101 GROUPE OPÉRANT SUR UN ENSEMBLE. EXEMPLES ET APPLICATIONS.

Soit $(G, .)$ un groupe et X un ensemble.

I. Action d'un groupe sur un ensemble [Rom17, §1.6-1.7, p19–25]

I. A. Action de groupe : double approche et vocabulaire

DÉFINITION 1. [ACTION D'UN GROUPE SUR UN ENSEMBLE]
On dit que G opère à gauche sur X si on a une application $G \times X \longrightarrow X, (g, x) \longmapsto g.x$ telle que $\forall g, h \in G, \forall x \in X, g.(h.x) = (gh).x$ et $\forall x \in X, 1.x = x$.

REMARQUE 2.
- Il revient au même de se donner un morphisme de groupes $\phi : G \longrightarrow \mathfrak{S}(X)$ en posant $\phi(g)(x) = g.x$.
- Lorsque $\forall g, h \in G, \forall x \in X, g.(h.x) = (hg).x$, on parle d'action à droite.

EXEMPLE 3.
- G opère sur lui-même par translation à gauche : $g.h = gh$.
- G opère sur lui-même par conjugaison : $g.h = ghg^{-1}$. On note $\mathrm{Int}(G) = \{\mathrm{Int}(g), g \in G\}$ où $\mathrm{Int}(g) : h \longmapsto ghg^{-1}$. On remarque alors que G agit sur tout sous-groupe distingué H de G par cette opération.
- $\mathfrak{S}(X)$ opère naturellement sur X : $\sigma.x = \sigma(x)$.

THÉORÈME 4. [THÉORÈME DE CAYLEY] *G est isomorphe à un sous-groupe de $\mathfrak{S}(G)$.*

DÉFINITION 5. [ORBITES, TRANSITIVITÉ, FIDÉLITÉ]
Soit G opérant sur X.
- Pour $x \in X$, on appelle orbite de x et on note $O(x)$ l'ensemble $G.x = \{g.x \mid x \in X\}$. On note $\mathcal{O}$ l'ensemble des orbites de X. C'est une partition de X.
- On dit que l'action est transitive s'il n'y a qu'une seule orbite pour l'action de G sur X, c'est-à-dire si $\forall x \in X, O(x) = X$.
- On dit que l'action est fidèle si $\phi(g) = \mathrm{Id} \iff g = e$.

EXEMPLE 6.
- L'action de G sur lui-même par translation à gauche est transitive et fidèle.
- Si $H < G$ agit sur G par translation à droite $h.g = gh^{-1}$, alors $O(g) = gH$ est la classe à gauche de g dans G/H. On note $[G : H]$ le cardinal des orbites lorsqu'il est fini.
- $\mathfrak{S}(X)$ opère transitivement sur X.
- Restreignons l'action de $\mathfrak{S}_n$ sur $[\![1, n]\!]$ à $\langle\sigma\rangle$, où $\sigma \in \mathfrak{S}_n$. Chaque orbite correspond aux éléments d'un des cycles de la décomposition en cycles disjoints de σ.

APPLICATION 7. Soit G un groupe infini et H un sous-groupe de G, distinct de G et d'indice fini. Alors G n'est pas simple.

I. B. Les orbites comme outil de dénombrement

On considère . une action de G sur X.

DÉFINITION 8. [STABILISATEUR, ACTION LIBRE, FIXATEUR]
On appelle stabilisateur de $x \in X$ le groupe $\mathrm{Stab}(x) = \{g \in G \mid g.x = x\}$.
On dit que G opère librement sur X si $\mathrm{Stab}(x) = \{e\}$ pour tout $x \in X$.
Pour $g \in G$, on note $\mathrm{Fix}(g) = \{x \in X \mid g.x = x\}$.

PROPOSITION 9. *Soit $x \in X$. L'application $g \in G \longmapsto g.x \in O(x)$ a pour noyau $\mathrm{Stab}(x)$. L'application quotient est alors une bijection de $G/\mathrm{Stab}(x)$ dans $O(x)$. En particulier, si $|G| < +\infty$, on a $\forall x \in X, |O(x)| = [G : \mathrm{Stab}(x)] = \frac{|G|}{|\mathrm{Stab}(x)|}$.*

Dans la suite de cette partie on suppose G et X finis.

