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

I Le groupe symétrique

A Définitions et propriétés Rom 2.1 2.2 1.6

On considère E un ensemble fini de cardinal $|E| = m$.

Définition 1 : Le groupe symétrique $S(E)$ de E est l'ensemble des bijections de E dans E appelés permutations.
Pour $E = [\![1, m]\!]$ on note $S_m = S(E)$ le groupe symétrique à m éléments.

Proposition 2 : Le centre du groupe de $S(E)$ est :
$$Z(S(E)) = \begin{cases} S(E) & \text{si } |E| = 2 \\ \{id_E\} & \text{si } |E| \geq 3 \end{cases}$$

Remarque 3. Pour $m \geq 3$, $S(E)$ n'est pas commutatif.

Exemple 4 : Si $E = [\![1, m]\!]$, $m \geq 3$, $(12)(13) = (132) \neq (123) = (13)(12)$

Théorème 5 : Si E et F sont deux ensembles non vides et φ une bijection de E sur F, alors les groupes $S(E)$ et $S(F)$ sont isomorphes.

Remarque 6 : Donc tout groupe de permutations d'un ensemble E à m éléments est isomorphe à S_m.

Corollaire 7 : $|S_m| = m!$

Proposition 8 : S_m agit naturellement sur $[\![1, m]\!]$ par permutation :
$$(\sigma, x) \in S_m \times [\![1, m]\!] \mapsto \sigma . x = \sigma(x) \in [\![1, m]\!].$$

Théorème 9 (Cayley) : Un groupe de cardinal n est isomorphe à un sous groupe de S_n.

B Cycles et décomposition Rom 2.1 2.3 2.4

Définition 10 : Soit $r \in [\![2, m]\!]$, on appelle r-cycle toute permutation $\sigma \in S(E)$ qui permute circulairement r éléments de E et laisse fixe les autres.
Si $r = 2$, on appelle le 2-cycle une transposition.

Lemme 11 : Soit $r \in [\![2, m]\!]$. Le conjugué dans S_m d'un r-cycle est un r-cycle. Réciproquement deux r-cycles de même longueur sont conjugués dans $S(E)$.

Application 12 : Il y a $(r-1)!\binom{m}{r}$ r-cycles.

Exemple 13 : Dans S_4 il y a 6 transpositions, 8 3-cycles et 6 4-cycles.

Définition 14 : Le support de $\sigma \in S(E)$ est le complémentaire dans E de l'ensemble de ses points fixes, soit l'ensemble : $\mathrm{Supp}(\sigma) = \{x \in E, \sigma(x) \neq x\}$

Théorème 15 : Soient $\sigma, \sigma' \in S(E)$:
i) $\sigma(\mathrm{supp}(\sigma)) = \mathrm{supp}(\sigma)$ iii) $\forall n \in \mathbb{Z}$, $\mathrm{supp}(\sigma^n) \subset \mathrm{supp}(\sigma)$
ii) $\mathrm{supp}(\sigma) = \mathrm{supp}(\sigma^{-1})$ iv) si $\mathrm{supp}(\sigma) \cap \mathrm{supp}(\sigma') = \emptyset$ alors $\sigma \circ \sigma' = \sigma' \circ \sigma$.

Remarque 16 : La réciproque de iv) est fausse, prendre $\sigma \neq id_E$ et $\sigma' = \sigma^{-1}$.

Définition 17 : On dit que σ et σ' sont disjoints si leurs supports sont disjoints dans E.

Théorème 18 : Toute permutation $\sigma \in S(E) \setminus \{id_E\}$ se décompose en produit de cycles deux à deux disjoints ($S(E)$ est engendré par les cycles). Cette décomposition est unique à l'ordre près.
Si $\sigma = \gamma_1 \dots \gamma_p$ est une telle décomposition, on a alors la partition : $\mathrm{supp}(\sigma) = \bigcup_{k=1}^{p} \mathrm{supp}(\gamma_k)$ et $\theta(\sigma) = \mathrm{ppcm}(\theta(\gamma_1), \dots, \theta(\gamma_p))$.

Exemple 19 : pour $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 2 & 3 & 4 & 5 & 1 & 7 & 6 & 8 \end{pmatrix}$ on a $\sigma = (1234)(5)(67)$.

C Signature et groupe alterné Rom 2.6 2.7

Définition 20 : Soit $\sigma \in S_m$ alors $\varepsilon(\sigma) = \prod_{1 \leq i < j \leq m} \frac{\sigma(j) - \sigma(i)}{j - i}$

Exemple 21 : Soit σ une transposition, alors $\varepsilon(\sigma) = -1$.
Si σ est un r-cycle, $\varepsilon(\sigma) = (-1)^{r-1}$.

