

I DÉFINITIONS ET PREMIÈRES PROPRIÉTÉS

1 Classes

Tout au long de cette leçon : $(G, \cdot)$ est un groupe et $H \leq G$ un de ses sous-groupes.

Def 1: Classe à gauche de $a \in G$ relativement à H
 $aH = \{ah \mid h \in H\}$.
 (de même Ha est la classe à droite)

On note G/H l'ensemble des classes à gauche relativement à H .

Def 2: Indice de H dans G : $(G:H) := \# G/H$.

Thm 3: Lagrange

Si G est fini, alors $\#G = \#H \cdot (G:H)$. ([CAL], p.75).

App 4: Si G est fini, $\forall x \in G$, l'ordre de x divise $\#G$.

2 Sous-groupes distingués

Def 5: Automorphisme intérieur

$\mathcal{I}_G : G \rightarrow G$, où $g \in G$ est un automorphisme intérieur.
 $\mathcal{I}_g : h \mapsto ghg^{-1}$

$\text{Int}(G) = \{\mathcal{I}_g \mid g \in G\}$ est le groupe des automorphismes intérieurs.

Def 6: Sous-groupes distingués.

H est distingué dans $G \Leftrightarrow \forall g \in G, \mathcal{I}_g(H) = H$

On note alors $H \triangleleft G$.

Ex 7: $\{e\} \triangleleft G, G \triangleleft G$.

• Si G est abélien, tout sous-groupe est distingué.

↳ la réciproque est fautive : considérer Q_8 , les quaternions.

• $\mathbb{Z} \triangleleft (\mathbb{R}, +)$ mais pour $n \geq 2, G_n(\mathbb{Z}) \not\triangleleft G_n(\mathbb{R})$ ([OAL], p.234)

Prop 8: Tout sous-groupe d'indice 2 est distingué. ([CAL], p.113)

Ex 9: $\mathcal{O}_n \triangleleft \mathcal{S}_n$

• $\langle \tau \rangle \triangleleft \mathcal{D}_n$, où τ la rotation d'angle $\frac{2\pi}{n}$.

Thm 10: Théorème de Frobenius ([FG], p.7)ⁿ

Soit G un groupe fini, p le plus petit diviseur premier de $\#G$.

Les sous-groupes de G d'indice p sont distingués dans G .

App 11: Si $\#G = p^3$, p premier, alors $\#H = p^2 \Rightarrow H \triangleleft G$.

3 Groupes quotients

Def 12:

Si $H \triangleleft G$, on peut munir G/H d'une structure de groupe par l'opération $(aH)(bH) = (ab)H$. On appelle G/H le groupe quotient.

De plus $\pi : G \rightarrow G/H$ est un morphisme de groupes surjectif. ([PER], p.11)

Ex 13: $\mathbb{Z} \triangleleft \mathbb{R}$, donc $\mathbb{R}/\mathbb{Z}$ est un groupe (le cercle)

Prop 14: $H \triangleleft G \Leftrightarrow H$ est le noyau d'un morphisme de groupes $f: G \rightarrow G'$.

Ex 15: $S_n(K) \triangleleft G_n(K)$ car $S_n(K) = \text{Ker}(\det)$.

Prop 16: Correspondance des sous-groupes.

Si $H \triangleleft G, \{K \leq G \mid K \geq H\} \longleftrightarrow \{\text{sous-groupes de } G/H\}$ ([CAL], p.150-152)

$$\begin{array}{ccc} K & \xrightarrow{\alpha} & \pi(K) \\ \pi^{-1}(\pi) \leftarrow \beta & & 1 \end{array}$$

Et α, β sont des bijections réciproques qui conservent le caractère distingué, les inclusions et les intersections.

Ex 17: Les sous-groupes de $\mathbb{Z}/n\mathbb{Z}$ sont les $k\mathbb{Z}/n\mathbb{Z} \simeq \mathbb{Z}/\frac{n}{k}\mathbb{Z}$ où $k \mid n$.

