101 : Groupe opérant sur un ensemble. Exemples et applications.

Réfs : [Ulm] Ulmer, Théorie des groupes. [Perr] Perrin, Cours d'Algèbre.
[H2G2] Caldero, Germoni : Histoires hédonistes de groupes et géométrie.

Devts :
Théo 33 + Théo 34 (Sylow)
Prop 64 (isomorphisme exceptionnel)
Appli 69 (groupe du cube).

Cadre : On fixe G un groupe et $X \neq \emptyset$ un ensemble

I. Premières définitions et propriétés

1) Actions de groupes.

Commençons par noter que l'ensemble des bijections de X vers X, noté $\mathfrak{S}(X)$, est un groupe, isomorphe à $\mathfrak{S}_n$ si X est fini de cardinal n.

[Ulm] 27-29

Def 1 : On appelle action (à gauche) de G sur X tout morphisme de groupes $G \to \mathfrak{S}(X)$. La donnée d'un tel morphisme munit X d'une structure de 'G-ensemble'.

Prop 2 : La donnée d'une action de G sur X est équivalente à celle d'une application $G \times X \to X$, $(g,x) \mapsto g.x$ telle que

- $\forall x \in X,\ 1.x = x$ • $\forall g,g' \in G,\ x \in X,\ g.(g'.x) = (gg').x$.

On notera $G \curvearrowright X$ pour 'G agit sur X' en l'absence d'ambiguïté sur la nature de l'action.

Rq 3 : On peut de même définir une action à droite comme un morphisme $G^{op} \to \mathfrak{S}(X)$.

Def 4 : Soit $G \curvearrowright X$ et $x \in X$. On pose

- $O_G(x) = \{g.x \mid g \in G\}$ l'orbite de x sous l'action de G
- $G_x = \{g \in G \mid g.x = x\}$ le stabilisateur de x.
- $X_g = \{x \in X \mid g.x = x\}$ le fixateur de g.

On dit que $Y \subseteq X$ est une partie stable sous l'action de G si $g(Y) \subseteq Y$ pour tout $g \in G$. On dit que x est un point fixe sous l'action si $G_x = G$.
On dit que l'action de G sur X est

- Fidèle si le morphisme $G \to \mathfrak{S}(X)$ est injectif
- Transitive si elle admet une unique orbite.
- Libre si tous les stabilisateurs sont triviaux.

[Ulm] 38 39

Rq 5 : Toute action de G sur X induit une action sur $\prod_{i \in I} X$ pour I un ensemble donnée par $g.(x_i)_{i \in I} = (g.x_i)_{i \in I}$.

Def 6 : On dit qu'une action de G sur X est k-transitive si l'action induite sur l'ensemble $\{(x_1, \dots, x_k) \mid x_i \in X,\ x_i \neq x_j \text{ si } i \neq j\}$ est transitive.

[Perr] 16

Ex 7 : L'action de $\mathfrak{S}_n$ sur $[\![1,n]\!]$ est n-transitive, celle de $\mathfrak{A}_n$ est $n-2$-transitive.

[Ulm] 30 31

Prop 8 : Le noyau du morphisme $G \to \mathfrak{S}(X)$ est l'intersection de tous les stabilisateurs

Cor 9 : Toute action libre est fidèle.

[Perr] 14-15

Prop 10 Soit $G \curvearrowright X$, les orbites de X sous l'action de G forment une partition de X. On note X/G l'ensemble des orbites.

Exemple 11 : Décomposition des permutations en produit de cycles à support disjoints.

Prop 12 : Pour $G \curvearrowright X$ et $x \in X$, l'application $G/G_x \to O_G(x)$ définie par $\bar{g} \mapsto g.x$ est bien définie et est une bijection.

2) Action d'un groupe fini sur un ensemble fini.

On fixe $|G| = m < \infty$ et $|X| = n < \infty$ et une action de G sur X pour cette partie.

[Ulm] 68-70

Prop 13 : Pour $x \in X$, on a $[G : G_x] = |O_G(x)|$.

Théo 14 : (Formule des orbites). Si $X = \bigsqcup_{i=1}^{r} O_G(x_i)$ est la partition de X en ses orbites sous l'action de G, on a

$$|X| = \sum_{i=1}^{r} |O_G(x_i)| = \sum_{i=1}^{r} [G : G_{x_i}]$$

Théo 15 (Formule de Burnside). Le cardinal de l'ensemble $|X/G|$ est donné par la formule $\frac{1}{|G|} \sum_{g \in G} |X_g|$

Prop 16 : Si $|G| = p^k$ est une puissance de nombre premier (on dit que G est un p-groupe). Alors, si X^G désigne l'ensemble des points fixes sous l'action de G, on a $|X^G| \equiv |X|\ [p]$.

