105

Groupe des permutations d'un ensemble fini. Applications.

I - Le groupe symétrique.

1) permutation d'un ensemble fini.

DEF 1 Soit E un ensemble fini. Une bijection de E dans E est appelée une permutation de E. On note $\mathcal{S}(E)$ l'ensemble des permutations de E.

PROP 2 $\mathcal{S}(E)$ muni de la loi de composition des application est un groupe.

DEF 3 Pour $E = \{1,\dots,n\}$ on note $\mathcal{S}_n$ au lieu de $\mathcal{S}(E)$.

PROP 4 Si $|E| = n$ alors $\mathcal{S}(E) \cong \mathcal{S}_n$, et $|\mathcal{S}_n| = n!$.

↳ On appelle $\mathcal{S}_n$ le groupe symétrique d'ordre n, on représente $\sigma \in \mathcal{S}_n$ par $\begin{pmatrix} 1 & 2 & \dots & n \\ \sigma(1) & \sigma(2) & \dots & \sigma(n) \end{pmatrix}$.

EX 5 $\mathcal{S}_3 = \left\{ \begin{pmatrix} 1&2&3\\1&2&3 \end{pmatrix}, \begin{pmatrix} 1&2&3\\1&3&2 \end{pmatrix}, \begin{pmatrix} 1&2&3\\2&1&3 \end{pmatrix}, \begin{pmatrix} 1&2&3\\3&2&1 \end{pmatrix}, \begin{pmatrix} 1&2&3\\2&3&1 \end{pmatrix}, \begin{pmatrix} 1&2&3\\3&1&2 \end{pmatrix} \right\}$ est le plus petit groupe non commutatif.

THM 6 Tout groupe G tel que $|G| = n$ est isomorphe à un sous groupe de $\mathcal{S}_n$.

Application on peut déduire de ce résultat une preuve des théorèmes de Sylow. $\boxed{\text{DEV}}$

2) $\mathcal{S}_n$ et son action naturelle.

DEF 7 On dit qu'un groupe G agit sur un ensemble E si il existe un morphisme de groupes φ tel que $\varphi : G \to \mathcal{S}(E)$.
L'action est dite fidèle si φ est injective, ie si G s'identifie à un sous-groupe de $\mathcal{S}(E)$.

EX 8 • l'identité donne une action fidèle de $\mathcal{S}_n$ sur $\{1,\dots,n\}$.
• $\mathcal{S}(E)$ agit naturellement sur E par : $\mathcal{S}(E) \times E \to E$, $(\sigma, x) \mapsto \sigma(x)$

PROP 9 L'action de $\mathcal{S}_n$ sur $\{1,\dots,n\}$ est transitive.

DEF 10 Pour $i \in \{1,\dots,n\}$ et $\sigma \in \mathcal{S}_n$ on note $O_\sigma(i) = \{\sigma^k(i), k \in \mathbb{Z}\}$, on dit que $O_\sigma(i)$ est la σ-orbite de i. Une σ-orbite est une partie de $\{1,\dots,n\}$ de la forme de $O_\sigma(i)$ pour au moins un i dans $\{1,\dots,n\}$.

DEF 11 On dit que $\sigma \in \mathcal{S}_n$ est un cycle si $\exists!$ σ-orbite O telle que $|O| > 1$. Le cardinal de O est appelé la longueur du cycle et O son support.

DEF 12 • Un q-cycle est un cycle de longueur q.
• Un 2-cycle est une transposition.

EX 13 • $\sigma = \begin{pmatrix} 1&2&3&4&5\\1&5&2&4&3 \end{pmatrix}$ est un 3-cycle de support $\{2,3,5\}$. On note $\sigma = (2,5,3)$
• $\begin{pmatrix} 1&2&3\\1&3&2 \end{pmatrix}$ est une transposition notée $(2,3)$

3) Générateurs

PROP 14 Les q-cycles sont conjugués dans $\mathcal{S}_n$, de plus ils sont d'ordre q.

