Chapitre 4

Le groupe symétrique et son dévissage

Le but de ce chapitre est d'étudier la structure du groupe symétrique S_n. Ce dernier agit naturellement sur $\{1, \ldots, n\}$ mais aussi sur tout un tas d'autres ensembles naturels. Cela nous conduit naturellement à discuter d'abord la notion d'action de groupe, qui de toutes façons est l'une des notions essentielles de ce cours. Au passage, en guise de première illustration de l'action de conjuguaison, nous démontrons le premier théorème de Sylow, mais nous reportons à plus tard les autres applications dans le même esprit à la structure des groupes finis.

Nous étudions ensuite S_n de manière systématique (systèmes de générateurs, classes de conjugaison), ainsi que son groupe alterné A_n. Les cas des petites valeurs de n est à la fois irrégulier et intéressant. C'est pourquoi nous dévisserons d'abord concrètement S_n pour $n \leqslant 4$, puis étudierons l'action *exotique* de S_5 sur $\{1, 2, 3, 4, 5, 6\}$. Nous introduirons ensuite le langage des suites exactes, agréable pour décrire les dévissages. Nous dévisserons ensuite S_n pour $n \geqslant 5$. Un énoncé crucial, connu de Galois, est la simplicité du groupe non abélien A_n.

Ces dévissages seront l'occasion d'introduire certains concepts importants, comme les notions de *commutateurs*, *groupes dérivés* et *résolubilité*. Le groupe S_n est résoluble si, et seulement si, on a $n \leqslant 4$, un énoncé particulièrement significatif en théorie de Galois, brièvement discutée dans un complément culturel. Nous expliquerons enfin la notion de *produit semi-direct*, que nous appliquerons ici aux structures de S_3 et S_4, ainsi qu'à la classification de groupes de petit ordre.

Nous terminerons par deux autres compléments importants : l'un sur la notion de filtration, avec notamment une démonstration du théorème de Jordan-Hölder et la détermination des facteurs de Jordan-Hölder de S_n, et l'autre sur la classification par Galois des sous-groupes résolubles et transitifs de S_p avec p premier.

1. Actions de groupes

1.1. Définition. Dans cette partie, on fixe un groupe G et un ensemble X.

Définition 1.1. *Une action de G sur X est une application*

$$\bullet : G \times X \to X, \ \ (g, x) \mapsto g \bullet x,$$

vérifiant $1 \bullet x = x$ et $g \bullet (h \bullet x) = (gh) \bullet x$ pour tout $x \in X$ et tout $g, h \in G$.

On notera en général simplement $g.x$ ou gx au lieu de $g \bullet x$. Un ensemble muni d'une action de G est aussi appelé G-ensemble. La plupart des groupes rencontrés agissent naturellement sur quelque chose !

Exemple 1.2. *(i) L'exemple canonique d'action est celle du groupe symétrique S_X sur X définie par $\mathrm{S}_X \times X \to X$, $(\sigma, x) \mapsto \sigma(x)$. Le groupe S_X agit aussi naturellement $\mathrm{P}(X)$ via $(\sigma, A) \mapsto \sigma(A)$, sur l'ensemble produit*

$X \times X$ via $(\sigma,(x,y)) \mapsto (\sigma(x),\sigma(y))$, sur l'ensemble des partitions de X via $(\sigma,\{P_i\}_{i\in I}) \mapsto \{\sigma(P_i)\}_{i\in I}$, etc...

(iii) Si V est un k-espace vectoriel, alors $\mathrm{GL}(V)$ agit naturellement sur V, sur l'ensemble $\mathbb{P}(V)$ des droites de V, sur l'ensemble des plans de V, etc..

(iv) Noter que si G agit sur X, il agit aussi naturellement sur tout sous-ensemble $Y \subset X$ qui est stable, i.e. tel que $gY \subset Y$ pour tout $g \in G$.

