

Rappel "groupe"

Groupe usuels:

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

$(M_n(\mathbb{K}), +)$; $(\mathbb{K}[X], +)$ sont

des groupes abéliens.

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

$(GL_n(\mathbb{K}), \cdot)$; $(\mathbb{K}(X)/\mathbb{K}[X], \cdot)$

$(\mathcal{L}(E), +)$, groupe abélien

$(GL(E), \cdot)$ groupe.

H s.g.d. G .

$H \subset G$.

$e \in H$ ($H \neq \emptyset$)

$\forall x, y \in H$; $xy^{-1} \in H$ (si la loi " $\cdot$ ")

$x - y$ (si la loi " $+$ ")

Ex:

$(O_n(\mathbb{R}), \cdot)$ est un s.g.d. $(GL_n(\mathbb{R}), \cdot)$.

$S_n(\mathbb{R})$ est un s.g.d. $(M_n(\mathbb{R}), +)$

Les sous-groupes d. $\mathbb{Z}$ sont.

les $n\mathbb{Z}$ avec $n \in \mathbb{N}$.

→ si H et K deux s.g.d. G , alors

$H \cap K$ s.g.d. G .

$H \cup K$ s.g.d. $G \Leftrightarrow H \subset K$ et $K \subset H$.

→ Soit $A \subset G$.

$\langle A \rangle = \bigcap_{\substack{H \text{ s.g. } G \\ A \subset H}} H = \text{le plus petit sous groupe contenant } A$

$$= \{x = a_1 \dots a_n \text{ avec } a_i \in A, a_i^{-1} \in A\}$$

→ $a \in G$

$$\langle a \rangle = \{a^n, n \in \mathbb{Z}\} \text{ ou } \langle a \rangle = \{n a, n \in \mathbb{Z}\}$$

→ Si $H \text{ s.g. } G$ et $a \in H$.

Donc $\langle a \rangle \subset H$.

Exp. $\langle i \rangle = \{1, -1, i, -i\}$

$$\langle e^{2\pi i/n} \rangle = \{z \in \mathbb{C} \mid z^n = 1\}$$

$$\mathbb{Z}/n\mathbb{Z} = ??$$

Dans $\mathbb{Z}$: $x \equiv y(n)$

$\equiv(n)$ est une relation d'équivalence.

$$\bar{x} = \mathcal{C}(x) = \{y \in \mathbb{Z} \mid y \equiv x(n)\}$$

$\mathbb{Z}/n\mathbb{Z}$ = l'ensemble des classes d'équivalence.

on définit.

$$\bar{x} \oplus \bar{y} = \overline{x+y}$$

$$\bar{x} \otimes \bar{y} = \overline{xy}$$

Soit $k \in \mathbb{Z}/n\mathbb{Z}$:

$$k = \overline{1 + k_1 + \dots + k_{n-1}} = \overline{1 + k_1 + \dots + k_{n-1}}$$

$$\boxed{\bar{k} = k \cdot \bar{1}} \text{ où } \bar{1} \text{ est l'élément neutre}$$

$(\mathbb{Z}/n\mathbb{Z}, +)$ est un groupe abélien.

$$\mathbb{Z}/n\mathbb{Z} = \{\overline{0}, \overline{1}, \dots, \overline{n-1}\}$$

$$\overline{n} = \overline{0} \Rightarrow k \cdot n = \overline{0}.$$

$$\mathbb{Z}/n\mathbb{Z} = \langle \overline{1} \rangle = \langle \overline{k} \rangle \text{ avec } k \cdot n = 1.$$