Théo 17 (Cauchy) Tout p-groupe admet un élément d'ordre p.

Prop 18 : Le centre d'un p-groupe est non trivial.

Appli 19 : Structure des groupes d'ordre p^2 pour p premier.

II. Action d'un groupe sur lui même ou d'autres groupes.

1) Action par translation.

[Ulm] 31.

L'application $g.g' := gg'$ munit toujours G d'une structure de G-ensemble. On appelle cette action l'action par translation. Cette action est fidèle (même libre) et transitive. Si $|G| = n$ est fini, on obtient

Théo 20 (Cayley) Tout groupe G d'ordre n fini s'injecte dans le groupe symétrique $\mathfrak{S}_n$.

[Ulm] 31-32

Prop 21 : Soit G un groupe et $H \leq G$ un sous-groupe. Le groupe G agit sur G/H par translation, cette action est transitive, et $[G:H] = \frac{|G|}{|H|}$.

Ex 22 : Considérons H le sous-groupe engendré par $\begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$ dans $GL_2(\mathbb{F}_2) =: G$. L'action de G sur G/H donne un morphisme $G \to \mathfrak{S}_3$ qui est en fait un isomorphisme.

2) Action par conjugaison.

[Ulm] 33-35

Def 23 : Soit $g \in G$, on définit l'automorphisme intérieur γ_g de g par $\gamma_g(h) = ghg^{-1}$. On remarque que l'application $g \mapsto \gamma_g$ est un morphisme de G dans $\mathrm{Aut}(G) \subseteq \mathfrak{S}(G)$. On note $\mathrm{Int}(G)$ son image, et on appelle action par conjugaison de G sur lui-même l'action induite par ce morphisme.

Def 24 : Les orbites sous l'action par conjugaison sont les classes de conjugaison, et les stabilisateurs sont les centralisateurs.

Prop 25 : Si $G \neq \{1\}$, l'action par conjugaison n'est ni transitive, ni libre car $C_G(e) = \{1\}$.

Rq 26 : Le centre de G est l'ensemble des points fixes sous la conjugaison.

Prop-def 27 : Le conjugué d'un sous-groupe étant un sous-groupe, le groupe G agit par conjugaison sur l'ensemble de ses sous-groupes. Les points fixes sous cette action sont exactement les sous-groupes normaux.

[Perr] 15-16

Ex 28 : Les classes de conjugaison de $\mathfrak{S}_n$ sont données par les types dans la décomposition en produit de cycles à supports disjoints.

[Ulm] 53

Appli 29 : $\mathfrak{A}_n$ est simple pour $n \geq 5$.

3) Théorèmes de Sylow.

Pour cette partie, on fixe p premier et G fini d'ordre $p^\alpha m$ où $p \nmid m$.

[Perr] 18-20

Def 30 : Un p-sous-groupe de Sylow (ou p-Sylow) de G est un sous-groupe de G d'ordre p^α. On note $\mathrm{Syl}_p(G)$ l'ensemble des p-Sylow de G.

Prop 31 : Soit $S \leq G$. On a équivalence entre $S \in \mathrm{Syl}_p(G)$ et
- S est un p-groupe d'indice premier à p.

Exple 32 : Le groupe $GL_n(\mathbb{F}_p)$, le sous-groupe des matrices triangulaires supérieures strictes $\{A = (a_{ij}) \mid a_{ij} = 0 \ i > j,\ a_{ii} = 1\}$ est un p-Sylow.

Théo 33 : Soit $H \leq G$ un sous-groupe, et $S \in \mathrm{Syl}_p(G)$. Alors il existe $a \in G$ tel que $aSa^{-1} \cap H \in \mathrm{Syl}_p(H)$. DVP

Théo 34 (Sylow) Soit G un groupe d'ordre $p^\alpha m$ où $p \nmid m$, on a
- $\mathrm{Syl}_p(G) \neq \emptyset$
- Si $H \leq G$ est un p-groupe, et S un p-Sylow de G, alors $\exists a \in G \mid aSa^{-1} \supseteq H$.
- $|\mathrm{Syl}_p(G)| \equiv 1 [p]$ et donc divise m.

DVP

[Perr] 18-20

Cor 35 : Le groupe G admet des sous-groupes d'ordre p^i pour tout $1 \leq i \leq \alpha$.