THM 15 • Deux cycles à supports disjoints commutent.
• Tout $\sigma \in \mathcal{S}_n \setminus \{id\}$ est produit de cycles à supports deux à deux disjoints, et un tel produit est unique à ordre des facteurs près.

x 16 $\begin{pmatrix}1&2&3&4&5\\2&3&1&5&4\end{pmatrix} = (4,5)(1,2,3)$

RO 17 Soient $(i,j)\in\mathfrak{S}_n$ et $\sigma\in\mathfrak{S}_n$. On a $\sigma(i,j)\sigma^{-1} = (\sigma(i),\sigma(j))$
c $\mathfrak{S}_n$ agit transitivement par conjugaison sur l'ens-
ble des transpositions.

O 18 Toute transposition (i,j), $i<j$, est conjuguée
une transposition plus simple :
$(i,j) = \sigma(j-1,j)\sigma^{-1}$ où $\sigma = (i,i+1,\dots,j-1,j)$.

P 19 • Toute permutation $\sigma\in\mathfrak{S}_n$ est produit de transpositions.
• transpositions simples $\tau_i = (i,i+1)$, $i\in[\![1,n-1]\!]$, engendrent $\mathfrak{S}_n$.
• τ_1 et $\sigma = (1,2,\dots,n)$ engendrent $\mathfrak{S}_n$.

Le groupe alterné

Morphisme de signature

F 20 Soit $\sigma\in\mathfrak{S}_n$ un q cycle. La signature de σ
l'élément $\varepsilon(\sigma)\in\{-1,1\}$ défini par :
$\varepsilon(\sigma) = (-1)^{q-1}$.

P 21 L'application $\varepsilon : \sigma \mapsto \varepsilon(\sigma)$ est morphisme
groupe $\mathfrak{S}_n$ dans $\{-1,1\}$. Si $\sigma\in\mathfrak{S}_n$ est un produit
k transpositions on a $\varepsilon(\sigma) = (-1)^k$.

marque la signature est bien définie sur $\mathfrak{S}_n$
isque $\sigma\in\mathfrak{S}_n$ s'écrit de manière unique en produit
cycle à support disjoints.

22 $\varepsilon(id) = 1$ ... si τ est une transposition alors

THM 23 La signature est l'unique morphisme de groupe non trivial de $\mathfrak{S}_n$ dans $\mathbb{C}^*$.

CORO 24 Pour les décompositions de $\sigma\in\mathfrak{S}_n$ en produit de k transpositions, l'entier k a toujours la même parité.

DEF 25 Le noyau du morphisme de signature ε est appelé groupe alterné, noté $\mathfrak{A}_n$.

PROP 26 $\mathfrak{A}_n$ est un sous-groupe distingué de $\mathfrak{S}_n$ et $[\mathfrak{S}_n : \mathfrak{A}_n] = 2$ et $|\mathfrak{A}_n| = \frac{n!}{2}$.

2) Sous-groupes de $\mathfrak{S}_n$ et $\mathfrak{A}_n$

PROP 27 • si $n\geq 3$, $\mathfrak{A}_n$ est engendré par les $(1,i)(1,j)$ $2\leq i,j\leq n$ ou les 3-cycles $(1,2,i)$ $3\leq i\leq n$.
• $\mathfrak{A}_n$ est engendré par les σ^2, $\sigma\in\mathfrak{S}_n$.

PROP 28 $\mathfrak{A}_n$ est le seul sous-groupe d'indice 2 de $\mathfrak{S}_n$.

PROP 29 $\mathfrak{A}_n$ est simple pour $n=3$ et $n\geq 5$.

Ex 30 • les groupes d'isométrie d'un tétraèdre T sont $Isom(T)\simeq\mathfrak{S}_4$ et $Isom^+(T)\simeq\mathfrak{A}_4$, $\boxed{\text{DEV}}$
• les groupes d'isométrie d'un cube C sont $Isom(C)\simeq\mathfrak{S}_4\times\mathbb{Z}/2\mathbb{Z}$ et $Isom^+(C)\simeq\mathfrak{S}_4$.