Exemple

$$\text{on a. } \overline{k} \in \mathbb{Z}/n\mathbb{Z} \Rightarrow \langle \overline{k} \rangle \subset \mathbb{Z}/n\mathbb{Z}$$

$$\text{Soit } \overline{p} \in \mathbb{Z}/n\mathbb{Z}$$

$$\text{on a. } k \cdot n = 1 \Rightarrow \exists u, v \in \mathbb{Z} \text{ tel.}$$

$$1 = uk + nv \Rightarrow p = uk + np$$

$$\Rightarrow \overline{p} = \overline{uk + np}$$

$$= \overline{uk} + \overline{np}$$

$$\Rightarrow \mathbb{Z}/n\mathbb{Z} = \langle \overline{k} \rangle.$$

$$\text{Exemple } \mathbb{Z}/4\mathbb{Z} = \{\overline{0}, \overline{1}, \overline{2}, \overline{3}\}.$$

$$= \langle \overline{3} \rangle.$$

$$\overline{0} = 0 \cdot \overline{3}$$

$$\overline{1} = 3 \cdot \overline{3} = \overline{9}$$

$$\overline{2} = 2 \cdot \overline{3} = \overline{6}$$

$$\overline{3} = 1 \cdot \overline{3}.$$

Def. $\forall x, y \in G$.
 $f(x \cdot y) = f(x) * f(y)$

$\cdot f(e_G) = e_{G'}$
 $\cdot f(x^{-1}) = (f(x))^{-1}$
 $\cdot \forall n \in \mathbb{Z}, f(x^n) = (f(x))^n$

$\cdot f \text{ injective} \Leftrightarrow \ker f = \{e_G\}$
 $\cdot f \text{ surj} \Leftrightarrow f(G) = G'$
 $\cdot f \text{ bij} \Leftrightarrow f \text{ inj} \text{ et } f \text{ surj}$

Exp:

$\cdot \text{Exp}: (R, +) \rightarrow (R^*, \cdot)$
 $x \mapsto e^x$

$\cdot L_n: (R^*, \cdot) \rightarrow (R, +)$
 $x \mapsto L_n x$

$\cdot \det: (GL_n(R), \cdot) \rightarrow (R^*, \cdot)$
 $A \mapsto \det A$

sont des morphismes de groupes

$\cdot \det(K) = \{ A \in GL_n(K) \mid \det A = 1 \}$
 $= \ker(\det)$
 $= 1.g \in GL_n(K)$

$f: (G, \cdot) \rightarrow (G', *)$
 f est un morphisme de groupes

$\cdot \text{si } H, 1.g \in G \Rightarrow f(H), 1.g \in G'$
 $\cdot \text{si } K, 1.g \in G' \Rightarrow f^{-1}(K) = 1.g \in G$

$\cdot \text{si } \text{card } G = \text{card } G' < \infty$
 $f \text{ bij} \Leftrightarrow f \text{ inj} \Leftrightarrow f \text{ surj}$

$\forall a \in G$
 $f(\langle a \rangle) = \langle f(a) \rangle$

$\cdot \ker f = \{ x \in G \mid f(x) = e_{G'} \}$
 $= f^{-1}(\{e_{G'}\})$
 $= 1.g \in G$
 $\Rightarrow \text{Im } f = f(G) = 1.g \in G'$

$$\text{19. } f(\langle a \rangle) = \langle f(a) \rangle$$

$$\text{ma. } a \in \langle a \rangle \Rightarrow f(a) \in f(\langle a \rangle)$$

$$\langle a \rangle \text{ s.g. } G \Rightarrow f(\langle a \rangle) \text{ s.g. } G'$$

$$\Rightarrow \langle f(a) \rangle \subset f(\langle a \rangle)$$

$$\text{"} \supset \text{"}. \text{ Se } y \in f(\langle a \rangle) \Rightarrow \exists x \in \langle a \rangle$$

$$\text{ s.t. } y = f(x)$$

$$\exists n \in \mathbb{Z} \text{ s.t. } x = a^n \Rightarrow y = f(a^n)$$

$$= (f(a))^n$$

$$\Rightarrow y \in \langle f(a) \rangle \Rightarrow f(\langle a \rangle) \subset \langle f(a) \rangle$$