(v) Si G agit sur X, et si $f : H \to G$ est un morphisme de groupes, alors $H \times X \to X, (h,x) \mapsto f(h)x$, est une action de H sur X, dite déduite de celle de G par restriction selon f.

En particulier, tout morphisme $f : G \to \mathrm{S}_X$ définit par (i) et (v), *i.e.* $(g,x) \mapsto f(g)(x)$, une action de G sur X. Nous allons voir que toute action de G sur X s'obtient ainsi. En effet, fixons une action $\bullet$ de G sur X, et pour $g \in G$, regardons

$$\mathrm{m}_g : X \to X, x \mapsto g \bullet x$$

(la *translation par g* associée à $\bullet$). Par hypothèse, on a $\mathrm{m}_1 = \mathrm{id}_X$, et $\mathrm{m}_g \circ \mathrm{m}_h = \mathrm{m}_{gh}$. Ainsi, m_g est inversible d'inverse $\mathrm{m}_{g^{-1}}$, et l'application $\mathrm{m}^\bullet : G \to \mathrm{S}_X, g \mapsto \mathrm{m}_g$, est un morphisme de groupes, appelé *morphisme associé à l'action* $\bullet$. Les deux constructions ci-dessus étant clairement inverses l'une de l'autre, on a montré :

Scholie 1.3. (*Propriété universelle de S_X*) *L'application $\bullet \mapsto \mathrm{m}^\bullet$ induit une bijection de l'ensemble des actions de G sur X sur celui des morphismes $G \to \mathrm{S}_X$.*

On passera en général d'un point de vue à l'autre sans commentaire.

Exemple 1.4. *(i) Se donner une action de G sur $\{1,\dots,n\}$ est la même chose que se donner un morphisme $G \to \mathrm{S}_n$.*

(ii) (Action de Cayley) *La multiplication de G définit une action de G sur lui-même, et correspond au morphisme $G \to \mathrm{S}_G$ de Cayley.*

(iii) (Action triviale) *Tout groupe G agit trivialement sur tout ensemble X en posant $g.x = x$ pour tout $g \in G$ et tout $x \in X$. C'est l'action correspondant au morphisme triviale $G \to \mathrm{S}_X$, $g \mapsto 1$. Cette action est moins inutile*[1] *qu'elle n'en a l'air !*

Remarque 1.5. *(Action à droite)* La notion d'action donnée ici est appelée parfois *action à gauche* de G sur X. La notion concurrente est celle d'*action à droite*, qui est une application $X \times G \to X, (x,g) \mapsto xg$ vérifiant $x1 = x$ et $(xg)h = x(gh)$ pour tout $x \in X$ et tout $g,h \in G$. En fait, si G agit à droite sur X, il y agit aussi à gauche par la formule $(g,x) \mapsto xg^{-1}$, (et réciproquement !) de sorte que la théorie des actions à droite se déduit de celle des actions à gauche. Pour cette raison, on ne considèrera que des actions à gauche dans ce cours.

1.2. Orbites et stabilisateurs.

Définition 1.6. *Soient G un groupe agissant sur l'ensemble X et $x \in X$.*

(i) Le sous-ensemble $\mathrm{O}_x = \{gx \mid g \in G\} \subset X$ est appelé orbite *de x sous (l'action de) G.*

1. L'intérêt typique d'une telle notion est que l'on peut avoir à démontrer qu'une action donnée est l'action triviale.

(ii) Le sous-groupe $G_x = \{g \in G \mid gx = x\}$ *de* G *est appelé* stabilisateur *de* x *(ou* groupe d'isotropie *de* x*). On le note aussi* $\mathrm{Stab}_G(x)$.

Dans le (ii) ci-dessus, le fait que G_x est un sous-groupe de G est immédiat.

EXEMPLE 1.7. *(i) Soit* E *un plan euclidien et* $G = \mathrm{O}(E)$ *son groupe orthogonal. L'action naturelle de* G *sur* E *a pour orbites le cercles centrés en l'origine* O*. Le stabilisateur d'un point* $P \neq 0$ *est le groupe d'ordre* 2 *engendré par la symétrie axiale d'axe* (OP).

