} \in H \end{cases}$$

$\Leftrightarrow$ $\begin{cases} H \text{ est stable par la loi } \cdot \\ H \neq \emptyset \\ \forall x \in H \quad x^{-1} \in H \end{cases}$

$(G, \cdot)$ est un groupe. H_1, H_2 deux sg de G.

$H_1 \cap H_2$ est un sg de G.

$(H_i)_{i \in I}$ une famille de sg de G.

$\bigcap_{i \in I} H_i$ sg de G.

- $H_1 \cup H_2$ sg de G ssi $H_1 \subset H_2$ ou $H_2 \subset H_1$

- $\varphi : G \to H$, $x \to \varphi(x)$ un morphisme de groupe.

si E st un sg de G alors

$\varphi(E)$ st un sg de H

si H' sg de H alors $\varphi^{-1}(H')$ sg de G

- φ st injective $\Leftrightarrow \ker\varphi = \{e_G\}$
- φ st surjective $\Leftrightarrow \varphi(G) = H$.

Soit $x \in G$, G st un groupe.

l'ordre de x $o(x) = k \in \mathbb{N}^*$ tq

$x^k = e$

$k = \min\{p \in \mathbb{N}^* / x^p = e\}$

$(GL_n(\mathbb{K}), .)$ $\mathbb{K} = \mathbb{C}$

$A = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$ on a $A^2 = I_2$.

$o(A) = 2$.

$A = \begin{pmatrix} e^{i\frac{\pi}{3}} & 0 \\ 0 & e^{i\frac{\pi}{6}} \end{pmatrix}$ $o(A) =$

$A^K = I_2 \iff \begin{cases} e^{i\frac{2K\pi}{3}} = 1 \\ e^{i\frac{K\pi}{6}} = 1 \end{cases}$

$\iff \begin{cases} 6/K \\ 12/K \end{cases} \Rightarrow K = 12$

$A^{12} = I_2$. $o(A) = 12$.

l'ordre d'un groupe $|G| = \text{Card}(G)$

G est un groupe fini

Soit $x \in G$. $o(x) = p$.

$x^m = e \Leftrightarrow p / m$.

G est fini et $x \in G$. alors

$o(x) / |G|$

G est fini et H sg de G.

alors $|H| / |G|$ Th de Lagrange.

$A \subset G$. avec G un groupe

$\langle A \rangle$: sg engendré par A

Exemple. G sera engendré par A CE

$$\mathrm{Vect}(A) = \bigcap_{\substack{H \text{ sev de } E \\ A \subset H}} H$$: le plus petit sev de E contenant A

$$\langle A \rangle = \bigcap_{\substack{H \text{ sg de } G \\ A \subset H}} H$$ le plus petit sg de G contenant A.

$$= \left\{ x_1^{\varepsilon_1} x_2^{\varepsilon_2} \dots x_r^{\varepsilon_r} \;/\; r \in \mathbb{N}^* \right.$$
$$\left. \forall i \in [\![1, r]\!] \; x_i \in A \right.$$
$$\left. \varepsilon_i \in \{1, -1\} \right\}$$

$$\left(GL_2(\mathbb{R}), \times\right)$$

$$A = \left\{ \underbrace{\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}}_{A_1} ; \underbrace{\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}}_{A_2} \right\}$$

$$\langle A \rangle = \left\{ \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}; \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}; A_1 A_2; A_1 A_2^{-1}; A_1^{-1}; A_2^{-1}; A_2 A_1 A_2^{-1} A_1; A_1 A_2^{-1}; A_2 A_1^{-1}; A_1^{-1} A_2^{-1}; A_2 A_1^{-1}; \underline{\underline{I_2}} \dots \right\}$$

$$A_1^2; A_2^2; A_1^3; A_2^3 \dots$$

$$A_1^2 A_2 \dots$$

$$A = \{x\}$$

$$\langle x \rangle = \{ x^n \mid n \in \mathbb{Z} \}$$

$$A = \{x, y\} \qquad x^0 = e$$

$$\langle A \rangle = \{ x^k y^p \mid k, p \in \mathbb{Z} \}$$

Si $xy = yx$.

$G = \langle x \rangle$ monogène

G un groupe monogène fini

$=$ G groupe cyclique.