Proposition 22 : Si $\sigma \in S(E)$ est un produit de p transpositions alors on a $\varepsilon(\sigma) = (-1)^p$

Lemme 23 : pour tout $\sigma \in S(E)$ et pour toute transposition $\tau \in S(E)$ on a
$$\varepsilon(\tau\sigma) = \varepsilon(\tau)\varepsilon(\sigma) = -\varepsilon(\sigma).$$

Théorème 24: Les seuls morphismes de groupes de $(S(E),\circ)$ dans $(\mathbb{R}^*,\cdot)$ sont l'application constante égale à 1 et la signature ε. La signature étant surjective de $S(E)$ dans $\{-1,1\}$

Définition 25: On définit $A_m = \ker \varepsilon$ le groupe alterné.

Proposition 26: $A_m \triangleleft S_m$ et $|A_m| = \frac{m!}{2}$

II Structure de S_m et A_m.

A Générateurs Rem 2.5 2.7

Lemme 27: Soit $r \in [\![2,m]\!]$, tout r-cycle dans $S(E)$ se décompose comme produit de $r-1$ transpositions.

Théorème 28: Toute permutation $\sigma \in S(E)$ se décompose en produit de transpositions ($S(E)$ est engendré par les transpositions).

Exemple 29: pour $\sigma = (1\,2\,3\,4\,5)(6\,7)$, $\sigma = (1\,2)(2\,3)(3\,4)(4\,5)(6\,7)$.

Remarque 30: puisque $S(E) \simeq S_m$ on se contente de décrire des générateurs de S_m.

Lemme 31: S_m est engendré par les $m-1$ transpositions $(1\,k)$ où $k \in [\![2,m]\!]$.

Exemple 32: Soit $1 \leq i < j \leq m$ alors $(i\,j) = (1\,i)(1\,j)(1\,i)$.

Lemme 33: S_m est engendré par les $m-1$ transpositions $(k,k+1)$ où k est compris entre 1 et $m-1$.

Exemple 34: pour $k \geq 3$, $(1\,k) = (k-1\;k)(1\;k-1)(k-1\;k)$

Lemme 35: S_m est engendré par $\overset{\tau=}{(1\,2)}$ et $\overset{\gamma=}{(1\,2\ldots m)}$

Exemple 36: $(k\;k+1) = \gamma^{k-1}\,\tau\,(\gamma^{k-1})^{-1}$ pour $1 \leq k \leq m-1$.

Théorème 37: Pour $m \geq 3$, $A(E)$ est engendré par les 3-cycles.

Exemple 38: $(1\,2)(3\,4) = (1\,2)(2\,3)(2\,3)(3\,4) = (1\,2\,3)(2\,3\,4)$.

B Sous-groupes distingués de S_m et A_m. Pau 1.8

Lemme 39: Si $m \geq 5$, soit $N \triangleleft A_m$ tel que N contienne un 3-cycle alors $N = A_m$.

Développement: Si $m \geq 5$, A_m est simple.

Remarque 40: A_1, A_2 et A_3 sont simples.
A_4 n'est pas simple car $V_4 \triangleleft A_4$ où V_4 est le groupe de Klein.
Dvlpt: à isom près A_5 seul groupe simple d'ordre 60.

Corollaire 41: On a $D(A_m) = A_m$ pour $m \geq 5$ et $D(S_m) = A_m$ pour $m \geq 2$.

Corollaire 42: Pour $m \geq 5$ les sous-groupes distingués de S_m sont $\{1\}$, A_m et S_m.

Corollaire 43: Si H est un sous-groupe d'indice n de S_m, alors H est isomorphe à S_{m-1}.

III Applications

A Régularité du déterminant Rem 17.1 17.2

On considère E un $\mathbb{K}$-ev de dimension finie $n \in \mathbb{N}^*$

Définition 44: Une forme p-linéaire ($p \geq 2$) sur E est une application $\varphi : E^p \to \mathbb{K}$ telle que pour tout $k \in [\![1,p]\!]$ et $(x_i)_{i \neq k} \in E^{p-1}$ fixés dans E^{p-1} l'application partielle $\varphi_i : x \in E \mapsto \varphi(x_1,\ldots,x_{k-1},x,\overset{i\neq k}{x_{k+1}},\ldots,x_p)$ est une forme linéaire sur E. On note $\mathcal{L}_p(E,\mathbb{K})$ leur ensemble.
On dit que φ est alternée si $\varphi(x_1,\ldots,x_p) = 0$ pour tout $(x_i)_{1\leq i\leq p} \in E^p$ pour lequel il existe $j \neq k$ compris entre 1 et p tels que $x_i = x_j$. On note $\mathcal{A}_p(E,\mathbb{K})$ leur ensemble.