Cor 36 : Soit $S \in \mathrm{Syl}_p(G)$, on a équivalence entre $S \trianglelefteq G$ et $|\mathrm{Syl}_p(G)| = 1$.

Exple 37 : Un groupe d'ordre 63 n'est pas simple.

4) Produit semi-direct

Prop-def 38. Soit H et N deux groupes, et une action par automorphismes $\varphi : H \to \mathrm{Aut}(N)$. On pose $h.n = \varphi(h)n$ pour $h \in H, n \in N$. L'ensemble produit $N \times H$ est un groupe pour la loi de composition

$$(n,h)(n',h') := (n(h.n'), hh')$$

On appelle produit semi-direct de N par H le groupe obtenu, on le note $N \rtimes_\varphi H$ ou $N \rtimes H$.

[Perr] 21-23

Rq 39 : Si l'action de H est triviale, on retrouve le produit direct.

Def 40. Une suite de morphismes de groupes composables $N \xrightarrow{i} G \xrightarrow{p} H$ est dite exacte courte si les conditions suivantes sont vérifiées : * i est injectif, * p est surjectif, * $\mathrm{Ker}\, p = \mathrm{Im}\, i$. En identifiant N à $\mathrm{Im}\, i$, on obtient $H \simeq G/N$ en particulier.

Def 41 : Une suite exacte courte $N \xrightarrow{i} G \xrightarrow{p} H$ est dite scindée à gauche s'il existe un morphisme $p' : H \to G$ tel que $p \circ p' = \mathrm{Id}_H$. On dit que p' est une section de p. On identifie dans ce cas H à son image $\mathrm{Im}(p')$ dans G.

Prop 42 : Avec les notations de la prop-def 38, on a une suite exacte courte scindée à gauche

$$N \to N \rtimes_\varphi H \to H.$$

Théo 43 : Soit $N \xrightarrow{i} G \xrightarrow{p} H$ une suite exacte courte, on a équivalence entre
- $G \simeq N \rtimes H$
- La suite est scindée à gauche
- $N \trianglelefteq G$, $N \cap H = \{1\}$ et $G = NH$.

Exemple 44 : $D_n \simeq \mathbb{Z}/n\mathbb{Z} \rtimes \mathbb{Z}/2\mathbb{Z}$. $\mathbb{H}_8$ n'est pas un produit semi-direct.

III. Actions de groupes et algèbre linéaire.

[H2G2] 3-11

1) Action sur les matrices.

Fixons K un corps, $n, m \in \mathbb{N}$, on pose $G = GL_m(K) \times GL_n(K)$. On a une action de G sur $\mathcal{M}_{m,n}(K)$ définie par

$$a : G \times \mathcal{M}_{m,n}(K) \longrightarrow \mathcal{M}_{m,n}(K)$$

$$((P,Q), A) \longmapsto (P,Q).A := PAQ^{-1}$$

[H2G2] 3-11

Def 45 : On dit que deux matrices A et B sont équivalentes si elles sont dans la même orbite sous cette action.

Prop 46 : Deux matrices de $\mathcal{M}_{m,n}(K)$ sont équivalentes si et seulement si elles ont le même rang.

Théo 47 : Si $K=\mathbb{R}$ ou $\mathbb{C}$, Pour r entier satisfaisant $0\leq r\leq \min(m,n)$, on note O_r l'orbite des matrices de rang r. On a alors

$$\overline{O_r}=\bigcup_{k=0}^{r} O_k$$

Cor 48 : Les matrices inversibles sont denses dans $\mathcal{M}_n(K)$ pour $k=\mathbb{R}$ ou $\mathbb{C}$.

Cor 69 : L'unique orbite fermée est l'orbite O_0, l'unique orbite ouverte est $O_{\min(m,n)}$, en particulier, $GL_n(K)$ est ouvert dans $\mathcal{M}_n(K)$.

2) Représentation des groupes.

[Ulm] p144

Def 50 : Soit V un $\mathbb{C}$-espace vectoriel, une représentation (linéaire complexe) d'un groupe G est un morphisme $G\to GL(V)$ (une action par automorphisme linéaire).

Ex 51 : Représentation triviale : $G\to\mathbb{C}$ morphisme trivial.
Représentation par permutation : $s : G\to\mathfrak{S}_n$ une action, induit une représentation sur $\mathbb{C}^n$.

Prop 51 : La composition de $G\to GL(V)$ avec la trace est une application constante sur les classes de conjugaison de G, on l'appelle caractère de la représentation. (cas où V est de dimension finie).