II THÉORÈMES D'ISOMORPHISME

Thm 18: Propriété universelle du quotient ([JUM], p.60)

Soit Γ un groupe, on suppose $H \triangleleft G$. Soit $\varphi: G \rightarrow \Gamma$ un morphisme de groupes tel que $H \subseteq \text{Ker } \varphi$.

Alors il existe un unique morphisme de groupes $\bar{\varphi}: G/H \rightarrow \Gamma$ tel que $\varphi = \bar{\varphi} \circ \pi$.

$$\begin{array}{ccc} G & \xrightarrow{\varphi} & \Gamma \\ \pi \downarrow & & \uparrow \bar{\varphi} \\ G/H & \xrightarrow{\bar{\varphi}} & \Gamma \end{array}$$

Cor 19: 1^{er} théorème d'isomorphisme ([JUM], p.63)

Avec les mêmes notations : $G/\text{Ker } \varphi \simeq \text{Im } \varphi$, via $\bar{\varphi}$.

App 20: Si G est cyclique fini, alors $G \simeq \mathbb{Z}/\#G\mathbb{Z}$. ([JUM], p.64)

• $\det$ fournit l'isomorphisme $G_n(K)/G_n(K) \simeq K^\times$.

Def 21: Normalisateur

$N_G(H)$ est le plus grand sous-groupe de G dans lequel H est distingué.

Ex 22: Si $H \triangleleft G, N_G(H) = G$.

• $N_{\mathcal{D}_3}(\langle s \rangle) = \langle s \rangle$

• $N_{\mathcal{D}_4}(\langle s \rangle) = \langle s, r^2 \rangle$.

Thm 23: 2^e théorème d'isomorphisme (JUM, p. 78)

Soit $K < G$ tel que $K \subseteq N_G(H)$.
Alors les groupes quotients KH/H et $K/K \cap H$ existent et sont isomorphes.

Ex 24: $G_2/N_2 \cong (G_2/N_2)/N_2 \cong G_2$ (JUM, p. 79).

Thm 25: 3^e théorème d'isomorphisme

Soit $K \triangleleft G$ tel que $K \subseteq H$, on suppose $H \triangleleft G$. (JUM, p. 64)

On a: $(G/K)/(H/K) \cong G/H$.

Ex 26: $G_2/N_2 \cong (G_2/N_2)/(N_2/N_2) \cong G_2$ (JUM, p. 65)

III GROUPE ET SOUS-GROUPE REMARQUABLES

1 Sous-groupes caractéristiques.

a. Définition et propriétés générales.

Def 27: H est caractéristique dans $G \Leftrightarrow \forall \alpha \in \text{Aut}(G), \alpha(H) \subseteq H$.

On notera alors $H \text{ car } G$.

Prop 28: $H \text{ car } G \Rightarrow H \triangleleft G$.

Prop 29: Soit $K \subseteq H$, $K < G$.

• $K \text{ car } H \text{ car } G \Rightarrow K \text{ car } G$ (JUM, p. 35)

• $K \text{ car } H \triangleleft G \Rightarrow K \triangleleft G$

Ex 30: $\langle (12)(34) \rangle \triangleleft V_4 \triangleleft G_4$ mais $\langle (12)(34) \rangle \not\triangleleft G_4$.

b. Centre (PER, p. 12)

Def 31: $Z(G) = \{a \in G \mid \forall g \in G, ag = ga\}$. On a: $Z(G) \text{ car } G$.

Ex 32: • G abélien $\Leftrightarrow Z(G) = G$

• Si $\#G = p^1$ (avec p premier, $n \in \mathbb{N}^*$), alors $Z(G) \neq \{e\}$. (FER, p. 5)

• $Z(G_n) = \{Id\}$ pour $n \geq 3$.

Prop 33: $\text{Int}(G) \cong G/Z(G)$.

c. Groupe dérivé. (PER, p. 13)

Def 34: On note $[x, y] = xyx^{-1}y^{-1}$ le commutateur de x et y .

On a: $\partial(G) = \langle [x, y] \mid x, y \in G \rangle$ est caractéristique dans G .