COROLLAIRE 10. [ÉQUATION AUX CLASSES]
Si $|G| < +\infty$, choisissons pour chaque orbite O un représentant x_O. Alors on a :

$$|X| = \sum_{O \in \mathcal{O}} |O| = \sum_{O \in \mathcal{O}} \frac{|G|}{|\mathrm{Stab}(x_O)|}$$

APPLICATION 11. [CARDINAL DE $\mathcal{D}_n(\mathbb{F}_q)$] [Rom17, §5.6, p148–151]
Soit $n \in \mathbb{N}, q = p^r$ où p premier, $r \neq 0$. Soit $\mathcal{D}_n(\mathbb{F}_q)$ l'ensemble des matrices diagonalisables de $\mathbb{F}_q$. Alors en posant $|\mathcal{GL}_0(\mathbb{F}_q)| = 1$, on a :

$$|\mathcal{D}_n(\mathbb{F}_q)| = \sum_{n_1+\cdots+n_q=n} \frac{|\mathcal{GL}_n(\mathbb{F}_q)|}{\prod_{i=1}^{q} |\mathcal{GL}_{n_i}(\mathbb{F}_q)|}$$

EXEMPLE 12. [ACTION PAR CONJUGAISON] Si G agit par conjugaison sur lui-même, notons $Z_h(G) = \{g \in G \mid ghg^{-1} = h\}$. Alors $|G| = |Z(G)| + \sum_{O \in \mathcal{O} \mid |O| \geq 2} \frac{|G|}{|Z_{x_O}(G)|}$.

COROLLAIRE 13. [FORMULE DE BURNSIDE] *[Rom17, §1.10, p37]*

$$|\mathcal{O}| = \frac{1}{|G|}\sum_{g\in G}|\mathrm{Fix}(g)|$$

APPLICATION 14. On peut colorier les 6 faces (toutes identiques) d'un cube avec 3 couleurs de 57 manières différentes.

II. Actions sur les groupes finis

On suppose toujours G de cardinal fini dans cette partie. On pose $|G| = n$.

II. A. Résultats généraux **[Rom17, §1.1/1.7, p2/25]**

THÉORÈME 15. [THÉORÈME DE LAGRANGE]
L'ordre de tout sous-groupe de G divise n. En particulier, l'ordre d'un élément de G divise n.

THÉORÈME 16. [THÉORÈME DE CAUCHY]
Si p est un diviseur premier de n, alors il existe un élément d'ordre p dans G.

II. B. Cas particulier des p-groupes **[Per96, §1.5, p18–20]**

Soit p un nombre premier diviseur de n. On notera $n = p^a m$ où $p \nmid m$.

DÉFINITION 17. [p-GROUPE, p-SOUS-GROUPE DE SYLOW]
Si n est une puissance de p $(m = 1)$, on dit que G est un p-groupe.
Plus généralement, on appelle p-sous-groupe de SYLOW (ou p-SYLOW) un sous-groupe de G de cardinal p^a.

APPLICATION 18. [DE L'EXEMPLE 12] Le centre d'un p-groupe non trivial est non trivial.

THÉORÈME 19. [THÉORÈME DE SYLOW 1] *Il existe au moins un p-SYLOW dans G.*

COROLLAIRE 20. *Il existe au moins un sous-groupe de G d'ordre p^i pour tout $i \in [\![1, a]\!]$.*

THÉORÈME 21. [THÉORÈME DE SYLOW 2]
(i) Si $H < G$ est un p-groupe, alors il existe un p-SYLOW S tel que $H < S$,
(ii) Les p-SYLOW de G sont tous conjugués,
(iii) Notons Σ le nombre de p-SYLOW de G. Alors $\Sigma \mid m$ et $\Sigma \equiv 1 \mod p$.

