105 - Groupe des permutations d'un ensemble fini. Applications

Cadre : $n \in \mathbb{N}$, $n \geq 2$. X est un ensemble non vide.

I. Groupe des permutations, générateurs de S_n et conjugaison

1) Définitions et premières propriétés. Support.

[Ber] **Déf. ①** : L'ensemble des bijections de X dans X, noté $S(X)$, est un

~ groupe pour la composition des applications appelé groupe des permutations

57 de X ou groupe symétrique de X. $\sigma \in S(X)$ est appelée une permutation.

Prop. ② : Si $|X| = n$, alors $|S(X)| = n!$

Déf./Prop ③ : On appelle groupe symétrique d'ordre n : $S_n = S(\{1 \dots n\})$. Si $|X| = n$, alors $S(X) \simeq S_n$.

Déf./Prop. ④ : Soit $(G,\cdot)$ un groupe. On dit que G agit sur X s'il existe une

169 application $\cdot : \begin{array}{l} G \times X \longrightarrow X \\ (g,x) \longmapsto g\cdot x \end{array}$ telle que : 1) $\forall g, g' \in G, \forall x \in X$, $g\cdot(g'\cdot x) = (gg')\cdot x$ 2) $\forall x \in X$, $1_G \cdot x = x$

170 Il est équivalent de se donner un morphisme de groupes $G \longrightarrow S(X)$.

Th. ⑤ : *(Cayley)*

177 Soit G un groupe fini d'ordre n. Alors, G est isomorphe à un sous-groupe de S_n.

200 **Déf. ⑥** : Soit $\sigma \in S_n$. Le support de σ est $\mathrm{Supp}(\sigma) = \{a \in \{1 \dots n\} / \sigma(a) \neq a\}$

Prop. ⑦ : 1) $\sigma \in S_n$. $\mathrm{Supp}(\sigma) = \sigma(\mathrm{Supp}(\sigma)) = \mathrm{Supp}(\sigma^{-1}) = \mathrm{Supp}(\sigma^m)$ $m \in \mathbb{Z}$.
2) $\sigma, \sigma' \in S_n$. $\mathrm{Supp}(\sigma\sigma') \subset \mathrm{Supp}(\sigma) \cup \mathrm{Supp}(\sigma')$ et si les supports sont disjoints, alors $\mathrm{Supp}(\sigma\sigma') = \mathrm{Supp}(\sigma) \cup \mathrm{Supp}(\sigma')$.

201 **Prop. ⑧** : Deux permutations à support disjoint commutent

♡ **Rq ⑨** : La réciproque est fausse ! *(prendre $\sigma = \sigma'$ par exemple)*

2) Cycles de S_n $E = \{1 \dots n\}$

[Ber] ~ **Rq ⑩** : Soit $\sigma \in S_n$. L'action naturelle de S_n sur E induit une action

♡ de $\langle \sigma \rangle$ sur E définie par : $(s, i) \in \langle\sigma\rangle \times E \longmapsto s(i)$.

202 **Déf. ⑪** : $\sigma \in S_n$ est un cycle s'il n'y a qu'une seule σ-orbite non réduite à un élément. Dans ce cas, si $|\mathrm{Supp}(\sigma)| = k \geq 2$, on dit que σ est un k-cycle.

Notation ⑫ : Soient $a_1 \dots a_k \in E$ et σ un k-cycle tel que : $\sigma(a_1) = a_2 \dots \sigma(a_{k-1}) = a_k$ et $\sigma(a_k) = a_1$, alors on notera $\sigma = (a_1 \cdots a_k)$.

Ex. ⑬ : $E = \{1 \dots 4\}$. $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 2 & 4 \end{pmatrix} = (1\,3\,2)$ est un 3-cycle de S_4. 203

Déf. ⑭ : Un 2-cycle est appelé une transposition

Prop. ⑮ : Soit $2 \leq k \in n$. Il y a $(k-1)!\binom{n}{k} = \frac{n!}{k(n-k)!}$ k-cycles dans S_n. ♡

Notation ⑯ : On notera $o(\sigma)$ l'ordre de $\sigma \in S_n$.