Prop 35: G abélien $\Leftrightarrow \partial(G) = \{e\}$

Ex 36: Pour $n \geq 2$, $\partial(S_n) = A_n$. (FER, p. 28)

• $\partial(GL_n(K)) = SL_n(K)$ sauf si $n=2$ et $K = \mathbb{F}_2$. (FER, p. 101)

Prop 37: Caractérisation

$\partial(G)$ est le plus petit sous-groupe distingué de G tel que $G/\partial(G)$ abélien.

App 38: Tout morphisme de G vers un groupe abélien se factorise par $\partial(G)$.

Thm 39: Frobenius-Zsigmondy (FOA, p. 251)

Soit p premier impair, $n \geq 2$.

Alors $\forall u \in GL_n(\mathbb{F}_p)$, $\epsilon(u) = \left(\frac{\det(u)}{p}\right)$

2. Produit direct

Def 40: Soient G et H deux groupes, l'ensemble $G \times H = \{(g, h) \mid g \in G, h \in H\}$ peut être muni d'une structure de groupe via $(g, h)(g', h') = (gg', hh')$.

Ex 41: $V_4 \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

• Si m et n sont premiers entre eux: $\mathbb{Z}/mn\mathbb{Z} \cong \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$.

Prop 42: Si H et K sont tels que: $H \cap K = \{e\}$, $H \in N_G(K)$, $K \in N_G(H)$ et $\#H \cdot \#K = \#G$, (JUM, p. 77)

Alors $G \cong H \times K$.

Thm 43: Structure des groupes abéliens finis

Soit G un groupe abélien fini d'ordre $n \geq 2$.

Il existe $q_1 \dots q_r$ entières déterminées par $G \cong \mathbb{Z}/q_1\mathbb{Z} \times \dots \times \mathbb{Z}/q_r\mathbb{Z}$.

Ex 44: Un groupe abélien d'ordre 18 est $\cong \mathbb{Z}/18\mathbb{Z}$ ou $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$.

3. Groupes simples (PER, p. 12)

Def 45: On suppose $G \neq \{e\}$. G est simple $\Leftrightarrow (H \triangleleft G \Rightarrow H = \{e\} \text{ ou } H = G)$.

Ex 46: Pour $n \geq 5$, A_n est simple (FER, p. 24 + JUM, p. 73) ← DÉVELOPPEMENT N°2

• $SO_3(\mathbb{R})$ est simple (FER, p. 148)

• Pour $n \geq 5$, $PSL_n(\mathbb{R})$ est simple. (FER, p. 150)

• Si p et q premiers distincts, $\#G = pq \Rightarrow G$ n'est pas simple.

App 47: Soit $f: G \rightarrow I$ un morphisme de groupes. Si G est simple, alors f est injectif ou trivial. (JUM, p. 133)

Prop 48: Les sous-groupes simples abéliens sont les $\mathbb{Z}/p\mathbb{Z}$ où p est premier.

4. Théorèmes de Sylow (PER, p. 18)

Dans cette section, $\#G = p^a m$, avec p premier et $p \nmid m$.

Def 49: On appelle p -Sylow de G un sous-groupe de cardinal p^a .

Ex 50: $\#GL_n(\mathbb{F}_p) = (p^n - 1)(p^n - p) \dots (p^n - p^{n-1}) = m p^{n(n-1)/2}$
→ Les matrices triangulaires supérieures unitaires forment un p -Sylow.

DÉVELOPPEMENT N°1.

Thm 54: Théorèmes de Sylow.

- 1) G contient au moins un p -Sylow.
- 2) Si H est un sous-groupe de G d'ordre une puissance de p ,
Alors il existe un p -Sylow S contenant H .
- 3) Les p -Sylow sont tous conjugués.
- 4) On note n_p le nombre de p -Sylow; on a: $n_p \equiv 1[p]$ et $n_p | m$.

Cor 52: Si S est un p -Sylow de G , on a: $S \triangleleft G \Leftrightarrow n_p = 1$.

App 53: • Un groupe d'ordre 15 est cyclique (FS, p26)

- Si $\#G \leq 55$ et si G est simple, alors G est cyclique d'ordre premier