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

1. Notion d'action de groupe

1.1. Action de groupe

1. Définition. Une *action* d'un groupe G sur un ensemble X est la donnée d'un morphisme de groupes $G \longrightarrow \mathfrak{S}(X)$.

2. Proposition. Soit $\varphi \colon G \times X \longrightarrow X$ une application. Alors l'application

$$\left|\begin{array}{l} G \longrightarrow \mathfrak{S}(X), \\ g \longmapsto \varphi(d, \cdot) \end{array}\right.$$

est bien définie et est une action si et seulement si, pour tous éléments $g, h \in G$ et tout élément $x \in X$, on a

$$\varphi(gh, x) = \varphi(g, \varphi(h, x)) \qquad \text{et} \qquad \varphi(e, x) = x.$$

3. Remarque. Lorsqu'un groupe G agit sur un ensemble X, cette action est donnée par un morphisme $\rho \colon G \longrightarrow \mathfrak{S}(X)$, ce dernier sera implicite et on note $g \cdot x \coloneqq \rho(g)(x)$ pour $g \in G$ et $x \in X$. De la sorte, les dernières relations se réécrivent sous la forme

$$(gh) \cdot x = g \cdot (h \cdot x) \qquad \text{et} \qquad e \cdot x = x.$$

4. Exemple. Soit X un ensemble. Alors le groupe $\mathfrak{S}(X)$ agit naturellement sur l'ensemble X par l'action définie par la relation $\sigma \cdot x \coloneqq \sigma(x)$ avec $\sigma \in \mathfrak{S}(X)$ et $x \in X$.

5. Exemple. Soit E un espace vectoriel. Alors le groupe $\mathrm{GL}(E)$ agit naturellement sur l'espace E.

6. Proposition. Soit G un groupe sur un ensemble X. Soit $H \leqslant G$ un sous-groupe. Alors l'action du groupe G sur l'ensemble X induit une action du groupe H sur ce dernier par le morphisme composée $H \hookrightarrow G \longrightarrow \mathfrak{S}(X)$.

1.2. Des actions particulières

7. Définition. Un *point fixe* sous l'action d'un groupe G sur un ensemble X est un élément $x \in X$ vérifiant

$$\forall g \in G, \qquad g \cdot x = x.$$

On note $X^G \subseteq X$ l'ensemble des points fixes.

8. Exemple. Le vecteur nul est un point fixe pour l'action du groupe $\mathrm{GL}(E)$ sur l'espace E.

9. Définition. Soit $k \in \mathbf{N}^*$ un entier non nuls. Une action d'un groupe G sur un ensemble X est

- *fidèle* si le morphisme $G \longrightarrow \mathfrak{S}(X)$ est injectif, c'est-à-dire si
$$\forall g \in G, \qquad (\forall x \in X,\ g \cdot x = x) \quad \Longrightarrow \quad g = e\ ;$$
- *libre* si, pour tous élément $x \in X$ et $g \in G$, on a
$$g \cdot x = x \quad \Longrightarrow \quad g = e.$$
- *k-transitive* si, pour tous k-uplets $(x_1, \dots, x_k) \in X^k$ et $(y_1, \dots, y_k) \in X^k$, il existe un élément $g \in G$ tel que
$$\forall i \in \{1, \dots, k\}, \qquad g \cdot x_i = y_i\ ;$$
- *simplement k-transitive* si elle est k-transitive et un tel élément g est unique ;
- *transitive* si elle est 1-transtive.
- *simplement transitive* si elle est simplement 1-transtive.

10. Proposition. Une action fidèle est libre.

11. Exemple. L'action du groupe $\mathrm{GL}_n(k)$ sur l'espace k^n est fidèle et simplement n-transitive. Elle es k-transitive et elle n'est pas simplement k-transitive pour $k < n$.

12. Exemple. Lorsque $n \geqslant 3$, l'action du groupe alterné $\mathfrak{A}_n$ sur l'ensemble $\{1, \dots, n\}$ est $n - 2$ transitive.

1.3. Orbites, stabilisateurs et équation aux classes

13. Définition. Soit G un groupe agissant sur un ensemble X. L'*orbite* d'un élément $x \in X$ est l'ensemble

$$\mathrm{Orb}_G(x) \coloneqq \{g \cdot x \mid g \in G\} \subset X$$

et son stabilisateur est l'ensemble

$$\mathrm{Stab}_G(x) \coloneqq \{g \in G \mid g \cdot x = x\} \subset G.$$

L'ensemble des orbites est noté G/X.