Appl 52 : Tables de caractères

Ex 53 : La table de caractère ne caractérise pas un groupe (cas des groupes non abéliens d'ordre 8!

IV Applications aux corps finis et à la géométrie.

1) Théorème de Wedderburn

Fixons k un corps et $n\in\mathbb{N}^*$.

[Perr] 80-82

Def 54 : On pose $\mu_n(k)=\{\xi\in k \mid \xi^n=1\}$ le groupe des racines n-ièmes de l'unité.

Prop 55 : Tout sous groupe de k^* est fini cyclique.

Def 55 : On pose K_n un corps de décomposition de $P_n(X)=X^n-1\in k[X]$. Le groupe $\mu_n(K_n)$ est cyclique d'ordre n. On note $\mu_n^*(K_n)$ l'ensemble des générateurs de $\mu_n(K_n)$. Les éléments sont les racines primitives n-ièmes de l'unité.

Rq 56 : $|\mu_n^*(K_n)|=\varphi(n)$

[Perr] 80-82

Def 57 : On définit le n-ième polynôme cyclotomique $\Phi_{n,k}\in k[X]$ par la formule

$$\Phi_{n,k}(X)=\prod_{\xi\in\mu_n^*(K_n)}(X-\xi).$$

Prop 58 : On a la formule $\Phi_n(X)=\prod_{d|n}\Phi_d(X)$.

Prop 59 : On a $\Phi_{n,\mathbb{Q}}\in\mathbb{Z}[X]$. De plus, pour $\mathbb{Z}\xrightarrow{\sigma}k$ le morphisme canonique, on a $\Phi_{n,k}(\ )=\sigma(\Phi_{n,\mathbb{Q}}(\ ))$. En particulier $\Phi_{n,\mathbb{F}_p}$ s'obtient par réduction modulo p de $\Phi_{n,\mathbb{Q}}$.

Théo 60 (Wedderburn). Tout corps gauche est infini.

2) Groupe projectif.

On fixe k un corps et V un k-ev

[Perr] 975-101

Prop 61 : On a une suite exacte courte $SL(V)\to GL(V)\xrightarrow{\det}k^*$, cette suite est scindée à gauche.

Def 62 : Le quotient $GL(V)/Z(GL(V))$ est noté $PGL(V)$ le groupe projectif linéaire. De même on note $PSL(V)$ le quotient de $SL(V)$ par son centre.

Théo 63 : Le groupe $PSL_n(k)$ est simple, sauf dans les cas suivants
1) $n=2$, $k=\mathbb{F}_2$ 2) $n=2$, $k=\mathbb{F}_3$.

Prop 64 (Isomorphismes exceptionnels) On a

$GL_2(\mathbb{F}_2)=SL_2(\mathbb{F}_2)=PSL_2(\mathbb{F}_2)\simeq\mathfrak{S}_3$ $\quad PGL_2(\mathbb{F}_3)\simeq\mathfrak{S}_4$ $\quad PSL_2(\mathbb{F}_3)\simeq\mathfrak{A}_4$

$PGL_2(\mathbb{F}_4)=PSL_2(\mathbb{F}_4)\simeq\mathfrak{A}_5$ $\quad PGL_2(\mathbb{F}_5)\simeq\mathfrak{S}_5$ $\quad PSL_2(\mathbb{F}_5)\simeq\mathfrak{A}_5$.

DVP

3) Espace affine, groupes d'isométrie.

On fixe k corps

Def 65 : On appelle espace affine de direction $\vec{E}$ (un k-ev) un ensemble muni d'une action fidèle et transitive.

Def 66 : Pour $F\subseteq E$ un espace affine, on note $Isom(F)$ (resp $Isom^+(F)$) le sous groupe du groupe affine de E laissant F invariant (resp les isométries positives laissant F invariant)

Prop 67 : Si $F\subseteq\mathbb{R}^n$ est un polytope convexe, alors $Isom\,F$ agit sur les sommets de F.

Exple 68 : Si $F=P_n\subseteq\mathbb{R}^2$ est un polygone régulier, alors $Isom(F)=D_n$ et $Isom^+(F)\simeq\mathbb{Z}/n\mathbb{Z}$.

Application 69 : Si $\mathcal{C}$ est un cube régulier de $\mathbb{R}^3$ alors $Isom(\mathcal{C})\simeq\mathfrak{S}_4\times\mathbb{Z}/2\mathbb{Z}$ et les 3-Sylow de ce groupe se lisent géométriquement comme des dupilications

DVP