Cadre : G désigne un groupe, $\mathbb{K}$ est un corps commutatif, $q = p^r$, $r \in \mathbb{N}^*$, p premier, $\mathbb{F}_q$ est le corps à q éléments.

I - Conjugaison dans un groupe

1 - Action par conjugaison

Def 1 : Soient G, $\tilde{G}$ deux groupes. On dit que G agit sur $\tilde{G}$ par conjugaison $(G \curvearrowright \tilde{G})$ s'il existe un morphisme

$$\rho : G \longrightarrow S_{\tilde{G}}$$
$$g \longmapsto [h \mapsto g h g^{-1}]$$

Prop 2 : $\forall g \in G$, $\rho(g)$ est un automorphisme de $\tilde{G}$.

Def 3 : On dit que $\rho(g)$ est un automorphisme intérieur de G. On note $\rho(g) = \text{int}_g$.

Prop 4 : On note $\text{Int}(G)$ l'ensemble des automorphismes intérieurs de G. $(\text{Int}(G), \circ)$ est un groupe.

Def 5 : On appelle classe de conjugaison de $g \in G$ l'ensemble $G_g = \text{Orb}_g(G) = \{hgh^{-1}, h \in G\}$.
On appelle stabilisateur (ou normalisateur) de $g \in G$ l'ensemble
$\text{Stab}_G(g) = \{h \in G : hgh^{-1} = g\}$

Prop 7 : $\forall g \in G$, $\text{Stab}_g(G) \leqslant G$

Prop 8 : $\forall g \in G$, $\forall h \in G$, $\text{Stab}_{hgh^{-1}}(G) = g\,\text{Stab}_h(G)\,g^{-1}$

Prop 9 : Si $|G| < +\infty$ alors $|G| = |G_g| \cdot |\text{Stab}_g(G)|$

Th 10 (Formule des classes)

$$|G| = |G^G| + \sum_{i=1}^{n} \frac{|G|}{|G_{g_i}|}$$

où $g_1, \dots, g_n$ est un système de représentants des orbites non triviales (non réduites à un élément), $G^G = \{g \in G : \forall h \in G, hgh^{-1} = g\}$

2 - Sous-groupes remarquables

Def 11 : On définit le centre de G par $Z(G) = \{g \in G : \forall h \in G, gh = hg\}$
G est dit abélien (commutatif) lorsque $Z(G) = G$

Rq 12 : L'équation aux classes se reformule avec $|G| = |Z(G)| + \sum_{i=1}^{r} \frac{|G|}{|G_{g_i}|}$

Def 13 : Soient $x, y \in G$. On appelle commutateur de x et y l'élément $[x, y] = xyx^{-1}y^{-1} \in G$.

Def 14 : On appelle groupe dérivé de G le groupe noté $D(G)$ défini par :
$$D(G) = \langle [x, y],\ x, y \in G \rangle$$

Ex 15 : $D(GL_2(\mathbb{R})) = SL_2(\mathbb{R})$

Def 16 : Soit $H \leqslant G$. On dit que H est normal (ou distingué) dans G si et seulement si $\forall g \in G$, $\forall h \in H$, $ghg^{-1} \in H$ (i.e. H est stable par tout automorphisme intérieur de G, i.e. $\forall g \in G$, $gH = Hg$). On note alors $H \triangleleft G$.

Prop 17 : $D(G)$, $Z(G) \triangleleft G$. Si $\varphi : G \to G'$ est un morphisme, $\ker(\varphi) \triangleleft G$, $\text{Im}(\varphi) \triangleleft G'$

Rq 18 : Si G est abélien, alors tous les sous-groupes de G sont distingués.

Rq 19 : $H \triangleleft G$ et $K \triangleleft H$ n'implique pas forcément $K \triangleleft G$

Ex 20 : $G = S_4$, $H = V_4 = \{Id, (12)(34), (13)(24), (14)(23)\} \leqslant G$
$K = \{Id, (12)(34)\} \leqslant H$ $\quad K \triangleleft V_4$, $V_4 \triangleleft S_4$ mais $K \ntriangleleft S_4$
En effet, $(123)(12)(34)(123)^{-1} = (23)(14) \notin K$

Def 21 : G est dit simple lorsque $H \triangleleft G \Rightarrow H = G$ ou $H = \{1_G\}$

Ex 22 : $A_3 = \{Id, (123), (132)\}$ est simple.