14. Exemple. En considérant l'action du groupe $\mathfrak{S}_3$ sur l'ensemble $\{1, 2, 3\}$, le stabilisateur de l'entier 1 est l'ensemble $\mathrm{Stab}_{\mathfrak{S}_3}(1) = \{\mathrm{Id}, (2\ 3)\}$ et son orbite est l'ensemble $\mathrm{Orb}_{\mathfrak{S}_3}(1) = \{1, 2, 3\}$.

15. Remarque. Une action est transitive si elle n'admet qu'une seule orbite.

16. Proposition. Les stabilisateurs sont des sous-groupes de G.

17. Proposition. Soit $x \in X$ un élément. Alors l'application

$$\left|\begin{array}{l} G/\mathrm{Stab}_G(x) \longrightarrow \mathrm{Orb}_G(x), \\ g\,\mathrm{Stab}_G(x) \longmapsto g \cdot x \end{array}\right.$$

est une bijection.

18. Corollaire. Soit $x \in X$ un élément. Alors $|\mathrm{Orb}_G(x)| = [G : \mathrm{Stab}_G(x)]$. En particulier, si le groupe G est fini, alors

$$|\mathrm{Orb}_G(x)| = |G| \,/\, |\mathrm{Stab}_G(x)|.$$

19. Théorème *(équation aux classes)*. Soit G un groupe agissant sur ensemble fini X. Soit $\{x_1, \dots, x_r\}$ un système de représentants des orbites. Alors

$$|X| = \sum_{i=1}^{r} \frac{|G|}{|\mathrm{Stab}_G(x_i)|}.$$

20. Remarque. Si l'action est transitive, alors $|X| = |G| \,/\, |\mathrm{Stab}_G(x)|$ avec $x \in X$.

21. Corollaire. Soit $\{x_1, \dots, x_r\}$ un système de représentants des orbites non ponctuelles. Alors

$$|X| = |X^G| + \sum_{i=1}^{r} \frac{|G|}{|\mathrm{Stab}_G(x_i)|}.$$

22. Corollaire. Soit G un p-groupe agissant sur un ensemble fini. Alors
$$|X^G| \equiv |X| \mod p.$$
23. Application *(théorème de Gauchy)*. Soient G un groupe fini et p un diviseur premier de son ordre. Alors le groupe G admet un élément d'ordre p.
24. Théorème *(Burnside)*. Soit G un groupe fini agissant sur un ensemble fini X. Pour un élément $g \in G$, on note
$$\operatorname{Fix}(g) \coloneqq \{x \in X \mid g \cdot x = x\}.$$
Alors le nombre d'orbites $t \geqslant 1$ vérifiant la relation
$$\sum_{g \in G} |\operatorname{Fix}(g)| = t\,|G|.$$

2. Des actions classiques et applications

2.1. L'action par translation

25. Définition. L'*action par translation (à gauche)* d'un groupe G est l'action sur lui-même définie par l'égalité
$$g \cdot h \coloneqq gh, \qquad g, h \in G.$$
26. Proposition. L'action par translation est fidèle et transitive. En particulier, l'action donne un morphisme de groupes injectif $G \longhookrightarrow \mathfrak{S}(G)$.
27. Théorème *(Cayley)*. Soit G un groupe fini d'ordre n. Alors il est isomorphe à un sous-groupe du groupe $\mathfrak{S}_n$.
28. Hypothèse. À présent, on considère l'action par translation du groupe $\mathrm{GL}_n(k)$ sur l'ensemble $\mathscr{M}_{n,m}(k)$ qui se définie de la même manière.
29. Théorème. Soient $A, B \in \mathscr{M}_{n,m}(k)$ deux matrices. Alors les points suivants sont équivalents :
- les matrices A et B sont dans la même orbite, c'est-à-dire qu'il existe une matrice inversible $P \in \mathrm{GL}_n(k)$ telle que $A = PB$;
- elle ont le même noyau.