$(\mathbb{Z}, \cdot)$; $(\{-1, 1\}, \cdot)$; $(\mathbb{Z}/n\mathbb{Z}, +)$

$\{i, -i, 1, -1\}$ $n = 4$.

$(\mathbb{Z}, +) = \langle 1 \rangle$ monogène.

$(-\mathbb{Z}, +)$ le sg de $(\mathbb{Z}, +)$

$= (n\mathbb{Z}, +)$ $n \in \mathbb{N}$

$\mathbb{Z}/n\mathbb{Z} = \langle \bar{1} \rangle = \langle \bar{m} \rangle$ avec

$m \wedge n = 1$.

Si G est un groupe cyclique

Ses sg sont aussi cyclique.

Si G est un groupe monogène

alors ses sg sont monogène.

$\mathbb{Z}/n\mathbb{Z} = \langle \bar{1} \rangle$.

sg $\mathbb{Z}/n\mathbb{Z}$ sont cyclique

donc si H sg $(\mathbb{Z}/n\mathbb{Z}, +)$

alors $H = \langle \bar{m} \rangle$ avec m/n.

$m = kn \qquad \bar{m} = \bar{0}$.

$H = \{\bar{0}\}$.

si m/n $\exists k \in \mathbb{N}^*$ tq $n = km$.

si $o(x) = k$.

$$\langle x \rangle = \{e, x, \dots, x^{k-1}\}$$

$$= \{x^p \mid p \in \mathbb{Z}\}$$

$$\langle x \rangle = \{0, x, 2x, \dots, (k-1)x\}$$

si m/n ; $o(\bar{m}) = k$ tq $n = km$.

$$\langle \bar{m} \rangle = \{0, \bar{m}, 2\bar{m}, \dots, (k-1)\bar{m}\}$$

$H \subseteq (\mathbb{Z}/n\mathbb{Z})$. $\Rightarrow H$ st un groupe cyclique $\exists m \in [\![2, n-1]\!]$ $(H = \langle \bar{m} \rangle)$

Si $|H| = o(\bar{m}) = d$.

$d\bar{m} = \bar{0} \iff dm \equiv 0 [n]$

~~$d \wedge m$~~ $\because o(\bar{m}) = d / n = |\mathbb{Z}/n\mathbb{Z}|$

$m < n$.

$d | n$ et $m < n$ et $dm \equiv 0 [n]$

$d m = n$.

Ce qui prouve m / n.

Sg de $\mathbb{Z}/n\mathbb{Z}$ sont $\langle \bar{m} \rangle$ m/n

So d'un groupe monoge est un groupe monoge.

G est un groupe monogène

$G = \{x^k \mid k \in \mathbb{Z}\}$

G est un groupe cyclique

$G = \{e, x, \dots, x^{n-1}\}$ $|G| = n$.

H sg de G.

Soit $y \in H$; $y = x^k$ $k \in \{0, n-1\}$

$H = \{x^{k_1}, \dots, x^{k_r} = e\} = \langle x^{k_1} \rangle$

$1 \leq k_1 < k_2 \dots < k_r$

H sg de G soit $y \in H$ $y = x^k$

$y \in G$.

$K = k_1 q + r \qquad r < k_1$

$y = x^k = x^{k_1 q} x^r$

on a $x^{k_1} \in H \quad x^{k_1 q} \in H$

$(x^{k_1})^q \in H$

$(x^{k_1 q})^{-1} \in H$ car H sg de G.

$x^r \in H$. Donc $r = 0$

$y = (x^{k_1})^q \in \langle x^{k_1} \rangle$

$H \subset \langle x^{k_1} \rangle$

$x^{k_1} \in H \quad (x^{k_1})^q \subset H$

$\Rightarrow \langle x^{k_1} \rangle \subset H$

$H = \langle x^{k_1} \rangle$ c'est un sg cyclique

A est un anneau intègre

A n'admet pas de diviseur de 0

$(A, +, \cdot)$ $\exists x, y \in A \setminus \{0\}$ $xy = 0$

0 1

$(A, +, \times)$: $+, \times$ sont des lois

- interne
- loi externe.

$\mathbb{K}$ corps

- $\cdot$ est une loi externe sur A.