3 - Application à l'étude de groupes classiques

Prop 23 : $\forall n \geqslant 5$, $D(A_n) = A_n$ et $\forall n \geqslant 2$, $D(S_n) = A_n$
$D(A_4) = V_4$

Def 24 : On dit que $\sigma \in S_n$ est du type $[k_1, \dots, k_n]$ si elle admet dans sa décomposition en produit de cycles k_i cycles à supports disjoints de longueur i.

Ex 25 : Dans S_6, $\sigma = (12)(456)$, type : $[0, 1, 1, 0, 0, 0]$

Prop 26 : Les classes de conjugaison de S_n contiennent exactement les éléments du même type. Le nombre d'éléments d'une classe de conjugaison contenant les éléments du type $[k_1, \dots, k_n]$ est $\dfrac{n!}{\prod_{i=1}^{n} k_i!\, i^{k_i}}$

Th 27 : $\forall n \geqslant 5$, A_n est simple.

Prop 28 : (i) $Z(GL_n(\mathbb{K})) = \{\lambda I_n, \lambda \in \mathbb{K}^*\}$ (ii) $Z(SL_n(\mathbb{K})) = \{\lambda I_n, \lambda^n = 1\}$
(iii) Si $(n, \mathbb{K}) \neq (2, \mathbb{F}_2)$, $D(GL_n(\mathbb{K})) = SL_n(\mathbb{K})$
(iv) Si $(n, \mathbb{K}) \neq (2, \mathbb{F}_2), (2, \mathbb{F}_3)$, $D(SL_n(\mathbb{K})) = SL_n(\mathbb{K})$

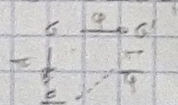
Rem 30 On peut faire agir $GL_n(\mathbb{K})$ sur $\mathcal{M}_n(\mathbb{K})$ par conjugaison.
Def 30 bis Les classes de conjugaison sont alors appelées classes de similitude.
Rem 30 bis La trace, le déterminant, le polynôme caractéristique [illegible] [illegible] ne sont pas des invariants de similitude. On sait que ce sont des invariants de similitude.

Th 31 (Comptage de matrices diagonalisables de $\mathcal{M}_n(\mathbb{F}_q)$)
Soit $\mathcal{D}_n(\mathbb{F}_q)$ l'ensemble des matrices diagonalisables de $\mathcal{M}_n(\mathbb{F}_q)$. Alors [illegible] la relation [illegible], on a : $|\mathcal{D}_n(\mathbb{F}_q)| = \sum_{\substack{n_1+\dots+n_q = n}} \frac{|GL_n(\mathbb{F}_q)|}{\prod_{i=1}^{q} |GL_{n_i}(\mathbb{F}_q)|}$ DVPT 1

II - Groupe quotient

1 - Définitions et propriétés élémentaires

Def 32 On définit le quotient $\frac{G}{H}$ comme l'ensemble des classes d'équivalence pour cette relation d'équivalence : $x \sim y \iff xy^{-1} \in H$
Prop 32 bis Si $H \lhd G$, $\frac{G}{H}$ est muni d'une structure de groupe et de cette loi de groupe $(g_1H) \times (g_2H) = (g_1g_2)H$
Prop 33 La projection $\pi : G \longrightarrow \frac{G}{H}$, $g \longmapsto gH$ est un morphisme de groupe surjectif tel que $H = \mathrm{Ker}(\pi)$
Cor 34 $\frac{G}{H}$ est muni d'une structure de groupe ssi $H \lhd G$
Def 35 Si $H \leq G$, on appelle indice de H dans G le nombre noté $[G:H]$ de $\left|\frac{G}{H}\right|$
Prop 36 Si G est un groupe fini, et $H \leq G$ alors $\left|\frac{G}{H}\right| = \frac{|G|}{|H|}$
Rem 37 Même si $H \ntrianglelefteq G$ on a toujours $|H| \mid |G|$ si $H \leq G$: il s'agit du théorème de Lagrange.
Prop 38 Si $H \leq G$, et $[G:H] = 2$ alors $H \lhd G$
Th 39 Soit G, G' deux groupes, soit $\varphi : G \longrightarrow G'$ un morphisme tel que $H \subset \ker(\varphi)$ alors il existe un unique morphisme $\bar{\varphi} : \frac{G}{H} \longrightarrow G'$ tel que $\varphi = \bar{\varphi} \circ \pi$ où $\pi : G \longrightarrow \frac{G}{H}$ est la projection du quotient