30. Théorème *(pivot de Gauss)*. Soit $A \in \mathscr{M}_{n,m}(k)$ une matrice. Alors il existe une matrice inversible $P \in \mathrm{GL}_n(k)$ qui est un produit de matrices de permutation et de transvection telle que la matrice PA soient échelonnée en ligne.
31. Exemple. Par opérations sur les lignes, on obtient les transformations
$$\begin{pmatrix} 1 & 2 & 3 \\ 0 & 4 & 5 \\ 6 & 7 & 8 \end{pmatrix} \longrightarrow \begin{pmatrix} 1 & 2 & 3 \\ 0 & 4 & 5 \\ 0 & -5 & 2 \end{pmatrix} \longrightarrow \begin{pmatrix} 1 & 2 & 3 \\ 0 & 4 & 5 \\ 0 & 0 & 29/2 \end{pmatrix}.$$

2.2. L'action par conjugaison

32. Définition. L'*action par translation* d'un groupe G est l'action sur lui-même définie par l'égalité
$$g \cdot h \coloneqq ghg^{-1}, \qquad g, h \in G.$$
L'orbite d'un élément $h \in G$ est appelée sa *classe de conjugaison* et son stabilisateur est appelé son *centralisateur*, noté $\mathrm{Z}_G(h)$.
33. Exemple. On a $\mathrm{Z}_G(e) = G$.
34. Proposition. Soit $h \in G$ un élément. Alors l'action par conjugaison vérifie les points suivants :
- si le groupe G n'est pas trivial, alors elle n'est jamais libre ;
- la classe de conjugaison du neutre e est réduite à l'élément e ;
- on a $h \in \mathrm{Z}(G) \Leftrightarrow \mathrm{Z}_G(h) = G$.

35. Corollaire. Un élément appartient au centre si et seulement si sa classe de conjugaison est réduit à un seul élément. En particulier, le centre est l'union des classes de conjugaison de taille une.
36. Application. Le centre d'un p-groupe n'est pas trivial.
37. Application *(Weddenburn)*. Tout corps fini est commutatif.
38. Lemme. Soient $\sigma \in \mathfrak{S}_n$ une permutation et $a_1, \dots, a_k \in \{1, \dots, n\}$ des entiers deux à deux distincts. Alors $\sigma(a_1 \ \cdots \ a_n)\sigma^{-1} = (\sigma(a_1) \ \cdots \ \sigma(a_n))$.
39. Théorème. Deux permutations du groupe $\mathfrak{S}_n$ sont conjuguées si et seulement si leurs décompositions en produit de cycles à supports disjoints contiennent le même nombre de k-cycles pour tout entier $k \in \{2, \dots, n\}$.
40. Exemple. Les permutations $(1\ 6\ 3)(2\ 4)$ et $(1\ 4)(2\ 3\ 5)$ sont conjuguées dans le groupe $\mathfrak{S}_6$.

2.3. Les actions au service du dénombrement

41. Lemme. Soit E un k-espace vectoriel de dimension n. Soient $u \in \mathscr{L}(E)$ un endomorphisme nilpotent et $x \in E \setminus \{0\}$ un vecteur non nul. Soit $r \in \mathbf{N}^*$ l'entier maximal tel que la famille $(x, u(x), \dots, u^{r-1}(x))$ soit libre. Alors $u^r(x) = 0$. D1
42. Théorème. Soit $\mathbf{F}_q$ le corps fini à q éléments. Alors l'ensemble des matrices nilpotentes de taille n à coefficients dans le corps $\mathbf{F}_q$ est de cardinal $q^{n(n-1)}$.
43. Lemme. Une matrice de taille n à coefficients dans le corps $\mathbf{F}_q$ est diagonalisable si et seulement si elle est annulée par le polynôme $X^q - X$.
44. Théorème. Le nombre de matrices diagonalisables de $\mathrm{GL}_n(\mathbf{F}_q)$ vaut
$$\sum_{\substack{(n_1, \dots, n_{q-1}) \in \mathbf{N}^{q-1} \\ n_1 + \dots + n_{q-1} = n}} \frac{|\mathrm{GL}_n(\mathbf{F}_q)|}{|\mathrm{GL}_{n_1}(\mathbf{F}_q)| \cdots |\mathrm{GL}_{n_{q-1}}(\mathbf{F}_q)|}.$$
45. Définition. Dans un corps fini $\mathbf{F}_p$ avec $p > 2$, on définit le *symbole de Legendre* par l'égalité
$$\left(\frac{a}{p}\right) = a^{(p-1)/2} \in \{\pm 1\}.$$
46. Lemme. Soient p un nombre premier impair et $a \in \mathbf{F}_p^\times$ un élément non nul. Alors
$$|\{x \in \mathbf{F}_p \mid ax^2 = 1\}| = 1 + \left(\frac{a}{p}\right).$$
47. Remarque. On peut faire agir le groupe $\mathbf{Z}/p\mathbf{Z}$ sur l'ensemble $\mathbf{F}_q^p$ par l'action définie par l'égalité
$$k \cdot (x_1, \dots, x_p) \coloneqq (x_{1+k}, \dots, x_{p+k}), \qquad k \in \mathbf{Z}/p\mathbf{Z},\ (x_1, \dots, x_p) \in \mathbf{F}_q^p.$$
48. Théorème. Soient p et q deux nombres premiers impairs distincts. Alors
$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{(p-1)/2 \times (q-1)/2}.$$