$\mathbb{K} \times A \to A$

$(\lambda, x) \mapsto \lambda . x$

$\left.\begin{array}{l}(A,+,\times) \text{ un anneau} \\ (A,+,\cdot) \text{ IK-ev.}\end{array}\right\}$ une algèbre

Exemple : $(\mathbb{K},+,\times,\cdot)$

$(\mathcal{M}_n(\mathbb{K}),+,\underbrace{\times}_{A\times B},\cdot)$ une algèbre.

$\left.\begin{array}{l}(\mathcal{M}_n(\mathbb{K}),+,\times) \text{ est un anneau.} \\ (\mathcal{M}_n(\mathbb{K}),+,\cdot) \text{ est IK-ev.}\end{array}\right\}$ une algèbre.

1er Exercice

$\varphi : G \to G'$

A une partie de G.

$$\langle \varphi(A) \rangle = \varphi(\langle A \rangle)$$

① On a $A \subset \langle A \rangle$ alors

$$\varphi(A) \subset \varphi(\langle A \rangle)$$

$$\left(A \subset B \Rightarrow f(A) \subset f(B) \right)$$

$$\varphi : \begin{array}{ccc} G & \to & G' \\ n & \to & \varphi(n) \end{array} \quad \text{application}$$

on $\varphi(A)$ est une partie de G'

$\varphi(\langle A \rangle)$ sg de G'

$$\langle \varphi(A) \rangle \subset \varphi(\langle A \rangle) \quad ①$$

2/

Soit $y \in \varphi(\langle A \rangle)$ alors

$\exists x \in \langle A \rangle$ tq $\varphi(x) = y$.

on a :

$x \in \langle A \rangle$ donc $\exists r \in \mathbb{N}^*$ tq

$$x = x_1^{\varepsilon_1} \dots x_r^{\varepsilon_r}$$

avec $\varepsilon_i \in \{1, -1\}$

et $x_i \in A$

on obtient $\varphi(x) = \varphi(x_1^{\varepsilon_1} \dots x_r^{\varepsilon_r})$

$\Rightarrow$

$$\varphi(x) = \varphi(x_1)^{\varepsilon_1} \dots \varphi(x_r)^{\varepsilon_r}$$

$\varphi(x_i) \in \varphi(A) \subset \langle \varphi(A) \rangle$ $\forall i \in [\![1, r]\!]$

$\varphi(x_1)^{\varepsilon_1} \dots \varphi(x_r)^{\varepsilon_r} \in \langle \varphi(A) \rangle$

D'où $g \in \langle \varphi(A) \rangle$.

Par la suite

$$\varphi(\langle A \rangle) \subset \langle \varphi(A) \rangle \quad (2)$$

D'après (1) et (2) on a :

$$\varphi(\langle A \rangle) = \langle \varphi(A) \rangle$$

Exo n°2 : G un groupe.

$$Z(G) = \{ g \in G \mid \forall h \in G \ gh = hg \}$$

Le centre de G.

$Z(G)$ de G.

$Z(G) \neq \phi$ $\quad e \in Z(G)$.

Soit $xy \in Z(G)$. Montrons que $xy^{-1} \in Z(G)$

Soit $h \in G$. Montrons que $y^{-1}h = hy^{-1}$

On a $yh = hy$.

On a $y^{-1}yh = y^{-1}hy$.

$\Leftrightarrow h = y^{-1}hy$.

$\Leftrightarrow hy^{-1} = y^{-1}hyy^{-1} = y^{-1}h$.

Donc $y^{-1} \in Z(G)$

Soit $h \in G$ on a $xy^{-1}h = xhy^{-1}$

$= hxy^{-1}$

Donc $xy^{-1} \in Z(G)$.

$Z(G)$ s.t m.s.g de G. Commutatif

Ex 3)

$\varphi : G \to G'$

$x \to \varphi(x)$.

$o(x) = p \Rightarrow o(\varphi(x))$ fini

fini

$\Rightarrow o(\varphi(x)) \mid p$

Ex G un groupe.

$\forall x \in G \quad x^2 = e$.

(1) G est abélien :

Soit $x, y \in G$. (1) $xy \times xy = (xy)^2 = e$.

(2) $x^2 y^2 = e \times e = e$.

