1. Soit E un ensemble. On note $\mathrm{S}(E)$ l'ensemble des bijections de E dans E. C'est un groupe pour la composition des applications. Si E est l'ensemble $\{1,\dots,n\}$ on note aussi S_n le groupe $\mathrm{S}(E)$ et on l'appelle le groupe symétrique.

Exemple :

- $E=\emptyset$ (!) alors il y a une seule application $E\to E$ et c'est une bijection (conformément à la définition d'une application, d'une bijection). $\mathrm{S}(E)$ est donc le groupe trivial formé d'un seul élément.
- E est formé d'un seul élément. A nouveau il y a une seule application $E\to E$ et c'est une bijection, donc $\mathrm{S}(E)$ est donc le groupe trivial.
- E est formé de deux éléments distincts : $E=\{a,b\}$. Il y a deux bijections $E\to E$: l'identité et l'application qui échange a et b. Cette dernière est une involution (sa composée avec elle-même est l'identité) d'où $\mathrm{S}(E)\cong\mathbb{Z}/2\mathbb{Z}$.

Exercice : $\mathrm{S}(E)$ n'est pas commutatif dès que le cardinal de E est strictement supérieur à 2.

Si $f:E\to E'$ est une bijection alors l'application $\mathrm{S}(E)\to\mathrm{S}(E')$, $\sigma\mapsto f\sigma f^{-1}$ est un isomorphisme de groupes.

Proposition. S_n est un ensemble fini de cardinal $n!$.

La démonstration de la proposition est un exercice classique de dénombrement (soigner la rédaction !). Supposons $n\geq 2$. On considère l'application $\mathrm{S}_n\to\{1,\dots,n\}$, $\sigma\mapsto\sigma(n)$. L'image réciproque d'un élément k de $\{1,\dots,n\}$ s'identifie à l'ensemble des bijections de $\{1,\dots,n-1\}$ dans $\{1,\dots,n\}\backslash\{k\}$, lequel est en bijection avec S_{n-1}. Comme S_n est la réunion disjointe des images réciproques des éléments de $\{1,\dots,n\}$, on obtient $|\mathrm{S}_n|=n|\mathrm{S}_{n-1}|$. La relation de récurrence obtenue est exactement celle définissant S_n.

2. Une action d'un groupe G sur un ensemble E est une application $G\times E\to E$ vérifiant les axiomes habituels. La donnée d'une action de G sur E équivaut à la donnée d'un morphisme de groupe $G\to\mathrm{S}(E)$. (Noter la précaution de langage : une application $G\times E\to E$ n'est pas une application $G\to\mathrm{S}(E)$. Il faut choisir une définition.) Voici deux exemples :

- Il y a une action canonique de $\mathrm{S}(E)$ sur E correspondant à l'identité de $\mathrm{S}(E)$ dans lui même : c'est l'application $\mathrm{S}(E)\times E\to E$, $(\sigma,x)\mapsto\sigma(x)$.
- Un groupe G opère sur lui même par translation à gauche ($(g,x)\mapsto gx$). Cette action correspond à un morphisme de groupes $G\to\mathrm{S}(G)$. On vérifie que ce morphisme est injectif (on dit alors que l'action est fidèle).

Si E à une structure d'espace vectoriel sur un corps k, on a une inclusion du groupe $\mathrm{GL}(E)$ des isomorphismes linéaires $E\to E$ dans $\mathrm{S}(E)$. Une action linéaire de G sur E correspond alors à un morphisme de groupes de G dans $\mathrm{GL}(E)$.

On peut aussi dans ce contexte parler de l'algèbre du groupe G notée $k[G]$ et vérifier qu'une action linéaire de G sur E équivaut à la donnée d'une structure de $k[G]$-module sur E. Pour un approfondissement de ce sujet (qui n'est pas explicitement au programme) voir [Elk].

3. Eléments remarquables de S_n : cycles

Un cycle de S_n est une permutation σ telle qu'on peut écrire l'ensemble $\{1,\dots,n\}$ comme réunion disjointe de deux parties A et B avec

- A et B sont stables par σ ($\sigma(A)\subset A$ et $\sigma(B)\subset B$) ;
- La restriction de σ à A est l'identité ;
- Il existe un élément $b\in B$ tel que tout élément de B soit une image itérée de b par σ.

Si σ est un cycle distinct de l'identité, la partie A est alors l'ensemble des points fixes de σ, c'est-à-dire l'ensemble $\{x, \sigma(x) = x\}$, et B est le complémentaire de A dans $\{1, \ldots, n\}$. On appelle B le support de σ Tout élément de B satisfait la troisième propriété ci-dessus (exercice !).

Soient σ un cycle ayant exactement $n - k$ points fixes ($k > 1$). La partie B est égale à l'ensemble $\{b, \sigma(b), \ldots, \sigma^{k-1}(b)\}$. On note σ par $(b, \sigma(b), \ldots, \sigma^{k-1}(b))$. L'entier k est l'ordre du sous-groupe de S_n engendré par σ, c'est à dire le plus petit entier strictement positif tel que σ^k soit l'identité. On l'appelle longueur du cycle σ.