3. Les actions de groupes en algèbre et géométrie

3.1. Classifications en algèbre linéaire : actions sur des espaces de matrices

49. Définition. Deux matrices $A, B \in \mathscr{M}_n(k)$ sont semblables si elles appartiennent à la même classe de conjugaison, c'est-à-dire s'il existe une matrice inversible $P \in \mathrm{GL}_n(k)$ vérifiant $A = PBP^{-1}$.

50. Théorème *(réduction de Frobenius).* Soit $u \in \mathscr{L}(E)$. Alors il existe un unique entier $r \geqslant 1$, des uniques polynômes unitaires non constants $P_1, \dots, P_r \in \mathbf{K}[X]$ et des sous-espaces vectoriels $E_1, \dots, E_r \subset E$ stables par l'endomorphisme u tels que
- $E = E_1 \oplus \cdots \oplus E_r$;
- $P_r \mid \cdots \mid P_1$;
- pour tout entier $i \in [\![1, r]\!]$, l'endomorphisme $u|_{E_i}$ induit sur le sous-espace vectoriel E_i est cyclique de polynôme minimal P_i.

La suite $(P_1, \dots P_r)$ sont les *invariants de similitude* de l'endomorphisme u.

51. Corollaire. Avec les mêmes hypothèses et notations, il existe une base de E dans laquelle l'endomorphisme u ait pour matrice
$$\mathrm{diag}(C_{P_1}, \dots, C_{P_r}).$$
De plus, on a $P_1 = \pi_u$ et $P_1 \cdots P_r = \chi_u$.

52. Corollaire. Deux matrices de taille n sont semblables si et seulement si elles ont les mêmes invariants de similitude.

53. Définition. Notons $\mathscr{S}_n(k) \subset \mathscr{M}_n(k)$ l'ensemble des matrices symétriques. L'*action de congruence* est l'action du groupe $\mathrm{GL}_n(k)$ sur l'ensemble $\mathscr{S}_n(k)$ définie par l'égalité
$$P \cdot A \coloneqq PA\,{}^{\mathrm{t}}P.$$
Deux matrices de $\mathscr{S}_n(k)$ sont *congruentes* si elles appartiennent à la même orbite pour l'action de congruence.

54. Remarque. Deux matrices symétriques congruentes sont congruentes si et seulement si elles représentent la même forme quadratique dans deux bases.

55. Théorème *(de classification des formes quadratiques).* Les orbites de l'action de congruence sont caractérisées par
- si $k = \mathbf{C}$, le rang ;
- si $k = \mathbf{R}$, la signature ;
- si $k = \mathbf{F}_q$, le discriminant.

3.2. Les groupes d'isométries préservant un ensemble

56. Définition. Le *groupe diédral de degré n* est le groupe $\mathbf{D}_n$ des isométries préservant le polygone régulier $\mathscr{P}_n \subset \mathbf{R}^2$ à n sommets.