Prop. ⑯ : Un k-cycle est d'ordre k. 207

3) Générateurs de S_n [Ber]

Th. ⑰ : Soit $\sigma \in S_n$. Alors σ se décompose en produit de cycles à supports disjoints, et cette décomposition est unique à l'ordre des facteurs près. 204

Coro ⑱ : S_n est engendré par les cycles. 206

Ex. ⑳ : Soit $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 5 & 6 & 2 & 4 & 1 & 3 \end{pmatrix} \in S_6$. Alors $\sigma = (1\,5)(2\,6\,3)$

Coro ⑲ : S_n est engendré par les transpositions. 207

Th. ⑳ : Soit $\sigma \in S_n$ et $\sigma = c_1 \cdots c_r$ sa décomposition en produit de cycles à supports disjoints. Alors $o(\sigma) = \mathrm{ppcm}(o(c_1), \dots, o(c_r))$. 208

Rq ㉑ : $\mathrm{Supp}(\sigma) = \coprod_{i=1}^{r} \mathrm{Supp}(c_i)$ ♡

Lemme ㉒ : Soit $\tau \in S_n$ et $(a_1 \dots a_k)$ un k-cycle. 209
Alors $\tau(a_1 \dots a_k)\tau^{-1} = (\tau(a_1) \dots \tau(a_k))$. En particulier, le conjugué d'un k-cycle est également un k-cycle.

Prop. ㉓ : Les parties suivantes sont génératrices de S_n : 212 213
1) $\{(1\,i), 2 \leq i \leq n\}$ 2) $\{(i\;i{+}1), 1 \leq i \leq n-1\}$ 3) $\{(1\,2), (1\,2 \dots n)\}$

4) Conjugaison dans S_n [Ber] ~

Prop. ㉔ : Deux k-cycles sont conjugués *(dans S_n)*

Th ㉕ : $\sigma, \sigma' \in S_n$ sont conjugués dans S_n SSI les listes (avec répétition) des longueurs des cycles à support disjoints qui les composent sont les mêmes à l'ordre près. 209

210 **Ex. 26** : $\sigma = (135)(24)$ et $\sigma' = (123)(67)$ sont conjugués dans S_7.

Si $\tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 1 & 6 & 2 & 7 & 3 & 4 & 5 \end{pmatrix} = (264753)$, alors $\tau \sigma \tau^{-1} = \sigma'$.

Déf. 27 : Une partition de n est une suite d'entiers $(p_k)_{k \geq 1}$, décroissante,
211 nulle à partir d'un certain rang et telle que $\sum_{k \geq 1} p_k = n$.

On notera $P(n)$ l'ensemble des partitions de n.

Ex. 28 : $P(4) = \{(4), (3,1), (2,2), (2,1,1), (1,1,1,1)\}$

Déf. 29 : Soit $\sigma \in S_n$. Le type de σ est la partition de n dont les éléments non nuls sont les cardinaux des diverses σ-orbites, rangés par ordre décroissant.

Ex. 30 : $\sigma = (13)(4765) \in S_9$ est de type $(4,2,1,1,1)$.

Th. 31 : Le Th. 25 peut se reformuler en : $\sigma, \sigma' \in S_n$ sont conjuguées SSI σ et σ' sont de même type.

212 **Coro. 32** : Il y a $P(n)$ classes de conjugaison dans S_n.

♡ **Appli. 33** : Il y a 5 caractères irréductibles sur S_4.

II. Groupe alterné

1) Le morphisme signature

♡ **Th. 34** : Il existe un unique morphisme de groupes $\varepsilon : (S_n, \circ) \to (\{\pm 1\}, \times)$ surjectif. De plus, ce morphisme vaut -1 sur les permutations.

♡ **Déf. 35** : ε est appelé morphisme signature, et si $\sigma \in S_n$, $\varepsilon(\sigma) \in \{\pm 1\}$ est appelé signature de σ.
σ est dite paire si $\varepsilon(\sigma) = 1$, impaire si $\varepsilon(\sigma) = -1$.

[Ber] 214 **Prop. 36** : Si $\sigma \in S_n$ est un k-cycle, alors $\varepsilon(\sigma) = (-1)^k$.

2) Le groupe alterné A_n [Ber]

Déf. 37 : Le groupe alterné d'ordre n est $A_n = \operatorname{Ker} \varepsilon$, où ε est défini sur S_n. 215

Prop. 38 : A_n est distingué dans S_n, et $[S_n : A_n] = 2$, donc $|A_n| = \frac{n!}{2}$.
En particulier, si $\tau \in S_n$ est une transposition, $S_n / A_n = \{A_n, \tau A_n\}$.

Ex. 39 : $A_2 = \{id\}$, $A_3 = \{1, \sigma, \sigma^2\}$ où $\sigma = (123)$

Th. 40 : $n \geq 3$. A_n est engendré par : 216
1) les produits de deux transpositions
2) les 3-cycles.

Lemme 41 : $n \geq 5$. Les 3-cycles sont conjugués dans A_5. 217

Coro. 42 : Si $n \geq 2$, alors $D(S_n) = A_n$ [Per]
si $n \geq 5$, alors $D(A_n) = A_n$ 28

Rq 43 : Si $n = 3$, $D(A_3) = \{id\} \neq A_3$. 30
Si $n = 4$, on pose $V_4 = \{id, (12)(34), (13)(24), (14)(13)\}$. Alors $D(A_4) = V_4$.