(ii) Si k *est un corps, le groupe* $\mathrm{GL}_n(k)$ *agit par conjugaison sur* $\mathrm{M}_n(k)$*, via* $(g, M) \mapsto gMg^{-1}$*. L'orbite d'une matrice* $M \in \mathrm{M}_n(k)$ *est sa classe de conjugaison/de similitude, le stabilisateur de* M *est son commutant dans* $\mathrm{GL}_n(k)$.

La propriété suivante est élémentaire mais importante (*principe de conjugaison*) :

LEMME 1.8. *Soient* G *agissant sur* X*,* $x \in X$ *et* $g \in G$*. On a* $G_{gx} = gG_xg^{-1}$.

DÉMONSTRATION — En effet, pour tout $h \in G$ on a

$$h \in G_{gx} \iff hgx = gx \iff g^{-1}hgx = x \iff g^{-1}hg \in G_x \iff h \in gG_xg^{-1}.$$

□

Soit G agissant sur X. À cette action est associée la relation R sur X définie par

$$y \, R \, x \iff \exists g \in G,\ y = gx.$$

C'est une relation d'équivalence. En effet, on a $x = 1x$ (reflexivité), $y = gx \Leftrightarrow x = g^{-1}y$ (symétrie), et enfin $y = gx$ et $z = hy$ entraînent $z = ghx$ (transitivité). La classe d'équivalence d'un point $x \in X$ est son orbite O_x. L'ensemble quotient X/R, sous-ensemble de $\mathrm{P}(X)$ constitué des orbites sous G, est parfois noté $G\backslash X$. Les classes d'équivalence formant une partition de X on a montré :

PROPOSITION 1.9. *Si* G *agit sur* X*, les orbites forment une partition de* X.

EXEMPLE 1.10. Se donner une action de $\mathbb{Z}$ sur X est la même chose que se donner une bijection de X. En effet, se donner un morphisme $\mathbb{Z} \to \mathrm{S}_X$ revient à se donner l'image de 1, un élément *a priori* quelconque de S_X. De même, se donner une action de $\mathbb{Z}/n\mathbb{Z}$ sur X est la même chose que se donner $\sigma \in \mathrm{S}_X$ tel que $\sigma^n = \mathrm{id}_X$. La relation ci-dessus, dans le cas de ces actions, n'est autre que la relation d'équivalence de l'Exemple 1.8 Chap. 1.

Un des énoncés les plus importants sur les actions de groupes est le suivant.

PROPOSITION 1.11. (Formule orbite-stabilisateur) *Soit* G *un groupe agissant sur l'ensemble* X*, et soit* $x \in X$*. On a une bijection* $G/G_x \xrightarrow{\sim} \mathrm{O}_x$ *envoyant* gG_x *sur* gx *pour tout* $g \in G$*. En particulier, si* G *est fini on a* $|G| = |G_x||\mathrm{O}_x|$.

DÉMONSTRATION — Soi $\pi : G \to \mathrm{O}_x, g \mapsto gx$. Par définition, π est surjective et on a

$$\pi(g') = \pi(g) \iff g'x = gx \iff g^{-1}g' \in G_x \iff g' \sim_{G_x} g.$$

Cela montre que π passe au quotient G/G_x, et aussi que l'application induite $\overline{\pi} : G/G_x \to \mathrm{O}_x, gG_x \mapsto gx$, est injective, donc bijective. Le dernier point résulte de $|G/G_x| = |G|/|G_x|$ (Lagrange). □

COROLLAIRE 1.12. (Équation aux classes) *On suppose X et G finis, et se donne $x_1, \dots, x_n \in X$ des représentants des orbites sous G. On a*

$$|X| = \sum_{i=1}^{n} |\mathrm{O}_{x_i}| = \sum_{i=1}^{n} |G|/|G_{x_i}|.$$

1.3. Un exemple : l'action de conjugaison. Nous verrons de nombreux exemples concrets d'actions de groupes par la suite. L'exemple suivant est aussi général qu'important.