Coro 40 Avec les mêmes notations, si $\varphi : G \longrightarrow G'$ est surjectif, alors $\bar{\pi} : \frac{G}{\ker(\varphi)} \longrightarrow G'$ est un isomorphisme.
Ex 41 En considérant le morphisme $\varphi : \mathbb{R} \longrightarrow \mathbb{S}^1$, $x \longmapsto e^{2i\pi x}$, on peut montrer que $\mathbb{S}^1 \simeq \frac{\mathbb{R}}{\mathbb{Z}}$
Prop 42 Soit $N \lhd G$. Alors $\frac{G}{N}$ est abélien si et seulement si $D(G) \subset N$. En particulier, $\frac{G}{D(G)}$ est abélien.

2 - Exemples de groupes quotients

Prop 43 Si $n \in \mathbb{N}^*$, $\frac{\mathbb{Z}}{n\mathbb{Z}}$ est muni de cette loi de groupe. $[x+y]_n = [x]_n + [y]_n$
Th 44 (Lemme Chinois) Si $m, n \in \mathbb{N}^*$ avec $m \wedge n = 1$, alors le morphisme $\varphi : \frac{\mathbb{Z}}{mn\mathbb{Z}} \longrightarrow \frac{\mathbb{Z}}{m\mathbb{Z}} \times \frac{\mathbb{Z}}{n\mathbb{Z}}$, $[x]_{mn} \longmapsto ([x]_m, [x]_n)$ est un isomorphisme de groupes
Appli 45 Résolution d'un système de congruences. Le système de congruences
$$\begin{cases} x \equiv 2\ [5] \\ x \equiv 1\ [2] \end{cases}$$
admet pour solution $\{7 + 10k,\ k \in \mathbb{Z}\}$
Prop 46 Les sous-groupes de $\frac{\mathbb{Z}}{m\mathbb{Z}}$ sont les $\frac{r\mathbb{Z}}{n\mathbb{Z}}$ où $r \mid n$, et ils sont monogènes
Coro 47 $\frac{\mathbb{Z}}{p\mathbb{Z}}$ est simple si et seulement si p est premier
Th 48 (Structure des groupes abéliens de type fini)
Si G est abélien de type fini, alors $\exists r \in \mathbb{N}$, $\exists d_1 \mid \dots \mid d_s \in \mathbb{N}^*$ tels que : $G \simeq \mathbb{Z}^r \times \frac{\mathbb{Z}}{d_1\mathbb{Z}} \times \dots \times \frac{\mathbb{Z}}{d_s\mathbb{Z}}$

Def 49 On définit le groupe projectif linéaire par
(i) $PGL_n(\mathbb{K}) = \frac{GL_n(\mathbb{K})}{Z(GL_n(\mathbb{K}))} = \frac{GL_n(\mathbb{K})}{\{\lambda I_n,\ \lambda \in \mathbb{K}^*\}}$
(ii) $PSL_n(\mathbb{K}) = \frac{SL_n(\mathbb{K})}{Z(SL_n(\mathbb{K}))} = \frac{SL_n(\mathbb{K})}{\{\lambda I_n,\ \lambda^n = 1\}}$ (groupe projectif spécial linéaire)
Th 50 Si $(n, \mathbb{K}) \neq (2, \mathbb{F}_2), (2, \mathbb{F}_3)$, $PSL_n(\mathbb{K})$ est simple
Prop 50 bis On a ces isomorphismes :
$PSL_2(\mathbb{F}_2) \simeq S_3$, $PGL_2(\mathbb{F}_3) \simeq S_4$, $PSL_2(\mathbb{F}_3) \simeq A_4$

III - Aspects géométriques

1 - Le groupe orthogonal

Def 51 On définit le groupe orthogonal $O_n(\mathbb{R})$ par
$O_n(\mathbb{R}) = \{A \in \mathcal{M}_n(\mathbb{R}) : AA^T = I_n\}$
De plus, on définit $SO_n(\mathbb{R}) = \{A \in O_n(\mathbb{R}) : \det(A) = 1\}$