$$\text{Dici } \langle f(a) \rangle = f(\langle a \rangle)$$

$$a \in G, a \text{ divisibile. } \exists k \in \mathbb{N}^* \text{ s.t. } a^k = e.$$

$$o(a) = \min \{ p \in \mathbb{N}^* \mid a^p = e \}$$

ordine

$$\text{Se } n = o(a) \Rightarrow a^n = e$$

$$\forall k \in \{1, \dots, n-1\}, a^k \neq e$$

$$\langle a \rangle = \{e, a, \dots, a^{n-1}\}$$

$$a^p = e \Leftrightarrow \alpha(a) \mid p$$

$$\text{card}(\langle a \rangle) = n = \alpha(a)$$

$$\text{Se } k, k' \in \{0, \dots, n-1\}, \text{ sepp } a^k = a^{k'}$$

$$\Rightarrow a^{k-k'} = e \Rightarrow n \mid k-k'$$

$$\Rightarrow k-k' \leq n-1 \Rightarrow k-k' = 0 \Rightarrow k = k'$$

$$\Rightarrow k \neq k' \Rightarrow a^k \neq a^{k'}$$

$$\Rightarrow \text{card}(\langle a \rangle) = n = o(a)$$

Si $\text{Card } G = n < \infty$

Alors $\forall a \in G$, a est d'ordre fini

et $a^n = e \Rightarrow o(a) \mid n = \text{Card}(G)$

Exercice 2.

$$O_n(\mathbb{R}) = \{ A \in M_n(\mathbb{R}) \mid {}^t A A = I_n \}$$

Pq. $O_n(\mathbb{R})$ est un sous-groupe de $GL_n(\mathbb{R})$
Compact

Pq. $O_n(\mathbb{R})$ est un compact de $M_n(\mathbb{R})$.

$$\|A\| = \sqrt{\text{tr}({}^t A A)}$$

$$\forall A \in O_n(\mathbb{R}); \|A\| = \sqrt{\text{tr}(I_n)} = \sqrt{n}.$$

$\Rightarrow O_n(\mathbb{R})$ est borné par $\sqrt{n}$.

Pq. $O_n(\mathbb{R})$ est un fermé.

$$O_n(\mathbb{R}) = f^{-1}(\{I_n\})$$

$$\text{avec } f: M_n(\mathbb{R}) \rightarrow M_n(\mathbb{R}) \\ \pi \mapsto \pi \cdot \pi.$$

$$\text{sit } g: M_n(\mathbb{R}) \rightarrow M_n(\mathbb{R}) \times M_n(\mathbb{R}) \\ \pi \mapsto ({}^t \pi, \pi)$$

g est linéaire $\Rightarrow g$ continue.
 $\cdot$ $\text{dim } M_n(\mathbb{R}) < \infty$

$$\text{et } h: M_n(\mathbb{R}) \times M_n(\mathbb{R}) \rightarrow M_n(\mathbb{R}) \\ (A, B) \mapsto A \times B.$$

h est bilinéaire
 $\cdot$ $\text{dim } M_n(\mathbb{R}) < \infty \Rightarrow h$ est continue.

$\Rightarrow f = h \circ g$ est continue.

$\Rightarrow \{I_n\}$ est un fermé de $M_n(\mathbb{R})$
 $\Rightarrow O_n(\mathbb{R})$ est un fermé de $M_n(\mathbb{R})$

Exercice 4

$(G, \cdot)$ groupe cyclique.

$$G = \langle a \rangle, \text{ Card } G = n.$$

$$\Rightarrow o(a) = n$$

G est abélien.

$$1) f: (G, \cdot) \rightarrow (G, \cdot)$$

$$x \mapsto f(x) = x^n$$

$$\forall x, y \in G, f(xy) = (xy)^n$$

$$= x^n \cdot y^n \quad \text{abélien}$$

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

$\Rightarrow f$ morphisme de groupes.