COROLLAIRE 22. *Soit S un p-SYLOW de G. Alors $S \lhd G \iff S$ est l'unique p-SYLOW de G.*

APPLICATION 23. Tout groupe d'ordre 63 ou 255 n'est pas simple.

II. C. Action sur le groupe $\mathfrak{S}_n$ **[Rom17, Ch2, p39]**

Lien entre orbites de l'action naturelle et support, décompositions en produits de cycles à support disjoints
Action par conjugaison : caractérisations des orbites par leur type.

III. Applications des actions de groupes en algèbre linéaire et en géométrie

III. A. Actions sur des ensembles matriciels **[CG13, ChI/III, p2/83]**

Soient $m, n \in \mathbb{N}^*$, $\mathbb{K}$ un corps.

DÉFINITION 24. [ACTION DE STEINITZ]
Posons $G = \mathcal{GL}_m(\mathbb{K}) \times \mathcal{GL}_n(\mathbb{K})$. On appelle action de STEINITZ l'action :

$$\begin{array}{ccc} G \times \mathcal{M}_{m,n}(\mathbb{K}) & \longrightarrow & \mathcal{M}_{m,n}(\mathbb{K}) \\ ((P,Q), A) & \longmapsto & PAQ^{-1} \end{array}$$

Les orbites pour cette action sont appelées classes d'équivalence.

THÉORÈME 25. *Deux matrices sont équivalentes si et seulement si elles ont même rang. Ainsi $\mathcal{O} = \{O_r \mid 0 \le r \le \min(m,n)\}$ où $O_r = \{A \in \mathcal{M}_{m,n}(\mathbb{K}) \mid \mathrm{rg}(A) = r\}$.*

DÉFINITION 26. [ACTION PAR CONJUGAISON]
Les orbites de l'action de $\mathcal{GL}_n(\mathbb{K})$ sur $\mathcal{M}_n(\mathbb{K})$ sont appelées classes de similitude.

PROPOSITION 27. *Dans $\mathbb{K} = \mathbb{C}$, $M \in \mathcal{M}_n(\mathbb{K})$ est diagonalisable si et seulement si sa classe de similitude est fermée dans $\mathcal{M}_n(\mathbb{K})$.*

III. B. Actions sur un espace vectoriel **[Rom17, Ch6, p179]**

Soit G un groupe et E un $\mathbb{C}$-espace vectoriel de dimension finie.

DÉFINITION 28. [REPRÉSENTATION]
Une représentation (linéaire) de G dans E est un morphisme de groupes $\rho : G \longmapsto \mathrm{GL}(E)$.

REMARQUE 29. Se donner une représentation de G dans E revient à se donner une action de groupes de G sur E en posant $\rho(g)(x) = g.x$.

EXEMPLE 30. [REPRÉSENTATION TRIVIALE] $\rho : g \longmapsto \mathrm{Id}_E$ est une représentation de G sur E.

EXEMPLE 31. Si E est de dimension 1 :
- les représentations de $\mathfrak{S}_n$ dans E sont $\rho : \sigma \longrightarrow \mathrm{Id}_E$ et $\rho : \sigma \longrightarrow \varepsilon(\sigma)\,\mathrm{Id}_E$.
- les représentations de $\mathbb{Z}/2\mathbb{Z}$ dans E sont $\rho : \overline{x} \longrightarrow \mathrm{Id}_E$ et ρ définie par $\rho(\overline{1}) = -\mathrm{Id}_E$.

Si E est de dimension 2, les représentations de $\mathbb{Z}/2\mathbb{Z}$ dans E sont $\rho : \overline{x} \longrightarrow \mathrm{Id}_E$ et ρ définie par $\rho(\overline{1}) = \mathrm{diag}(\pm 1, \pm 1)$ dans une certaine base.

