105
Groupe des permutations d'un ensemble fini. Applications

Ref : [Ulm] Ulmer, Théorie des groupes [Per] Perrin, Cours d'algèbre.
[Tau] Tauvel Algèbre [Coz] Cozzand, Théorie de Galois

Dev :
G1 Théorème de Sylow. [Per]
G8 Groupe du cube [H2G2]
G9 Sous-groupes distingués et table de $\mathfrak{S}_4$. [Pey]

I. Généralités sur les groupes symétriques

1) Définitions et premières propriétés

[Ulm] 41.

Def 1 : Pour E un ensemble, l'ensemble $\mathfrak{S}(E)$ des bijections de E dans E forme un groupe pour la composition des applications. La classe d'isomorphie de $\mathfrak{S}(E)$ ne dépend que du cardinal de E, si celui-ci est fini égal à n. On parlera du groupe symétrique d'indice n, noté $\mathfrak{S}_n$.

Rq 2 : Par défaut, on modélise $\mathfrak{S}_n$ par $\mathfrak{S}([\![1,n]\!])$.

Prop 3 : Le groupe $\mathfrak{S}_n$ est d'ordre $n!$, non abélien pour $n \geq 3$

Notation 4 : Pour $\sigma \in \mathfrak{S}_n$, on notera σ par le tableau $\begin{pmatrix} 1 & 2 & \dots & n \\ \sigma(1) & \sigma(2) & \dots & \sigma(n) \end{pmatrix}$

Ex 5 : Dans $\mathfrak{S}_3$, on considère $\sigma = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$, $\tau = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$, la composée est donnée par $\sigma\tau = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$ et $\tau\sigma = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$, donc $\tau\sigma \neq \sigma\tau$

Prop 6 : Soit G un groupe agissant sur E un ensemble de cardinal n. L'application $g \mapsto (x \mapsto g.x)$ induit un morphisme de groupes $G \to \mathfrak{S}(E)$, donc dans $\mathfrak{S}_n$. En fait la donnée d'un morphisme de groupes $G \to \mathfrak{S}_n$ est équivalente à celle d'une action de G sur un ensemble de cardinal n.

Co 7 (Cayley). Soit G un groupe fini d'ordre n, l'action de G sur lui-même par translation induit un morphisme injectif $G \hookrightarrow \mathfrak{S}_n$.

Rq 8 : Ce plongement est très sous-optimal dans beaucoup d'exemples (au sens où $n!$ est en pratique bien trop grand pour que ce résultat soit calculatoirement utile).

2) Orbites et cycles

[Ulm] 42.

Def 9 : Soient $n \in \mathbb{N}^*$ et $\sigma \in \mathfrak{S}_n$
- On appelle points fixes de σ les éléments de $[\![1,n]\!]$ avec $\sigma(i) = i$
- Par opposition, l'ensemble $[\![1,n]\!]$ privé des points fixes de σ forme le support de σ, noté $\mathrm{supp}(\sigma)$
- Une partie A de $[\![1,n]\!]$ est dite stable par σ si $\sigma(A) = A$.

Rq 10 : Le support de $\sigma \in \mathfrak{S}_n$ en est une partie stable.

[Ulm] 42 46

Prop 11 : Pour $\sigma, \rho \in \mathfrak{S}_n$, on a $\mathrm{Supp}(\sigma\rho) \subset \mathrm{Supp}\,\sigma \cup \mathrm{Supp}\,\rho$. Si σ et ρ sont à support disjoint, alors on a $\mathrm{Supp}(\sigma\rho) = \mathrm{Supp}(\sigma) \cup \mathrm{Supp}(\rho)$, ρ et σ commutent, et si $\rho\sigma = \mathrm{Id}$ alors $\rho = \mathrm{Id} = \sigma$.

Def 12 : Soient $1 \leq l \leq n$, $i_1, \dots, i_l$ des éléments de $[\![1,n]\!]$. La permutation $\gamma \in \mathfrak{S}_n$ définie par $\gamma(j) = \begin{cases} j & \text{si } j \notin \{i_1, \dots, i_l\} \\ i_{k+1} & \text{si } j = i_k \text{ avec } k < l-1 \\ i_1 & \text{si } j = i_l \end{cases}$

est notée $(i_1, \dots, i_l)$ et est appelée cycle de longueur l, un cycle de longueur 2 est appelé transposition.

Prop 13 : Dans $\mathfrak{S}_n$, les k-cycles sont au nombre de $\binom{n}{k}(k-1)!$ pour $k \geq 2$.

Théo 14 : Tout $\sigma \in \mathfrak{S}_n$ s'écrit comme produit $\sigma = \gamma_1 \dots \gamma_m$ de cycles γ_i de longueur ≥ 2 dont les supports sont deux à deux disjoints et correspondent aux orbites de l'action de $\langle\sigma\rangle$ sur $[\![1,n]\!]$. Cette décomposition est unique à réordonnancement des facteurs près.