Prop 52 $SO_n(\mathbb{R}) \lhd O_n(\mathbb{R})$. En d'autres termes, toute conjugaison d'une rotation de $\mathbb{R}^n$ par une isométrie reste une rotation directe de $\mathbb{R}^n$

Prop 53 : i) $D(O_n(\mathbb{R})) = SO_n(\mathbb{R})$ si $n \geq 2$

ii) $D(SO_n(\mathbb{R})) = SO_n(\mathbb{R})$ si $n \geq 3$

Coro 54 : Si $n \in \mathbb{N}$, $\forall s \in O_n(\mathbb{R})$, $\exists s' \in SO_n(\mathbb{R})$: $s = s's''$

Prop 55 : i) $Z(O_n(\mathbb{R})) = \{-I_n, I_n\}$

ii) - Si n est impair, $Z(SO_n(\mathbb{R})) = \{I_n\}$

Si n est pair, $Z(SO_n(\mathbb{R})) = \{-I_n, I_n\}$

1 - Générateurs dans le plan et l'espace :

Prop 56 : $D(SO_2(\mathbb{R})) = \{I_2\}$ En particulier $SO_2(\mathbb{R}) \simeq \mathbb{S}^1 = \frac{\mathbb{R}}{\mathbb{Z}}$ est un groupe abélien.

$$\frac{\mathbb{R}}{\mathbb{Z}} \xrightarrow{\sim} SO_2(\mathbb{R})$$

$$\theta \longmapsto \begin{bmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{bmatrix}$$

Prop 57 : $O_2(\mathbb{R}) = \left\{ \begin{bmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{bmatrix}, \begin{bmatrix} \cos\theta & \sin\theta \\ \sin\theta & -\cos\theta \end{bmatrix} \right\}_{\theta \in [0, 2\pi[}$

Rotation — Symétrie

Prop 58 : Comme $D(O_n(\mathbb{R})) = SO_n(\mathbb{R})$ cela implique que deux retournements du plan sont toujours conjugués par une isométrie (retournement) du plan.

Def 59 : Soit $n \in \mathbb{N}^*$. On définit le groupe diédral d'ordre n comme le groupe des isométries du polygone régulier à n côtés. On le note D_n.

Prop 60 : On a $D_n = \langle r, s \rangle$ où r est la rotation d'angle $\frac{2\pi}{n}$ et s est une symétrie.

On a donc $r^{-1} = srs^{-1}$ et $D_n = \langle r, s \mid r^n = s^2 = Id, srs = r^{-1} \rangle$

Rmq 61 : Les sous-groupes de D_n sont $\frac{\mathbb{Z}}{n\mathbb{Z}}$ et $\langle s \rangle$ et $\frac{\mathbb{Z}}{2\mathbb{Z}} \simeq \langle s \rangle$

Cor 62 : On a $\langle s \rangle < D_n$

Prop 63 : $SO_3(\mathbb{R})$ préserve la sphère unité de $\mathbb{R}^3$ donc de l'ensemble des retournements dans $\mathbb{R}^3$.

Prop 64 : Comme $D(SO_3(\mathbb{R})) = SO_3(\mathbb{R})$, deux retournements de l'espace sont toujours conjugués entre eux par une autre rotation.

Def 65 : Une rotation de $\mathbb{R}^3$ est une rotation d'angle π : retournement à un axe.

Si u est un retournement, alors il existe $\mathcal{D}$ une droite de $\mathbb{R}^3$ telle que

$$Mat_{\mathcal{B}}(u) = \begin{bmatrix} -1 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$$

Prop 66 : Deux retournements $u_1, u_2 \in SO_3(\mathbb{R})$ sont distincts respectivement aux droites $\mathcal{D}_1$ et $\mathcal{D}_2$ sont conjugués entre eux par une rotation entre $\mathcal{D}_1$ et $\mathcal{D}_2$.

Th 67 : $SO_3(\mathbb{R})$ est simple

Bibliographie

Perrin Cours d'Algèbre

Nouvelles Histoires Mathématiques de Groupes et Géométrie

P. Caldero & J. Germoni