Exemple 45: Un produit scalaire est une forme bilinéaire.

Théorème 46: Pour tout entier $p \geq 1$, $\mathcal{L}_p(E,\mathbb{K})$ est un $\mathbb{K}$-ev de dimension n^p.

Théorème 47: Une forme p-linéaire φ sur E est alternée si et seulement si $\varphi(x_{\sigma(1)},\ldots,x_{\sigma(p)}) = \varepsilon(\sigma)\,\varphi(x_1,\ldots,x_p)$ pour tout $\sigma \in S_p$ et pour tout $(x_1,\ldots,x_p) \in E^p$.

Théorème 48: L'ev $A_n(E,\mathbb{K})$ est de dimension 1 engendré par $\det_B : E^n \to \mathbb{K}$, $(x_1,\ldots,x_n) \mapsto \sum_{\sigma\in S_n} \varepsilon(\sigma) \prod_{i=1}^{n} x_{\sigma(i),i}$

où $x_j = \sum_{i=1} \tilde{x}_{i,j} e_i$ pour tout $j \in [\![1, m]\!]$.

Définition 49 : Avec les notations qui précèdent on dit que $\det_B(x_1, \dots, x_m)$ est le déterminant dans la base B du m-uplet de vecteurs $(x_i)_{1 \le i \le m}$.

Proposition 50 : L'application $\det_B : \mathcal{M}_m(\mathbb{K}) \to \mathbb{K}$ est une fonction polynomiale homogène de degré m.

Corollaire 51 : $GL_m(\mathbb{K}) = \det_B^{-1}(\mathbb{K}^*)$ est un ouvert de $\mathcal{M}_m(\mathbb{K})$.

B Polynômes symétriques et relation coefficients-racines X-G § 4

Définition 52 : Un polynôme $P \in A[X_1, \dots, X_m]$ est dit symétrique si pour tout $\sigma \in S_m$, $P(X_{\sigma(1)}, \dots, X_{\sigma(m)}) = P(X_1, \dots, X_m)$.

Exemple 53 : Dans $\mathbb{R}[X, Y, Z]$, $P = XY + YZ + ZX$ est symétrique

Définition 54 : On appelle polynômes symétriques élémentaires de $A[X_1, \dots, X_m]$ les polynômes notés Σ_p $(1 \le p \le m)$ et définis par : $\Sigma_p = \sum_{i_1 < \dots < i_p} X_{i_1} \cdots X_{i_p}$.

Exemples 55 : $\Sigma_1 = X_1 + \dots + X_m$, $\Sigma_2 = \sum_{i<j} X_i X_j$

Propriétés 56 : Les polynômes symétriques élémentaires vérifient :
$(T - X_1) \cdots (T - X_m) = T^m - \Sigma_1 T^{m-1} + \Sigma_2 T^{m-2} + \cdots + (-1)^m \Sigma_m$.
En particulier, si $P = X^m + a_1 X^{m-1} + \cdots + a_m \in \mathbb{K}[X]$ scindé sur $\mathbb{K}$ et si $u_1, \dots, u_m$ sont ses racines, alors $\forall i$, $1 \le i \le m$, $(-1)^i a_i = \Sigma_i(u_1, \dots, u_m)$.

Remarque 57 : Si $\phi \in A[X_1, \dots, X_m]$, alors $\phi[\Sigma_1(X_1, \dots, X_m), \dots, \Sigma_m(X_1, \dots, X_m)]$ est un polynôme symétrique de $A[X_1, \dots, X_m]$.

Théorème 58 : Soit A un anneau commutatif unitaire et $P \in A[X_1, \dots, X_m]$ un polynôme symétrique dans $A[X_1, \dots, X_m]$. Il existe un unique polynôme $\phi \in A[X_1, \dots, X_m]$ tel que $P = \phi(\Sigma_1, \dots, \Sigma_m)$.

Exemple 59 : Dans $A[X_1, \dots, X_m]$, $\sum X_i^2 = \Sigma_1^2 - 2\Sigma_2$.
Si $P = X^3 + Y^3 + Z^3 \in \mathbb{R}[X, Y, Z]$ $P = \Sigma_1^3 - 3\Sigma_1\Sigma_2 + 3\Sigma_3$.

Références :

- Rombaldi Mathématiques pour l'agrégation Rom
- Daniel Perrin Cours d'Algèbre Per
- Xavier Gourdon Algèbre X.G
- Felix Ulmer Théorie des groupes Ulm