III. Applications

1) Le déterminant

DEF 31 Soit K ...

des formes p-linéaires sur E est noté $\mathcal{L}(E,K)$

- f est dite alternée si $f(x_1 \dots x_p) = 0$ dès que deux vecteurs parmi les x_i sont égaux.
- f est dite antisymétrique si l'échange de deux vecteurs de $(x_1 \dots x_p)$ donne à f des valeurs opposées

PROP 32 f est antisymétrique ssi pour tout $\sigma \in \mathcal{S}_n$ $f(x_{\sigma(1)} \dots x_{\sigma(n)}) = \varepsilon(\sigma) f(x_1 \dots x_n)$.

THM 33 L'ensemble des formes n-linéaires alternées sur un K-espace vectoriel de dimension 1. En conséquence, il existe une unique forme n-linéaire alternée valant 1 sur une base donnée de E.

DEF 34 Soit $B = (e_1 \dots e_n)$ une base de E. La forme n-linéaire alternée valant 1 sur B est appelée déterminant dans la base B et on a

$$\det_B(x_1 \dots x_n) = \sum_{\sigma \in \mathcal{S}_n} \varepsilon(\sigma) x_{1\sigma(1)} \dots x_{n\sigma(n)}$$ où les

x_{ij} sont les coordonnées de x_i dans B $\forall i \in [\![1,n]\!]$.

2) Polynômes symétriques.

DEF 35 Un polynôme $P \in A[X_1, \dots, X_n]^*$ est dit symétrique si pour tout $\sigma \in \mathcal{S}_n$, on a :

$$P(X_{\sigma(1)}, \dots, X_{\sigma(n)}) = P(X_1 \dots X_n).$$

*A est un anneau intègre.

Ainsi $\mathcal{S}_n$ agit sur $A[X_1, \dots, X_n]$ où, $\forall \sigma \in \mathcal{S}_n$

$$\sigma . P(X_1 \dots X_n) = P(X_{\sigma(1)} \dots X_{\sigma(n)})$$

EX 36 On a : $P = XY + YZ + ZX$ est symétrique

- $P = X^2 + Y^2$ aussi.

C-EX 37 $P = X^2Y + Y$ n'est pas symétrique.

DEF 38 $n \in \mathbb{N}^*$, $k \leq n$. Le polynôme symétrique élémentaire de degré k, noté σ_k, dans $A[X_1, \dots, X_n]$, est :

$$\sigma_k = \sum_{I \subset \{1, \dots, n\}, |I| = k} \left(\prod_{i \in I} X_i \right)$$

Pour $k > n$, $\sigma_k = 0$

EX 39
- pour $n = 0$, $\sigma_0 = 1$, $\sigma_k = 0$ sinon
- $n = 1$, $\sigma_0 = 1$, $\sigma_1 = X_1$ ...
- $n \geq 2$, $\sigma_0 = 0$, $\sigma_1 = \sum_{1 \leq i \leq n} X_i$, $\sigma_2 = \sum_{1 \leq i < j \leq n} X_i X_j$

  et $\sigma_n = \prod_{i=1}^{n} X_i$

PROP 40
- pour tout $n \geq 0$, on a dans $\mathbb{Z}[X_1 \dots X_n][X]$

$$\prod_{1 \leq i \leq n} (X - X_i) = \sum_{0 \leq k \leq n} (-1)^k \sigma_k (X_1, \dots X_n) X^{n-k},$$

- si $P(X) = \sum_{0 \leq k \leq n} a_k X^k$ est un polynôme unitaire de degré n et de racines $x_1, \dots, x_n$ dans K corps on a :

$$a_{n-k} = (-1)^k \sigma_k (x_1, \dots, x_n) \quad \forall k \in [\![0,n]\!].$$

EX 41
- $P = X^3 + aX^2 + bX + c$ alors

  $x_1 + x_2 + x_3 = -a$; $x_1x_2 + x_1x_3 + x_3x_1 = b$

  et $x_1x_2x_3 = c$
- $P = X^2 + aX + b$

  $-a = x_1 + x_2$ et $b = x_1x_2$

Références :
- P. Tauvel, Cours d'Algèbre.
- Cortella A, Théorie des groupes
- F. Combes, Algèbre et géométrie
- J.P. Escofier, Théorie de Galois
- X. Gourdon, Algèbre.