EXEMPLE 1.13. (*Action de conjugaison*) Soit G un groupe. L'application $G \times G \to G, (g, x) \mapsto gxg^{-1}$ est manifestement une action de G sur lui-même appelée *action de conjugaison*. Pour cette action, l'orbite d'un élément $x \in G$ est appelée *classe de conjugaison* de x, et notée $\mathrm{Conj}(x) = \{gxg^{-1} \mid g \in G\}$. De plus, le stabilisateur de x est appelé *centralisateur* ou *commutant* de x, et il est noté $\mathrm{C}_G(x) = \{g \in G \mid gx = xg\}$. On a $\langle x \rangle \subset \mathrm{C}_G(x)$ (inclusion stricte en générale).

Donnons-en ici une application typique. Notons que pour $x \in G$, on a $|\mathrm{Conj}(x)| = 1$ si, et seulement si, $x \in \mathrm{Z}(G)$. Supposons G fini et choisissons $x_1, \dots, x_n \in G \smallsetminus \mathrm{Z}(G)$ des représentants des classes de conjugaison non triviales de G. On a alors

$$|G| = |\mathrm{Z}(G)| + \sum_{i=1}^{n} |\mathrm{Conj}(x_i)|, \text{ avec } |\mathrm{Conj}(x_i)|\,|\mathrm{C}_G(x_i)| = |G|, \tag{20}$$

d'après l'équation aux classes. Cette égalité permet par exemple de montrer le :

THÉORÈME 1.14. (Premier théorème de Sylow) *Soit G un groupe fini d'ordre $p^n m$ avec p premier ne divisant pas m. Alors G possède un sous-groupe d'ordre p^n.*

Un tel sous-groupe s'appelle un p-Sylow de G.

DÉMONSTRATION — On raisonne par récurrence sur $|G|$. Supposons qu'il existe $x \in G \smallsetminus \mathrm{Z}(G)$ tel que $|\mathrm{Conj}(x)|$ est premier à p. Dans ce cas $H = \mathrm{C}_G(x)$ est un sous-groupe de G d'indice premier à p, donc de la forme $p^n m'$ avec $m' | m$ et $m' < m$ (Lagrange). Par hypothèse de récurrence, H a un sous-groupe d'ordre p^n, ainsi donc que G. On peut donc supposer $p \mid |\mathrm{Conj}(x)|$ pour tout $x \in G \smallsetminus \mathrm{Z}(G)$. Par l'équation aux classes (20) on a alors $p \mid |\mathrm{Z}(G)|$. Choisissons $x \in \mathrm{Z}(G)$ d'ordre p (par exemple par Cauchy, mais c'est plus élémentaire ici car G est abélien). Alors $H = \langle x \rangle$ est d'ordre p et distingué dans G. Par hypothèse de récurrence, le groupe quotient G/H a un sous-groupe d'ordre p^{n-1}. Il est donc de la forme P/H, avec P sous-groupe de G contenant H, et on a $|P| = |P/H||H| = p^n$. □

Nous poursuivrons ce type d'applications théoriques à la structure générale des groupes finis au Chapitre 6.

1.4. Vocabulaire : actions transitives, fidèles et libres.

DÉFINITION 1.15. *Une action de G sur X est dite* transitive *si on a $X \neq \varnothing$ et si pour tout $x, y \in X$ il existe $g \in G$ tel que $y = gx$. Il est équivalent de demander qu'il existe $x \in X$ avec $X = \mathrm{O}_x$.*

EXEMPLE 1.16. (i) Pour tout $1 \leqslant k \leqslant n$, l'action naturelle de S_n sur l'ensemble des parties à k éléments de $\{1, \dots, n\}$ est transitive.