Exemples.

- Soit σ un élément de S_n ayant exactement $n - 2$ points fixes ; alors σ est un cycle de longueur 2. On appelle σ une transposition.
- Dans S_4 les cycles $(1, 3, 4)$, $(3, 4, 1)$, $(4, 1, 3)$ sont égaux.

Observons que tout cycle de S_n se prolonge de façon unique en un cycle de S_{n+1}.

Proposition.

(a) Soient σ, τ deux cycles de supports disjoints ; alors $\sigma\tau = \tau\sigma$.

(b) Soit σ un cycle de longueur k : $\sigma = (a, \sigma(a), \ldots, \sigma^{k-1}(a))$ pour un $a \in \{1, \ldots, n\}$. Soit τ une permutation quelconque de $\{1, \ldots, n\}$. Alors $\tau\sigma\tau^{-1}$ (le conjugué de σ par τ) est le cycle $(\tau(a), \tau(\sigma(a)), \ldots, \tau(\sigma^{k-1}(a)))$.

(c) Toute permutation s'écrit comme un produit de cycles de supports disjoints.

Le point (c) de la proposition se montre en considérant la restriction de l'action canonique de S_n sur l'ensemble $\{1, \ldots, n\}$ au sous-groupe engendré par la permutation σ : il s'agit de l'application $(\sigma^k, x) \mapsto \sigma^k(x)$. L'ensemble $\{1, \ldots, n\}$ s'écrit comme la réunion disjointe des orbites pour cette action. La restriction de σ à chaque orbite est un cycle de longueur le cardinal de l'orbite, lequel se prolonge de façon unique en un cycle de $\{1, \ldots, n\}$, et σ est le produit de ces cycles.

Exercice . Comment peut on caractériser la classe de conjugaison d'un élément de S_n en terme de sa décomposition en produit de cycles disjoints ?

Générateurs de S_n

C'est par leur description qu'on répond aux questions des deux prochaines sections. On observe que S_n est engendré comme groupe par les transpositions $(i, i+1)$, i décrivant $\{1, \ldots, n-1\}$. On peut le montrer par récurrence sur n : Si $\sigma \in \mathrm{S}_n$ vérifie $\sigma(n) = n$ alors σ est dans l'image de l'inclusion $\mathrm{S}_{n-1} \subset \mathrm{S}_n$. Sinon la composé de σ avec la transposition $(\sigma(n), n)$ fixe n...

4. Sous-groupes distingués de S_n

Tout sous-groupe distingué d'un groupe G s'interprète comme le noyau d'un morphisme de groupes de source G. On connait un (et un seul) morphisme non trivial de S_n dans $\{\pm 1\} \cong \mathbb{Z}/2$: la signature qu'on note ϵ. Son noyau s'appelle le groupe alterné $\mathcal{A}_n$.

Le morphisme ϵ est caractérisé par le fait que l'image d'une transposition vaut -1 mais il faut vérifier que ceci est bien compatible avec la composition (S_n n'est pas librement engendré par les transpositions : il y a des relations). On peut aussi définir ϵ par $\epsilon(\sigma) = \prod_{(i,j)\in\{1,\ldots,n\}^2, i<j \text{ et } \sigma(i)>\sigma(j)} (-1)$ et il faut alors montrer que ϵ est un morphisme de groupe.

Proposition. Pour $n \geq 5$ les seuls sous-groupes distingués de S_n sont $\{1\}$, $\mathcal{A}_n$ et $\mathcal{S}_n$.

Voir [Pe, chap I, §8] pour une démonstration.

5. Automorphismes de S_n

On note $\mathrm{Aut}(\mathrm{S}_n)$ l'ensemble des morphismes de groupes bijectifs $\mathrm{S}_n \to \mathrm{S}_n$. C'est un groupe pour la composition des applications. On dispose d'une application $\mathrm{S}_n \to \mathrm{Aut}(\mathrm{S}_n)$, $\sigma \mapsto (\tau \mapsto \sigma\tau\sigma^{-1})$ qui est triviale si $n \leq 2$ mais injective si $n \geq 3$ (pourquoi ?). On appelle automorphisme intérieur tout élément de l'image de cette application.

PROPOSITION. Pour $n \neq 6$ tout automorphisme de S_n est intérieur.

A nouveau on renvoie à [PE, chap I, §8] pour une démonstration.

6. Hors programme :

La description des représentations linéaires de $\mathcal{S}_n$.

7. Références

[AD1] J. F. ADAMS, *Stable Homotopy and Generalized Homology*, University of Chicago Press, 1974.

[ELK] R. ELKIK, *Cours d'algèbre*, Ellipse 2002.

[PE] D. PERRIN, *Cours d'algèbre*, Ellipse 1996.