Autour des groupes

Valentin Moguérou
valentin.moguerou@universite-paris-saclay.fr

§ 1. Définition et premières propriétés

Soit G un groupe noté multiplicativement et X un ensemble.

On appelle action de groupe (à gauche) toute application $\cdot : G \times X \to X$ (l'image de (g, x) étant notée $g \cdot x$) telle que

$$g' \cdot (g \cdot x) = (g'g) \cdot x \quad \text{et} \quad e \cdot x = x$$

pour tout $(g, g') \in G^2$.

On dit alors que G opère sur X. La donnée d'une action de G sur X est équivalente à celle d'un morphisme $G \to \mathfrak{S}(X)$.

1. On définit sur X la relation binaire suivante : $x \mathcal{R} y \iff \exists g \in G, y = g \cdot x$. Montrer qu'il s'agit d'une relation d'équivalence. La classe d'équivalence de x se note alors $G \cdot x$ et est appelée *orbite* de x. L'ensemble des orbites se note $G \setminus X$.
2. On appelle stabilisateur de $x \in X$, noté G_x, l'ensemble $\{g \in G, g \cdot x = x\}$. Montrer qu'il s'agit d'un sous-groupe de G.

On rappelle que si H est un sous-groupe de G, alors G/H représente l'ensemble des classes d'équivalences d'éléments de G pour la relation $x^{-1}y \in H$. L'application $\pi : G \to G/H, g \mapsto \overline{g}$ s'appelle projection canonique.

3. Montrer que les fibres $\pi^{-1}(\overline{g})$ sont en bijection avec H. En déduire le théorème de Lagrange.
4. Montrer que l'application

$$\begin{aligned} \varphi_x : G/G_x &\longrightarrow G \cdot x \\ \overline{g} &\longmapsto g \cdot x \end{aligned}$$

est bien définie et bijective. On l'appelle bijection canonique (équivariante). Lorsque G/G_x est fini, son cardinal, appelé indice de G_x dans G est noté $[G : G_x]$.

5. On suppose G fini. Montrer que

$$|G \cdot x| = [G : G_x] = \frac{|G|}{|G_x|}.$$

§ 2. Quelques exemples

On dit qu'une action $\cdot$ de G sur X est

— *transitive* ssi pour tous $x, y \in X$ il existe $g \in G$ tel que $y = g \cdot x$;

— *simplement transitive* ssi de plus, un tel g est unique ;

— *fidèle* ssi le seul $g \in G$ stabilisant tous les éléments de X est l'élément neutre ;

— *libre* ssi tout élément de G différent du neutre agit sans point fixe.

6. Montrer que le groupe spécial orthogonal agit (par l'action que l'on devine) transitivement sur chaque sphère de $\mathbb{R}^n$. Cette action est-elle simplement transitive ?
7. On fait agir le groupe $\mathrm{GL}_2(\mathbb{R})$ sur les triplets de droites deux à deux distinctes de $\mathbb{R}^2$. Montrer que l'action est transitive.
8. Le groupe G agit sur lui-même par translation à gauche i.e. $g \cdot x = gx$. Décrire l'action. En déduire le théorème de Cayley : G est isomorphe à un sous-groupe de $\mathfrak{S}(G)$.

§ 3. Équation des classes, formule de Burnside

Dans la suite G fini opère sur X fini.

9. On note $G \cdot x_1, \dots, G \cdot x_r$ les orbites d'éléments de X sous l'action de G. Montrer la formule des classes
$$|X| = \sum_{i=1}^{r} |G \cdot x_i| = \sum_{i=1}^{r} [G : G_{x_i}].$$

10. On note $X^g = \{x \in X, g \cdot x = x\}$ (points fixes de g) et $\chi(g)$ son cardinal.
En dénombrant l'ensemble $\{(g, x) \in G \times X, g \cdot x = x\}$ de deux façons différentes, montrer la formule de Burnside
$$r = \frac{1}{|G|} \sum_{g \in G} \chi(g).$$