EXEMPLE 32. [REPRÉSENTATIONS DE PERMUTATIONS]
$\mathfrak{S}_n \longrightarrow \mathcal{GL}_n(\mathbb{C}), \sigma \longmapsto P_\sigma$ est une représentation de $\mathfrak{S}_n$ sur $\mathbb{C}^n$.
Plus généralement, si G est fini de cardinal n et E est de dimension n, soit $(e_g)_{g\in G}$ une base de E. Alors l'application linéaire $\rho(g)$ définie par $\rho(g)(e_h) = e_{gh}$ pour $h \in G$ définit une représentation de G dans E.

III. C. Applications en géométrie

[Aud06, ChIII/V, p111/360] [Rom17, §3.4.3/6.1, p87/180]

EXEMPLE 33. Isométries du plan conservant un segment $[A, B]$ de centre O :
- Id l'identité,
- ρ la rotation d'angle π et de centre O,
- s la symétrie d'axe (AB),
- $s\rho$ la symétrie d'axe la droite orthogonale à (AB) passant par O.

On vérifie que ces isométries forment un groupe isomorphe au groupe de KLEIN $(\mathbb{Z}/2\mathbb{Z})^2$.

DÉFINITION 34. [DÉPLACEMENT, ANTIDÉPLACEMENT]
Un déplacement (resp. antidéplacement) est un isomorphisme dont la partie linéaire est de déterminant 1 (resp. -1).

Soit G groupe fini d'isométries. On note G^+ ses déplacements et G^- ses antidéplacements.

PROPOSITION 35.
- *Il existe un point fixe à toutes les isométries de G,*
- *G^+ est cyclique, engendré par une rotation ρ.*
- *Si G contient un antidéplacement σ, alors $[G : G^+] = 2$ et $G^- = \sigma G^+$. σ est une réflexion dont l'axe contient le centre de ρ. On a $G = \langle \sigma, \rho \rangle$.*

EXEMPLE 36. Le groupe des isométries du plan préservant un polygone régulier à n sommets de centre O contient les rotations d'ordre n autour du centre et les n réflexions par rapport aux droites joignant :

i) n rotations de centre O et d'angle $\frac{k2\pi}{n}$ pour $k \in [\![0, n-1]\!]$,

ii) n symétries d'axe 2 sommets opposés ou 2 milieux de côtés opposés si n est pair, 1 sommet et le milieu du côté opposé si n est impair.

C'est le groupe diédral D_{2n}.

APPLICATION 37. D_{2n} s'injecte naturellement dans $\mathcal{GL}_2(\mathbb{C})$, envoyant la rotation d'angle $2\pi/n$ et la symétrie sur

$$R = \begin{pmatrix} \cos(2\pi/n) & -\sin(2\pi/n) \\ \sin(2\pi/n) & \cos(2\pi/n) \end{pmatrix} \quad \text{et} \quad S = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

On a donc une représentation naturelle de D_{2n} dans $\mathbb{C}^2$.

SPEECH

La théorie des actions de groupes permet d'étudier les interactions entre ensembles et ainsi d'obtenir des propriétés sur le groupe agissant ou l'ensemble sur lequel il agit.
Historiquement, les premières opérations apparaissent naturellement en géométrie dès l'antiquité (rotations, symétries, ...).
Dans la première partie, on définit de deux manières différentes mais équivalentes les actions de groupes, ce qui offre deux visions différentes. On parle du théorème de CAYLEY, du vocabulaire associé aux actions de groupes. La notion de partitionnement en orbites amène l'équation aux classes qui possède de nombreuses applications notamment en dénombrement : on peut par exemple dénombrer le nombre de matrices inversibles diagonalisables à coefficients dans un corps fini, proposé en développement, ou encore utiliser la formule de BURNSIDE.
Ensuite,, on introduit des résultats généraux des actions sur des groupes finis, avec notamment le très utile théorème de LAGRANGE, et le théorème de CAUCHY qui constitue une forme de réciproque. Puis on parle de la théorie des p-SYLOW, dont le premier théorème constituera le second développement.
Enfin la dernière partie se consacre aux nombreux domaines d'applications des actions de groupes :

- notions de classes d'équivalences et de classes de similitudes dans le cas d'ensembles matriciels,
- représentations de groupes dans le cas d'espaces vectoriels (avec toujours 2 définitions comme au début),
- groupes isomorphes au groupe d'isométries préservant des figures (polygone à n côtés et tétraèdre) en géométrie.