$$2) \text{ Soit } d = \text{pgcd}(n, n)$$

$$n = h'd$$

$$n = h'd$$

$$\text{avec } h'r = 1.$$

$$14. \ker f = \langle a^{n'} \rangle.$$

$$\text{Soit } x \in \ker f \Rightarrow \begin{cases} f(x) = a^n x^n = e \\ x \in G \end{cases}$$

$$x \in G = \langle a \rangle \Rightarrow x = a^k, k \in \mathbb{Z}$$

$$\Rightarrow a^{kn} = e.$$

$$o(a) = n \Rightarrow n \mid kn$$

$$\Rightarrow d \mid n' / k \mid n' \Rightarrow n' \mid kn'$$

$$o(n' \wedge n') = 1 \Rightarrow n' \mid k$$

$$\Rightarrow k = n' k' \Rightarrow x = (a^{n'})^{k'}$$

$$\Rightarrow \ker f \subset \langle a^{n'} \rangle.$$

$$f(a^{n'}) = a^{n'n} = e$$

$$\Rightarrow a^{n'} \in \ker f \Rightarrow \langle a^{n'} \rangle \subset \ker f.$$

$$\text{Donc } \ker f = \langle a^{n'} \rangle.$$

b) πq . $\text{Im } f = \langle a^{\dagger} \rangle$

$$\text{ana. } d = \text{pgcd.}(n, r)$$

$$\Rightarrow \exists u, v \in \mathcal{U} \text{ s.t. } d = u \vee v$$

$$\Rightarrow a^d = a^{Un+Ur} = a^{Un} \cdot a^{Ur}$$

$$= (a^n)^u \cdot (a^v)^r = f(a^v)$$

$$\Rightarrow \langle ad \rangle \subset \text{Im } f$$

$$\Rightarrow \langle \text{ad} \rangle \subset \text{Imp.}$$

$\Rightarrow \exists h \in \mathcal{C}$ s.t. $x = ah$.

$$\Rightarrow \exists k \in \mathbb{Z} \text{ s.t. } x = a + k$$

$$\Rightarrow y = f(a^k) = a^{k \cdot n} = a^{k \cdot n'} \\ \Rightarrow \text{Imp}$$

$\Rightarrow \text{Inf } C \subseteq \text{rad}$
 $\text{Also } \text{Inf} = \text{rad}$

3) $y \in G$, combien d'eq. $x' = y$ admet
- elle la solution
 $y = f(x)$

$$y = f(x)$$

→ si $y \notin \text{Inf}$. par la relation

$$\rightarrow s_i y \in \text{Im } f \Rightarrow \exists x_0 \in G \text{ s.t. } f(x_0) = y$$

$$\Rightarrow x^r = x_0^r.$$

$$\Rightarrow x^n x_0^{-n} = e \Leftrightarrow (x x_0^{-1})^n = e$$

$$\Rightarrow f(xx^{-1}) = e \Rightarrow xx^{-1} \in \ker f.$$

$$\Rightarrow \text{Con}(\{x \in G \text{ s.t. } f(x) = y\}) = \text{Con}(\ker f) = \text{Con}(\ker \varphi)$$

$$\text{card}(\langle a^{n'} \rangle) = o(a^{n'})$$

$$\text{Pq } o(a^{n'}) = d.$$

$$\text{sit } p = o(a^{n'}).$$

$$\text{oua. } (a^{n'})^d = a^n = e.$$

$$\Rightarrow o(a^{n'}) = \underline{p \cdot d}.$$

Don't repeat oua.

$$(a^{n'})^p = e. \Rightarrow n/n'p.$$

$$\Rightarrow n'd/n'p \Rightarrow \underline{d/p}.$$

$$\Rightarrow o(a^{n'}) = d.$$

$$\Rightarrow \text{card}\{x \in G \mid f(x) = y\} = d.$$