Th. 44 : Si $n \geq 3$ et $n \neq 4$, alors A_n est simple. DVP 1 28

Lemme 45 : $n \geq 3$. $Z(S_n) = \{id\}$. [Ber] 219

Coro. 46 : Si $n \neq 4$, les sous groupes distingués de S_n sont : $\{id\}$, A_n et S_n 220

Th. 47 : Si $n \neq 6$, alors les automorphismes de S_n sont intérieurs. DVP 2 [Per] 30

III. Applications

1) Déterminant [Ber]

Cadre : A est un anneau commutatif intègre, K un corps (commutatif).
Dans cette partie E est un K-ev de dimension finie $n \geq 1$.

Lemme 48 : Soient $f_1 \dots f_n$ n formes linéaires sur E. 63
Alors
$$\varphi : E \times \dots \times E \longrightarrow K, \quad (x_1 \dots x_n) \longmapsto \sum \varepsilon(\sigma) f_{\sigma(1)}(x_1) \dots f_{\sigma(n)}(x_n)$$
est une forme n-linéaire alternée.

Notation 49 : $\mathrm{Alt}_n(E)$ désigne le K-ev des formes n-linéaires alternées sur E.

63 Th. (50) : Soit $e = (e_1 \dots e_n)$ une base de E. Alors :
$\exists !\ \det_e \in \mathrm{Alt}_n(E)$ / $\det_e(e_1 \dots e_n) = 1$. De plus $\det_e$ engendre $\mathrm{Alt}_n(E)$.

65 Coro (51) : Soit $u \in \mathcal{L}(E)$.
$\exists !\ \det_e(u) \in K$ / $\forall (x_1 \dots x_n) \in E^n$, $\det_e(u(x_1) \dots u(x_n)) = \det_e u \times \det_e(x_1 \dots x_n)$

66 Prop. / Déf. (52) : Soit $u \in \mathcal{L}(E)$ et e une base de E. Alors $\det_e(u)$ est indépendant du choix de e. On l'appelle déterminant de u.

Prop. (53) : Soit $u, v \in \mathcal{L}(E)$. Alors $\det(u \circ v) = \det(u) \times \det(v)$.

Déf. (54) : Soit $M = (m_{ij}) \in \mathcal{M}_n(A)$. Le déterminant de M est :

~67 $$\det M = \sum_{\sigma \in S_n} \varepsilon(\sigma)\, m_{\sigma(1)1} \dots m_{\sigma(n)n} \in A.$$

68 Prop. (55) : $M, N \in \mathcal{M}_n(A)$. 1) $\det(MN) = \det M \times \det N = \det(NM)$.
2) $\det({}^t M) = \det M$.

Ex. (56) : $M = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathcal{M}_2(A)$. $\det M = \varepsilon(id) \cdot ad + \varepsilon((12)) cb = ad - cb$

Prop. (57) : Soit $u \in \mathcal{L}(E)$. On note $\chi_u = a_n X^n + \dots + a_0 \in K[X]$ son
946 polynôme caractéristique.
Alors : $a_n = 1$, $a_{n-1} = -\mathrm{Tr}(u)$ et $a_0 = (-1)^n \det u$.

♡ ## 2) Matrices de permutation

Déf. (58) : Soit $(e_1 \dots e_n)$ la base canonique de K^n et $\sigma \in S_n$. La matrice de permutation M_σ et σ est définie par : $M_\sigma e_i = e_{\sigma(i)}$ $\forall 1 \leq i \leq n$

Ex (59) : $M_{(132)} = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix}$.

Rq (60) : $\det(M_\sigma) = \varepsilon(\sigma)$

Prop. (61) : L'application $\begin{array}{ccc} S_n & \longrightarrow & GL_n(K) \\ \sigma & \longmapsto & M_\sigma \end{array}$ est un morphisme de groupes injectif.

Appli. (62) (Sylow)
Si G est un groupe tel que $|G| = p^\alpha m$, p premier, $\alpha \geq 2$, $m \in \mathbb{N}$ et $p \nmid m$, l'utilisation du théorème de Cayley et de Prop. (61) avec $K = \mathbb{Z}/p\mathbb{Z}$ permet de montrer l'existence dans G d'un p-Sylow.

Rq (63) : Les matrices de transposition $P_{ij} = M_{(ij)}$ jouent un rôle fondamental dans l'algorithme du pivot de Gauss, grâce à la correspondance :

$P_{ij} A$	$A P_{ij}$
$L_i \leftrightarrow L_j$	$C_i \leftrightarrow C_j$

où $A \in \mathcal{M}_n(K)$, $1 \leq i \neq j \leq n$

⚠ calcul du déterminant ($\det P_{ij} = -1$) !

Références :

- [Ber] Berhuy, Algèbre : le grand combat (2e éd.)
- [Per] Perrin, Cours d'algèbre