Ex 15 : $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 1 & 4 & 3 & 5 \end{pmatrix} \in \mathfrak{S}_5$ se décompose comme $(12)(34)$

Def 16 : Soit $\sigma \in \mathfrak{S}_n$, on appelle type de σ la liste $\{l_1 \dots l_k\}$ des ordres respectifs des cycles à support disjoints apparaissant dans la décomposition de σ (rangés par ordre croissant).

Prop 17 : Un élément $\sigma \in \mathfrak{S}_n$ de type $[l_1 \dots l_k]$ a pour ordre le ppcm des l_i.

Théo 18 : Deux permutations σ et ρ de $\mathfrak{S}_n$ sont conjuguées si et seulement si elles ont même type. En particulier, pour $\omega \in \mathfrak{S}_n$, et $(i_1 \dots i_l)$ un l-cycle, on a
$$\omega(i_1 \dots i_l)\omega^{-1} = (\omega(i_1) \dots \omega(i_l))$$

Ex 19 : Dans $\mathfrak{S}_4$, les types possibles sont
- $(1,1,1,1)$, identité
- $(2,2)$ doubles transpositions
- (4), 4-cycles.
- $(2,1,1)$ transposition
- $(3,1)$ 3-cycles

Avec la proposition 13, on peut connaître les ordres de ces classes.

3) Générateurs.

[Ulm] 48. Le théorème 14 affirme que les cycles forment une famille de générateurs de $\mathfrak{S}_n$.

Prop 20 : Tout l-cycle de $\mathfrak{S}_n$ $(i_1 \dots i_l)$ est un produit de $l-1$ transpositions

$$(i_1 \dots i_l) = (i_1\, i_l)(i_1\, i_{l-1}) \dots (i_1\, i_2).$$

Ainsi : le groupe $\mathfrak{S}_n$ est engendré par les transpositions.

[Perr] 11 Prop 21 : Les transpositions $(1\,2), (1\,3) \dots (1,n)$ engendrent $\mathfrak{S}_n$.

Prop 22 : Le couple $(1,2), (1\,2 \dots n)$ engendre $\mathfrak{S}_n$, ce système de générateurs est minimal pour $n \geq 3$ car $\mathfrak{S}_n$ est alors non abélien.

II. Signature, groupe alterné.

1) Signature.

[Ulm] 49 51 Def 23 : Soit $n \geq 1$ un entier et $\sigma \in \mathfrak{S}_n$. On appelle signature de $\sigma \in \mathfrak{S}_n$ et on note $\varepsilon(\sigma)$ le nombre $\varepsilon(\sigma) = \prod_{1 \leq i < j \leq n} \frac{\sigma(i) - \sigma(j)}{i-j}$

Prop 24 : La signature d'une transposition est -1.

Prop 25 : La signature est un morphisme de groupes, à valeurs dans $\{\pm 1\}$. La signature d'une permutation est donnée par la parité dans une décomposition en produit de transpositions.

2) Groupe alterné

Def 26 : Le noyau du morphisme signature est appelé groupe alterné d'indice n, $\mathfrak{A}_n$. Il s'agit d'un sous groupe distingué de $\mathfrak{S}_n$ d'indice 2.

Ex 27. Le groupe $\mathfrak{A}_4$ est d'ordre 12, qui ne contient pas de sous groupe d'indice 2. C'est donc un contre exemple à la réciproque du théorème de Lagrange.

Rq 28. Les doubles transpositions forment un sous groupe de $\mathfrak{A}_4$, isomorphe au groupe $K_4 = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. Ce sous groupe est distingué dans $\mathfrak{S}_4$. Or une double transposition engendre un sous groupe distingué dans le groupe des doubles transpositions mais pas dans $\mathfrak{S}_4$.

Prop 29 : La relation de normalité n'est pas transitive.

[Ulm] Prop 30 : Le groupe alterné $\mathfrak{A}_n$ est engendré par les cycles de la forme $(1\, i\, j)$ pour $i, j \in [\![2, n]\!]$ distincts. En particulier, les trois cycles engendrent $\mathfrak{A}_n$.

[Perr] Prop 31 : L'action de $\mathfrak{A}_n$ sur $\{1, \dots, n\}$ est $n-2$ transitive : pour deux parties $(a_i)_{i=1,\dots,n-2}$, $(b_i)_{i=1,\dots,n-2}$ de $[\![1, n]\!]$, il existe $\sigma \in \mathfrak{A}_n$ telle que $\sigma(a_i) = b_i$ $\forall i \in [\![1, n-2]\!]$.

Prop 32 : Pour $n \geq 5$, les trois cycles sont conjugués dans $\mathfrak{A}_n$.

