Groupe des permutations d'un ensemble fini. Applications.

Par Nicolas Lanchier [1]

1 Groupe symétrique.

Définition 1.1 — On appelle groupe symétrique d'indice n le groupe, noté $\mathfrak{S}_n$, des permutations de $E = \{ 1, 2, \dots n \}$.

Proposition 1.2 — Le groupe $\mathfrak{S}_n$ est d'ordre $n!$

Théorème 1.3 (Cayley) — Si G est un groupe fini de cardinal n alors G est isomorphe à un sous-groupe du groupe symétrique $\mathfrak{S}_n$. [6], Sect. 1.4

Définition 1.4 — On appelle cycle d'ordre k toute permutation $\sigma = (a_1, a_2, \dots a_k) \in \mathfrak{S}_n$, telle que pour tout $1 \leq i \leq k$, $\sigma(a_i) = a_{i+1}$, l'indice étant pris modulo k, et telle que pour tout $a \notin \{ a_1, a_2, \dots a_k \}$, $\sigma(a) = a$. [6], Sect. 1.0

Définition 1.5 — On appelle transposition tout cycle d'ordre $k = 2$. [6], Sect. 1.0

Théorème 1.6 — Toute permutation $\sigma \in \mathfrak{S}_n$ se décompose de façon unique en produit de cycles disjoints, le nombre de ces cycles étant égal au nombre de σ-orbites distinctes dans E. [6], Sect. 1.4

Application 1.7 — Le nombre N de façons de colorier un cube avec k couleurs distinctes est donné par

$$N \ = \ \frac{1}{24} \ (k^6 + 3k^4 + 12k^3 + 8k^2)$$

[5], Sect. 4.3

Théorème 1.8 — Le groupe $\mathfrak{S}_n$ est engendré par les transpositions. [6], Sect. 1.1

2 Groupe alterné.

Définition 2.1 — On appelle signature l'application $\varepsilon : \mathfrak{S}_n \longrightarrow \{ -1 , +1 \}$ définie par $\varepsilon(\sigma) = (-1)^{n-k}$ où k désigne le nombre de σ-orbites dans E. [1], Sect. 3.2

Définition 2.2 — Une permutation σ est dite paire si $\varepsilon(\sigma) = 1$, impaire sinon.

Proposition 2.3 — Si σ est un cycle d'ordre k alors $\varepsilon(\sigma) = (-1)^{k+1}$. En particulier, si τ est une transposition $\varepsilon(\tau) = -1$.

Proposition 2.4 — Pour tout $\sigma \in \mathfrak{S}_n$

$$\varepsilon(\sigma) \ = \ \prod_{1 \leq i < j \leq n} \frac{\sigma(j) - \sigma(i)}{j - i}$$

[4], Sect. 1.2

Définition 2.5 — On appelle groupe alterné d'indice n le groupe, noté $\mathfrak{A}_n$, des permutations paires, i.e. $\mathfrak{A}_n = \mathrm{Ker}(\varepsilon)$. [6], Sect. 1.0

Théorème 2.6 — Pour $n \geq 3$, les 3-cycles engendrent $\mathfrak{A}_n$. [6], Sect. 1.1

Théorème 2.7 — Pour $n \geq 5$, le groupe alterné $\mathfrak{A}_n$ est simple, i.e. n'admet pas de sous-groupe distingué non trivial. [6], Sect. 1.8

3 Application à la théorie de Galois.

Définition 3.1 — Le groupe de Galois d'une extension de corps $K \subset L$ est le groupe, noté $\mathrm{Gal}(L|K)$, des K-automorphismes de L, i.e. des automorphismes $\sigma : L \longrightarrow L$ tels que pour tout $x \in K$, $\sigma(x) = x$. [2], Sect. 8.5

Définition 3.2 — Le groupe de Galois d'un polynôme $P \in K[X]$ est, par définition, le groupe $\mathrm{Gal}(L|K)$ où L est le corps de décomposition de P sur K. [2], Sect. 8.5

Proposition 3.3 — Soient $P \in K[X]$ un polynôme, G son groupe de Galois et E l'ensemble de ses racines. Alors G s'identifie à un sous-groupe du groupe $\mathfrak{S}(E)$ des permutations de E. [3], Ex 4.16

Définition 3.4 — Un groupe fini G est dit résoluble s'il existe une suite finie G_0, $G_1 \dots G_r$ de sous-groupes de G, appelée suite de résolubilité, telle que

1. $\{e\} = G_r \subset G_{r-1} \subset \cdots \subset G_0 = G$;
2. G_{i+1} est distingué dans G_i pour tout $0 \leq i \leq r-1$;
3. G_i/G_{i+1} est un groupe commutatif pour tout $0 \leq i \leq r-1$.

De façon équivalente, un groupe G est résoluble s'il existe un entier s tel que $D^s(G) = \{e\}$, où $D(G)$ désigne le groupe engendré par les commutateurs de G. [2], Ch. 11

Définition 3.5 — Une extension $K \subset L$ est dite radicale s'il existe une tour de corps K_1, $K_2 \dots K_r$, appelée tour radicale, telle que

1. $K = K_0 \subset K_1 \subset \cdots \subset K_r = L$;
2. Pour tout $1 \leq i \leq r$, il existe $a_i \in K_i$ et $n_i \geq 1$ tels que $K_i = K_{i-1}[a_i]$ et ${a_i}^{n_i} \in K_{i-1}$.

[2], Ch. 12

Définition 3.6 — Un polynôme $P \in K[X]$ est dit résoluble par radicaux s'il existe une extension radicale L de K contenant le corps de décomposition de P. [2], Sect. 12.1

Théorème 3.7 (Galois) — Si un polynôme P est résoluble par radicaux alors son groupe de Galois est résoluble. [2], Ch. 12

Théorème 3.8 — Le polynôme $P(X) = X^5 - 10X + 5$ de $\mathbb{Q}[X]$ n'est pas résoluble par radicaux. [2], Sect. 12.3

Références

[1] Josette Calais. *Eléments de théorie des groupes.* Puf, 1998.

[2] Jean-Pierre Escofier. *Théorie de Galois, cours et exercices corrigés.* Dunod, 1997.

[3] Hervé Francinou, Serge Gianella. *Exercices de mathématiques pour l'agrégation, algèbre 1.* Masson, 1995.

[4] Xavier Gourdon. *Les maths en tête. Algèbre.* Ellipses, 1994.

[5] Eric Lehman. *Mathématiques pour l'étudiant de première année. Algèbre et géométrie.* Belin, 1984.

[6] Daniel Perrin. *Cours d'algèbre.* Ellipses, 1996.