$xy\,xy = xxyy \Rightarrow yx = xy$.

Dans 1 groupe tous les él sont réguliers.

② si $|G| < +\infty$ alors $|G| = 2^p$.

puisque $|G| < +\infty$ alors G admet $G = \langle x_1, \dots, x_p \rangle$.

Soit $\{x_1, \dots, x_p\}$ la plus petite famille (question de cardinal) qui engendre G.

$\forall x \in G$. $x = x_1^{\alpha_1} \dots x_p^{\alpha_p}$ avec $\alpha_1 \in \mathbb{Z} \dots \alpha_p \in \mathbb{Z}$

$$\left(\mathbb{Z}/2\mathbb{Z}^{+}\right)^{p} \longrightarrow G_r$$

$$f\left(\bar{\alpha}_1, \bar{\alpha}_2, \ldots \bar{\alpha}_p\right) \longrightarrow x_1^{\alpha_1} \ldots x_p^{\alpha_p}$$

$$\bar{\alpha}_1 \in \{\bar{0}, \bar{1}\}$$

$$x_1^{\alpha_1} = \begin{cases} e \\ x_1 \end{cases} \qquad \underline{x^2 = e}$$

$$f\left((\bar{\alpha}_1, \ldots \bar{\alpha}_p) + (\bar{\beta}_1, \ldots \bar{\beta}_p)\right)$$

$$= f\left(\bar{\alpha}_1 + \bar{\beta}_1, \ldots, \bar{\alpha}_p + \bar{\beta}_p\right)$$

$$= x_1^{\alpha_1 + \beta_1} \times \ldots \times x_p^{\alpha_p + \beta_p}$$

$$= x_1^{\alpha_1} \cdot x_p^{\alpha_p} \times x_1^{\beta_1} \ldots x_p^{\beta_1}$$

$$= f(\bar{\alpha}_1, \ldots \bar{\alpha}_p) \times f(\bar{\beta}_1, \ldots \bar{\beta}_p)$$

f est un morphisme.

Soit $(\bar{\alpha}_1, \dots, \bar{\alpha}_p) \in (\mathbb{Z}/2\mathbb{Z})^p$ tq

$f(\bar{\alpha}_1, \dots, \bar{\alpha}_p) = e$.

$\Rightarrow x_1^{\alpha_1} \dots x_i^{\alpha_i} \dots x_p^{\alpha_p} = e$.

l'elt neutre de $(\mathbb{Z}/p\mathbb{Z})^p$ est $(\bar{0}, \dots, \bar{0})$

Par l'absurde $\exists i \in [1, p]$ $\bar{\alpha}_i \neq \bar{0}$

$\bar{\alpha}_i = \bar{1}$

$x_i^{\alpha_i} x_1^{\alpha_1} \dots x_{i-1}^{\alpha_{i-1}} x_{i+1}^{\alpha_{i+1}} \dots x_p^{\alpha_p} = e$.

$x_i x_i^{-1} x_1^{\alpha_1} \dots x_{i-1}^{\alpha_{i-1}} x_{i+1}^{\alpha_{i+1}} \dots x_p^{\alpha_p} = e \cdot x_i$

e

$x_i = x_1^{\alpha_1} \dots x_{i-1}^{\alpha_{i-1}} x_{i+1}^{\alpha_{i+1}} \dots x_p^{\alpha_p} x_i$

$x_i \in \langle x_1, x_{i-1}, x_{i+1}, \dots x_p \rangle$

$\langle x_1 \dots x_i \dots x_p \rangle \subset \langle x_1 \dots x_{i-1}, x_{i+1} \dots x_p \rangle$

sg de G

G.

$G = \langle x_1 \dots x_{i-1}, x_{i+1}, \dots x_p \rangle$

D'où $(x_1, \dots, x_p)$ y $\not\in x_i$ est une famille génératrice de G.

Ce qui est absurde $\alpha_i = 0$

D'où f est injectif

f est surjective D'après la construction de f.

$\forall x \in G \quad x = x_1^{k_1} \dots x_p^{k_p} \quad k_1 \dots k_p \in \mathbb{Z}$

Est bijective

$|G| = |(\mathbb{Z}/2\mathbb{Z})^p| = 2^p$.