COMMENTAIRES

Le produit semi-direct est hors programme, mais très rentable si on est à l'aise dessus (pour les groupes diédraux, la géométrie, ...)
Dans la troisième partie, il n'y a pas vraiment de lien entre les applications, mais ce n'est pas grave car les actions de groupes sont des outils. On peut aller plus loin dans la théorie des représentations : application, transformée de FOURIER (le jury insiste dessus, voir [Pey04]).

QUESTIONS

Q Mise à part les matrices à coefficients réels ou complexes, y a-t-il des exemples naturels de groupes topologiques ?

Q Soit G fini tel que $\mathrm{Aut}(G)$ agit transitivement sur $G \setminus \{1\}$. Montrer que $Z(G) \neq \{1\}$.

R La transitivité de l'action implique que les ordres de tous les éléments distinct de 1 sont égaux, notons o cette ordre commun. Pour p diviseur premier de $n = |G|$, on a qu'il existe un élément d'ordre p (théorème de CAUCHY), donc $o = p$ puis $n = p$. Ainsi G est un groupe d'ordre p et on conclut avec l'exemple 12.

Q Calculer $|\mathcal{GL}_n(\mathbb{F}_q)|$, puis le nombre de sous-espaces vectoriels de dimension r de $(\mathbb{F}_q)^n$.

R Cela revient à dénombrer le nombre de bases[1] de $(\mathbb{F}_q)^n$. En effet si $\mathcal{B} = (e_1, \dots, e_n)$ est une base de $(\mathbb{F}_q)^n$, alors $\mathcal{GL}_n(\mathbb{F}_q) \longrightarrow B, M \longmapsto (Me_1, \dots, Me_n)$ où B est l'ensemble des bases de $(\mathbb{F}_q)^n$ est une bijection.
On a $q^n - 1$ choix pour le premier vecteur de la base, puis $q^n - q$ pour le deuxième, ..., puis $q^n - q^{k-1}$ pour le k-ième. Finalement : $|\mathcal{GL}_n(\mathbb{F}_q)| = \prod_{k=1}^n q^n - q^{k-1}$.
Considérons ensuite l'action $\mathcal{GL}_n(\mathbb{F}_q) \times A_r \longrightarrow A_r, (M, V) \longmapsto M.V$ où A_r est l'ensemble des sous-espaces vectoriels de dimension r. L'action est transitive (penser aux matrices de passage, ...). Calculons $\mathrm{Stab}(V)$. En se plaçant dans la bonne base, on voit que $M \in \mathrm{Stab}(V)$ si et seulement si $M = \begin{pmatrix} M_V & \star \\ 0 & M_U \end{pmatrix}$ où $M_V \in \mathcal{GL}_r, M_U \in \mathcal{GL}_{n-r}$.
Donc $|\mathrm{Stab}(V)| = |\mathcal{GL}_r(\mathbb{F}_q)|\,|\mathcal{GL}_{n-r}(\mathbb{F}_q)|\,q^{r(n-r)}$ et l'équation aux classes donne $|A_r| = |\mathcal{GL}_n(\mathbb{F}_q)| \,/\, |\mathrm{Stab}(V)|$.

BIBLIOGRAPHIE

[Aud06] M. AUDIN : *Géométrie*. EDP Sciences, 2006.

[CG13] P. CALDERO et J. GERMONI : *Histoires hédonistes de groupes et de géométries - Tome 1*. Calvage et Mounet, 2013.

[Per96] D. PERRIN : *Cours d'algèbre*. Ellipses, 1996.

[Pey04] G. PEYRÉ : *L'algèbre discrète de la transformée de* FOURIER. Ellipses, 2004.

[Rom17] J.-E. ROMBALDI : *Mathématiques pour l'agrégation : Algèbre et géométrie*. De Boeck, 2017.

1. comptées avec l'ordre des éléments