(ii) L'action naturelle de $\mathrm{GL}(V)$ sur V n'est pas transitive pour $V \neq \{0\}$. Elle a exactement deux orbites : celle de 0 et celle d'un vecteur non nul quelconque.

Un exemple aussi important que général d'action transitive est le suivant.

EXEMPLE 1.17. *(Action par translations de G sur G/H)* Supposons que l'on ait un groupe G et H un sous-groupe de G. Alors la multiplication des parties dans G induit une action de G sur G/H

$$G \times G/H \to G/H, (g, xH) \mapsto gxH,$$

appelée action par translations de G sur G/H. Cette action est clairement transitive car l'orbite de H sous G est G/H. De plus, le stabilisateur de l'élément $H \in G/H$ dans G est par définition $\{g \in G \mid gH = H\} = H$. Le stabilisateur dans G de l'élément $xH \in G/H$ est xHx^{-1} par le principe de conjugaison.

Étant donné un sous-groupe arbitraire H de G, on a donc construit une action transitive de G sur un ensemble (à savoir G/H) dont H est un stabilisateur.

DÉFINITION 1.18. *Le noyau d'une action donnée de G sur X est le sous-groupe*

$$\cap_{x \in X} G_x = \{g \in G |\ gx = x \quad \forall x \in X\}$$

de G. Autrement dit, c'est le noyau du morphisme $G \to \mathrm{S}_X$ associé à l'action. C'est donc un sous-groupe distingué de G. Une action est dite fidèle *si son noyau est $\{1\}$, i.e. si le morphisme associé $G \to \mathrm{S}_X$ est injectif.*

EXEMPLE 1.19. (i) Le noyau de l'action de conjugaison de G sur lui-même est $\mathrm{Z}(G)$. Pour l'action par translations de G sur G/H, c'est $\cap_{g \in G} gHg^{-1}$.

(ii) Le noyau de l'action naturelle de $\mathrm{GL}(V)$ sur $\mathbb{P}(V)$ est le sous-groupe $k^\times$ des homothéties de V.

(iii) L'action la moins fidèle possible est l'action triviale, dont le noyau est G.

DÉFINITION 1.20. *Une action de G sur X est dite libre si on a $G_x = \{1\}$ pour tout $x \in X$.*

Les orbites d'une action libre de G sont donc en bijection avec G. Il ne faut pas confondre libre et fidèle : une action libre est fidèle, mais la réciproque est (très) fausse.

EXEMPLE 1.21. (i) L'action de Cayley est libre.

(ii) L'action naturelle de S_n sur $\{1, \ldots, n\}$ est fidèle, mais pas libre pour $n > 2$.

1.5. Classification des actions d'un groupe donné. Comme pour la notion d'isomorphisme entre groupes, la notion naturelle d'isomorphismes entre actions de G est la suivante.

DÉFINITION 1.22. *Soient $(X, \bullet)$ et $(Y, \star)$ deux actions d'un même groupe G. Un* isomorphisme *de $(X, \bullet)$ vers $(Y, \star)$ est une bijection $f : X \to Y$ vérifiant $f(g \bullet x) = g \star f(x)$ pour tout $g \in G$ et $x \in X$. On dit que $(X, \bullet)$ et $(Y, \star)$ sont* isomorphes*, et on note $(X, \bullet) \simeq (Y, \star)$, s'il existe un isomorphisme de l'une vers l'autre.*

On constate que l'identité définit un isomorphisme entre $(X, \bullet)$ et lui-même, que l'inverse d'un isomorphisme est un isomorphisme, et que les isomorphismes entre actions se composent quand cela a un sens : la notion d'isomorphisme entre actions est une relation d'équivalence ! Nous allons restreindre notre étude aux actions transitives. C'est en fait le cas important, et nous renvoyons aux exercices pour voir comment le cas général s'en déduit (Exercice 4.27) et pour de nombreux exemples.