11. ($\star$) Soit p un nombre premier.
    (a) Soit $\Sigma = \{a, b\}$ l'alphabet à deux éléments. On fait agir $\mathbb{Z}/p\mathbb{Z}$ sur Σ^p par
    $$\overline{k} \cdot u_{\overline{1}} \cdots u_{\overline{p}} = u_{\overline{1+k}} \cdots u_{\overline{p+k}}. \qquad \text{(permutation cyclique des lettres)}$$
    Quelles sont les orbites possibles et leurs cardinaux ?
    (b) Soit A, B deux matrices de $\mathcal{M}_n(\mathbb{Z})$. Montrer que
    $$\operatorname{tr}(A + B)^p \equiv \operatorname{tr} A^p + \operatorname{tr} B^p \pmod{p}.$$
    (c) Montrer que pour tout $A \in \mathcal{M}_n(\mathbb{Z})$, $\operatorname{tr} A^p \equiv \operatorname{tr} A \pmod{p}$.

12. ($\star$) Un roi demande à son orfèvre de lui confectionner une couronne différente chaque année. Chaque couronne est un décagone régulier, et sur sa face avant, on dispose sur chaque sommet une pierre précieuse : un rubis, un saphir ou une émeraude.
Montrer que le nombre de combinaisons est
$$\sum_{d \mid 10} \varphi(d)\, 3^{10/d}.$$

§ 4. Le lemme de Cauchy

On donne ici la preuve classique du lemme de Cauchy à l'aide des actions de groupes.
Soit G un groupe fini de cardinal N, et soit p un diviseur premier de N.
On appelle ordre d'un élément g le cardinal du sous-groupe qu'il engendre.

13. On note d l'ordre de g. Montrer que $g^n = 0$ si et seulement si $d \mid n$.
14. Montrer que l'ordre d'un élément divise le cardinal du groupe.

Le lemme de Cauchy fournit une réciproque partielle à ce résultat.

15. Calculer le cardinal de $E = \{(g_1, \dots, g_p) \in G^n \mid g_1 \cdots g_n = e\}$.
16. Montrer qu'on peut faire agir le grand cycle $(1\ 2\ \cdots\ p)$ sur E.
17. Combien peut-il y avoir d'orbites de cardinal 1 ? En déduire le lemme de Cauchy : il existe un élément d'ordre p dans G.

§ 5. Dévissage de $\mathrm{Sim}(\mathbb{C})$

On note $\mathrm{Sim}(\mathbb{C})$ l'ensemble des similitudes directes ($z \mapsto az + b$) ou indirectes ($z \mapsto a\overline{z} + b$) du plan complexe.

18. Montrer que $\mathrm{Sim}(\mathbb{C})$ est un groupe.

On rappelle qu'un sous-groupe H est distingué dans G si, et seulement si pour tout $g \in G, gH = Hg$. Dans ce cas, le quotient G/H est un groupe. On note alors $H \triangleleft G$.

On note $\mathrm{Iso}(\mathbb{C})$ l'ensemble des isométries (au sens réel) du plan complexe, $\mathrm{Iso}^+(\mathbb{C})$ l'ensemble des isométries directes, on identifie $\mathbb{C}$ à l'ensemble des translations.

19. Montrer que le stabilisateur de tout point $z \in \mathbb{C}$ pour l'action de $\mathrm{Iso}^+(\mathbb{C})$ est isomorphe à $SO_2(\mathbb{R})$. Expliquer géométriquement (c'est le principe d'un compas).
20. Montrer qu'on a la suite de composition suivante :

$$\{\mathrm{id}\} \triangleleft \mathbb{C} \triangleleft \mathrm{Iso}^+(\mathbb{C}) \triangleleft \mathrm{Iso}(\mathbb{C}) \triangleleft \mathrm{Sim}(\mathbb{C}).$$

21. Montrer que les quotients sont abéliens, les identifier avec des groupes bien connus, et leur associer des invariants géométriques bien connus.

On dit alors que $\mathrm{Sim}(\mathbb{C})$ est résoluble.