57. Remarque. Le groupe $\mathbf{D}_n$ agit naturellement sur le polygone $\mathscr{P}_n$.

58. Proposition. Le groupe $\mathbf{D}_n$ est d'ordre $2n$ et il est isomorphe au groupe
$$\langle r, s \mid r^n = e,\ s^2 = e,\ srs^{-1} = r^{-1} \rangle.$$

59. Proposition. Soit G un groupe. Alors les points suivants sont équivalents :
- le groupe G est isomorphe au groupe $\mathbf{D}_n$;
- il est engendré par deux éléments $a, b \in G$ tels que $\mathrm{o}(a) = \mathrm{o}(ab) = 2$ et $\mathrm{o}(b) = n$.

60. Définition. Soit $\mathscr{E}$ un espace affine. Une isométrie $\varphi \in \mathrm{Isom}(\mathscr{E})$ *stabilise* une partie $X \subset \mathscr{E}$ si $\varphi(X) \subset X$. On note $\mathrm{Isom}(X)$ le groupe des isométries de $\mathscr{E}$ stabilisant X ainsi que $\mathrm{Isom}^+(X)$ le groupe des isométries positives de $\mathscr{E}$ stabilisant X

61. Lemme. Soit $X \subset \mathscr{E}$. On suppose que la partie X est l'enveloppe convexe d'une partie $S \subset \mathscr{E}$ et que les points de S sont extrémaux. Alors toute isométrie stabilisant X stabilise S, c'est-à-dire $\mathrm{Isom}(X) = \mathrm{Isom}(S)$.

62. Théorème. Les groupes d'isométries du cube $C \subset \mathbf{R}^3$ sont
$$\mathrm{Isom}^+(C) \simeq \mathfrak{S}_4 \qquad \text{et} \qquad \mathrm{Isom}(C) \simeq \mathfrak{S}_4 \times \mathbf{Z}/2\mathbf{Z}.$$

– D2 –

3.3. Vers la théorie des représentations linéaires des groupes finis

63. Définition. Une *représentation linéaire* d'un groupe fini G est la donnée d'un $\mathbf{C}$-espace vectoriel V et d'un morphisme de groupes $\rho\colon G \longrightarrow \mathrm{GL}(V)$. Un *morphisme* entre deux représentations $\rho\colon G \longrightarrow \mathrm{GL}(V)$ et $\rho'\colon G \longrightarrow \mathrm{GL}(V')$ est une application linéaire $f\colon V \longrightarrow V'$ telle que
$$\forall g \in G, \qquad f \circ \rho(g) = \rho'(g) \circ f.$$

64. Remarque. Comme $\mathrm{GL}(V) \subset \mathfrak{S}(V)$, une représentation linéaire est un cas particulier d'action de groupe.

65. Exemple. L'espace vectoriel $\mathbf{C}^3$ représente le groupe $\mathfrak{S}_3$ par l'action
$$\sigma \cdot (x_1, x_2, x_3) \coloneqq (x_{\sigma(1)}, x_{\sigma(2)}, x_{\sigma(3)}).$$

66. Définition. Une *sous-représentation* d'une représentation $\rho\colon G \longrightarrow \mathrm{GL}(V)$ est un sous-espace vectoriel $W \subset V$ qui est stable par tous les isomorphismes $\rho(g)$ avec$g \in G$. Une sous-représentation est irréductible si elle n'admet pas de sous-représentations autres que $\{0\}$ et V.

67. Théorème *(Maschke).* Toute sous-représentation possède un supplémentaire qui est une sous-représentation.

68. Théorème *(Schur).* Soit $f\colon V \longrightarrow V'$ une morphisme de représentations. Alors
- il est soit nul soit un isomorphisme ;
- si $V = V'$, alors c'est une homothétie.

[1] Josette Calais. *Éléments de théorie des groupes.* 3e édition. Presses Universitaires de France, 1998.
[2] Philippe Caldero et Jérôme Germoni. *Nouvelles histoires hédonistes de groupes et de géométries.* T. Tome premier. Calvage & Mounet, 2017.
[3] Philippe Caldero et Jérôme Germoni. *Nouvelles histoires hédonistes de groupes et de géométries.* T. Tome second. Calvage & Mounet, 2018.
[4] Daniel Perrin. *Cours d'algèbre.* Ellipses, 1996.
[5] Jean-Étienne Rombaldi. *Mathématiques pour l'agrégation. Algèbre et géométrie.* 2e édition. De Boeck Supérieur, 2021.
[6] Felix Ulmer. *Théorie des groupes.* 2e édition. Ellipses, 2021.