Appli 33 : Pour $n \geq 5$, le groupe $\mathfrak{A}_n$ est simple.

3) Structure des groupes symétriques et alternés.

[Perr] 28 31 Rq 44 : On a $\mathfrak{A}_3 \simeq 3$ et $\mathfrak{A}_2 \simeq \mathbb{Z}/2\mathbb{Z}$, donc $\mathfrak{A}_4$ est le seul groupe alterné non simple.

Prop 45 : On a $D(\mathfrak{A}_n) \simeq \mathfrak{A}_n$ pour $n \geq 5$ et $D(\mathfrak{S}_n) \simeq \mathfrak{A}_n$ pour $n \geq 2$.

Rq 46 : On a $D(\mathfrak{A}_n) = 1$ pour $n = 2$ et 3, et $D(\mathfrak{A}_4) \simeq K_4$ (doubles transpositions).

Cor 47 : Pour $n \geq 5$, les sous groupes distingués de $\mathfrak{S}_n$ sont 1, $\mathfrak{A}_n$, $\mathfrak{S}_n$.

Cor 48 : Tout sous groupe d'indice n de $\mathfrak{S}_n$ est isomorphe à $\mathfrak{S}_{n-1}$.

Théo 49 : La signature $\varepsilon : \mathfrak{S}_n \to \{\pm 1\}$ induit une suite exacte courte scindée à droite : on a $\mathfrak{S}_n \simeq \mathfrak{A}_n \rtimes \{\pm 1\}$.

Théo 50 : Pour $n \neq 6$, tout automorphisme de $\mathfrak{S}_n$ est intérieur : $\mathrm{Int}\, \mathfrak{S}_n \simeq \mathrm{Aut}\, \mathfrak{S}_n$.

Prop 51 : Pour $n \geq 4$, $Z(\mathfrak{S}_n) = \{Id\}$, donc pour $n \geq 7$ et $n = 4, 5$, $\mathrm{Aut}\, \mathfrak{S}_n \simeq \mathfrak{S}_n$.

III. Applications.

1) Déterminant

[Tau] 187 On considère ici A un anneau commutatif unitaire, et $E_1 \dots E_p$, F des A-modules pour $p \geq 1$.

Def 52 : Une application $f : E_1 \times \dots \times E_p \to F$ est p-linéaire si pour $j \in [\![1, p]\!]$, et pour toute famille $(u_1 \dots \check{u}_j, u_{j+1} \dots u_p) \in E_1 \times \dots \times \check{E}_j \times \dots \times E_p$, l'application $x_j \mapsto f(u_1 \dots u_{j-1}, x_j, u_{j+1}, \dots, u_p)$ de E_j dans F est linéaire. On dira bilinéaire ou trilinéaire au lieu de 2 ou 3-linéaire. Une application p-linéaire $E_1 \times \dots \times E_p$ dans A est appelée forme p-linéaire.

[Tom] 189 190 Not 53 On note $L_p(E)$ les formes p-linéaires sur $E\times E\times\dots\times E$, il s'agit d'un A-module.

Ex 54 : Si $\varphi_1\dots\varphi_p\in E^*$ pour E un A-module, alors $(x_1\dots x_p)\mapsto\varphi_1(x_1)\dots\varphi_p(x_p)$ est une forme p-linéaire.

Le groupe $\mathfrak{S}_p$ opère sur $L_p(E,F)$ par $f^\sigma(x_1\dots x_p)=f(x_{\sigma(1)},\dots,x_{\sigma(p)})$

Def 55 : On dit que $f\in L_p(E,F)$ est symétrique (resp antisymétrique) si $f^\sigma=f$ (resp $\varepsilon(\sigma)f$) pour $\sigma\in\mathfrak{S}_p$. On dit que f est alternée si $f(x_1\dots x_p)=0$ dès que deux des x_i sont égaux.

Rq 56 : Si $2\cdot 1_A$ n'est pas diviseur de 0 dans A, alors antisymétrique équivaut à alterné.

Prop 57 : Si E est libre de avec une base $(e_1\dots e_n)$, pour $f\in L_p(E)$ antisymétrique, on a
$$f(x_1\dots x_p)=\sum_{\sigma\in\mathfrak{S}_n}\varepsilon(\sigma)\prod_{j=1}^{n}x^j_{\sigma(j)}\,f(e_1\dots e_n)\text{ où } x_k=\sum_{j=1}^{n}x_k^j e_j.$$

On appelle déterminant dans la base $(e_1\dots e_n)$ la forme n-linéaire alternée valant 1 sur la base $(e_1\dots e_n)$.

Appli 58 : Toutes les bases d'un module libre ont même cardinal, le rang de E.

2) Théorèmes de Sylow.