PROPOSITION 1.23. *Soient $(X, \bullet)$ une action transitive de G et $x \in X$. Alors $(X, \bullet)$ est isomorphe à l'action par translations de G sur G/G_x.*

DÉMONSTRATION — On a $X = \mathrm{O}_x$ par transitivité. Par le (ii) de la Proposition 1.11, on a une bijection $f : G/G_x \xrightarrow{\sim} X$ envoyant gG_x sur $g \bullet x$ pour tout $g \in G$. C'est un isomorphisme d'actions : pour $h, g \in G$ on a $f(hgG_x) = hg \bullet x = h \bullet f(gG_x)$. □

Le groupe G agit par conjugaison $(g, H) \mapsto gHg^{-1}$ sur l'ensemble de ses sous-groupes. L'orbite d'un sous-groupe H pour cette action, appelée *classe de conjugaison* de H, est alors $\mathrm{Conj}_G(H) := \{gHg^{-1} \mid g \in G\}$. Ceci étant dit, supposons donnée une action transitive $(X, \bullet)$ de G. Observons que les stabilisateurs associés G_x, avec $x \in X$, forment une classe de conjugaison de sous-groupes de G. En effet, par le principe de conjugaison on a $G_{g \bullet x} = gG_xg^{-1}$ pour tout $x \in X$ et tout $g \in G$, et pour x donné tout $y \in X$ est de la forme $g \bullet x$ pour un g bien choisi par transitivité. On note $\mathrm{Stab}(X, \bullet)$ cette classe de conjugaison de sous-groupes de G associé à $\bullet$.

PROPOSITION 1.24. *Deux actions transitives $(X, \bullet)$ et $(Y, \star)$ d'un même groupe G sont isomorphes si, et seulement si, on a $\mathrm{Stab}(X, \bullet) = \mathrm{Stab}(Y, \star)$.*

DÉMONSTRATION — Soit $f : X \to Y$ un isomorphisme entre $(X, \bullet)$ et $(Y, \star)$. Pour $x \in X$ et $g \in G$, $g \bullet x = x \iff f(g \bullet x) = f(x) \iff g \star f(x) = f(x)$ par injectivité de f. On a donc $G_x = G_{f(x)}$, puis $\mathrm{Stab}(X, \bullet) = \mathrm{Stab}(Y, \star)$. Supposons réciproquement $\mathrm{Stab}(X, \bullet) = \mathrm{Stab}(Y, \star)$. Il existe $x \in X$ et $y \in Y$ avec $H := G_x = G_y$. Par la Proposition 1.23, on a alors $(X, \bullet) \simeq (G/H, \text{translations}) \simeq (Y, \star)$. □

SCHOLIE 1.25. *Il est équivalent de se donner une classe d'isomorphisme d'actions transitives de G sur un ensemble à n éléments, et de se donner une classe de conjugaison de sous-groupes d'indice n de G.*

REMARQUE 1.26. (Transport de structure) Si G agit sur X et si $\varphi : Y \to X$ est une bijection. Il existe une unique action de G sur Y telle que φ soit un isomorphisme d'actions. Par exemple, si X est fini à n éléments, et si $\varphi : \{1, \ldots, n\} \xrightarrow{\sim} X$ est une numérotation des éléments de X, on en déduit une action de G sur $\{1, \ldots, n\}$ isomorphe à celle sur X.

2. Groupes symétrique et alterné

On rappelle que pour $n \geqslant 1$, S_n désigne le groupe des bijections, aussi appellées *permutations*, de l'ensemble $\{1, \ldots, n\}$. C'est un groupe d'ordre $n!$. Un élément σ de S_n est parfois noté sous la forme de la matrice $2 \times n$

$$\sigma = \begin{pmatrix} 1 & 2 & \cdots & n \\ \sigma(1) & \sigma(2) & \cdots & \sigma(n) \end{pmatrix}.$$