[Per] 18 20. Def 59 : Soit G un groupe fini de cardinal $p^\alpha m$ où $p\wedge m$ et p est premier. On appelle p-sous-groupe de Sylow de G (ou p-Sylow) tout sous-groupe de G d'ordre p^α. On note $Syl_p(G)$ leur ensemble.

Théo 60 : Soit G un groupe d'ordre $p^\alpha m$, $p\wedge m$, et H un sous-groupe de G. Pour $S\in Syl_p(G)$ il existe $a\in G$ tel que $aSa^{-1}\cap H\in Syl_p(H)$.

Appli 61 : (Théorèmes de Sylow) Avec les notations précédentes, on a :
- $Syl_p(G)\neq\emptyset$ - $\forall S\in Syl_p(G)$ et $H\leq G$ un p-groupe, $\exists a\in G\mid aSa^{-1}\supseteq H$ **DVP**
- $|Syl_p(G)|\equiv 1[p]$ et divise m.

Appli 62 : Tout groupe d'ordre 200 n'est pas simple.

Appli 63 : Soit G un groupe fini, p le plus petit nombre premier divisant $|G|$, alors tout sous-groupe de G d'indice p est distingué.

3) Isomorphismes exceptionnels.

[Per] 106 Prop 64 : On a les isomorphismes de groupes suivants
1) $GL_2(\mathbb{F}_2)\simeq SL_2(\mathbb{F}_2)\simeq PSL_2(\mathbb{F}_2)\simeq\mathfrak{S}_3$
2) $PGL_2(\mathbb{F}_3)\simeq\mathfrak{S}_4$ $PSL_2(\mathbb{F}_3)\simeq\mathfrak{A}_4$
3) $PGL_2(\mathbb{F}_4)\simeq PSL_2(\mathbb{F}_4)\simeq\mathfrak{A}_5$
4) $PGL_2(\mathbb{F}_5)\simeq\mathfrak{S}_5$ $PSL_2(\mathbb{F}_5)\simeq\mathfrak{A}_5$.

4) Groupes d'isométrie

E désigne un $\mathbb{R}$-espace affine euclidien.

Def 65 : Si $X\subseteq E$, on note $Isom(X)$ le sous-ensemble de $O_n(\mathbb{R})$ des isométries qui stabilisent X.

Prop 66 : Si $M_1\dots M_m\in E$, M leur enveloppe convexe, $Isom(M)$ agit sur les points extrémaux de M.

Pour le n-gone régulier de $\mathbb{R}^2\simeq\mathbb{C}$, le groupe $Isom(P_n)$ est D_n le groupe diédral d'ordre $2n$, son action sur les sommets donne un morphisme injectif $D_n\hookrightarrow\mathfrak{S}_n$ (c'est un raffinement du théorème de Cayley).

Prop 67 : Si T est un tétraèdre régulier de $\mathbb{R}^3$, $Isom(T)\simeq\mathfrak{S}_4$ et $Isom^+(T)\simeq\mathfrak{A}_4$ ($Isom(T)\cap SO_3(\mathbb{R})$).

Prop 68 : Si K est un cube régulier, alors $Isom(K)\simeq\mathfrak{S}_4\times\mathbb{Z}/2\mathbb{Z}$ et $Isom^+(K)\simeq\mathfrak{S}_4$. de plus les sous-groupes de Sylow se réalisent comme invariants de l'action de $Isom^+(K)$ sur K. **DVP**

Appli 69 : Les sous-groupes distingués d'un groupe fini se réalisent comme intersection des noyaux des représentations irréductibles. On peut ainsi construire la table du groupe $\mathfrak{S}_4$ (F; 7) et lister ses sous-groupes distingués. **DVP**

5) Polynômes symétriques.

Def 70 : Soit A un anneau, $\mathfrak{S}_n$ agit sur $A[X_1\dots X_n]$ par permutation des variables, les points fixes de cette action sont appelés polynômes symétriques. [Goz] 12 15

Def 71 : Pour $j\leq n$, on pose $\Sigma_j(X_1\dots X_n)=\sum_{1\leq i_1<\dots<i_j\leq n}X_{i_1}\dots X_{i_j}$ le j-ème polynôme symétrique élémentaire.

Théo 72 (Relation coefficients racines) Pour $P=(X-\alpha_1)\dots(X-\alpha_n)$ un polynôme, alors si $P=X^n+a_{n-1}X^{n-1}+\dots+a_0$, on a $a_j=(-1)^{n-j}\Sigma_{n-j}(\alpha_1\dots\alpha_n)$.

Théo 72 : L'application $A[X_1\dots X_n]\longrightarrow A[\Sigma_1\dots\Sigma_n]\subseteq A[X_1\dots X_n]^{\mathfrak{S}_n}$ envoyant $P(X_1,\dots,X_n)$ sur $P(\Sigma_1\dots\Sigma_n)$ est un isomorphisme de A-algèbre.