

Chapitre 33

Groupe symétrique

Sommaire.

| | | |
|----------|-----------------------------------|----------|
| 1 | Permutations | 1 |
| 2 | Cycles. | 1 |
| 3 | Transpositions | 1 |
| 4 | Théorème de décomposition. | 1 |
| 5 | Signature | 1 |

Les propositions marquées de ★ sont au programme de colles.

1 Permutations

Définition 1

Une bijection de $\llbracket 1, n \rrbracket$ dans lui-même est appelée une **permutation** de $\llbracket 1, n \rrbracket$.

L'ensemble des permutations de $\llbracket 1, n \rrbracket$ sera noté S_n .

Exemple 2

Soient

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 5 & 4 & 3 & 1 \end{pmatrix} \quad \text{et} \quad \sigma' = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 4 & 1 & 5 \end{pmatrix}$$

Calculer $\sigma\sigma'$, $\sigma'\sigma$, σ^2 et σ^{-1} .

Solution :

On a :

$$\begin{aligned} \sigma\sigma' &= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 4 & 3 & 2 & 1 \end{pmatrix} & \sigma'\sigma &= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 5 & 1 & 4 & 2 \end{pmatrix} \\ \sigma^2 &= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 1 & 3 & 4 & 2 \end{pmatrix} & \sigma^{-1} &= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 1 & 4 & 3 & 2 \end{pmatrix} \end{aligned}$$

Proposition 3

- (S_n, \circ) est une groupe, appelé **groupe symétrique**.
- S_n est fini et son cardinal vaut $n!$.
- Ce groupe n'est pas abélien dès que $n \geq 3$.

Preuve :

[1] Cours sur les structures algébriques.

[2] On pose $\Phi : \begin{cases} S_n \rightarrow \mathcal{A}(\llbracket 1, n \rrbracket) \\ \sigma \mapsto (\sigma(1), \dots, \sigma(n)) \end{cases}$ bijective et $|\mathcal{A}(\llbracket 1, n \rrbracket)| = n!$.

[3] S_3 n'est pas abélien car $\tau := \dots$ et $\tau' = \dots$ ne commutent pas.
Soient $\sigma, \sigma' \in S_n \mid \sigma_{\{1,2,3\}} = \tau$ et $\sigma'_{\{1,2,3\}} = \tau'$, fixes sur $\llbracket 4, n \rrbracket$, alors $\sigma\sigma' \neq \sigma'\sigma$.

Définition 4: Vocabulaire

Soit $\sigma \in S_n$.

- Si $x \in \llbracket 1, n \rrbracket$, l'ensemble $\{\sigma^k(x), k \in \mathbb{Z}\}$ est appelé **orbite** de x .
- On dit que x est un **point fixe** de σ si $\sigma(x) = x$.
- On appelle **support** de σ l'ensemble des éléments de $\llbracket 1, n \rrbracket$ qui ne sont pas des points fixes.
- Deux permutations σ et σ' sont dites **conjuguées** s'il existe $\alpha \in S_n$ tel que $\sigma' = \alpha\sigma\alpha^{-1}$.

Proposition 5

Deux permutations dont les supports sont disjoints commutent.

Preuve :

Soient $\sigma, \sigma' \in S_n$. On note $S(\sigma) = \{x \in \llbracket 1, n \rrbracket \mid \sigma(x) \neq x\}$.

Supposons $S(\sigma) \cap S(\sigma') = \emptyset$.

Soit $x \in \llbracket 1, n \rrbracket$.

- Si $x \in S(\sigma) : x \notin S(\sigma')$ donc $\sigma\sigma'(x) = \sigma(x) \in S(\sigma)$ par bijectivité de σ .
- Si $x \notin S(\sigma) : \text{Soit } x \in S(\sigma') \text{ et on se ramène au 1er cas, soit } x \notin S(\sigma') \text{ et } \sigma\sigma'(x) = x = \sigma'\sigma(x)$.

Dans tous les cas, $\sigma\sigma'(x) = \sigma'\sigma(x)$

2 Cycles.

Définition 6: p -cycles

Soit p un entier supérieur à 2.

Une permutation γ est appelée un **p -cycle** s'il existe p éléments distincts a_1, \dots, a_p de $\llbracket 1, n \rrbracket$ tels que

$$a_1 \xrightarrow{\gamma} a_2 \xrightarrow{\gamma} \dots \xrightarrow{\gamma} a_p \xrightarrow{\gamma} a_1 \quad \text{et} \quad \forall b \in \llbracket 1, n \rrbracket \setminus \{a_1, \dots, a_p\} \quad \gamma(b) = b.$$

On note alors $\gamma = (a_1 \ a_2 \ \dots \ a_p)$.

Exemple 7: Conjugué d'un cycle

Soit $\gamma = (a_1, \dots, a_p)$ un p -cycle et $\sigma \in S_n$. Montrer que

$$\sigma\gamma\sigma^{-1} = (\sigma(a_1) \ \sigma(a_2) \ \dots \ \sigma(a_p)).$$

Solution :

Soit $b \in \llbracket 1, n \rrbracket \setminus \{\sigma(a_1), \dots, \sigma(a_p)\}$.

Alors $\sigma\gamma\sigma^{-1}(b) = \sigma\gamma(\sigma^{-1}(b)) = \sigma\sigma^{-1}(b) = b$ car $b \notin \{\sigma(a_1), \dots, \sigma(a_p)\}$ donc $\sigma^{-1}(b) \notin \{a_1, \dots, a_p\}$ donc c'est un point fixe de γ .

Soit $j \in \llbracket 1, p \rrbracket$, on a $\sigma\gamma\sigma^{-1}(\sigma(a_j)) = \sigma\gamma(a_j) = \sigma(a_{j+1})$ avec $a_{p+1} := a_1$.

On a bien que $\sigma\gamma\sigma^{-1}$ et $(\sigma(a_1) \ \dots \ \sigma(a_p))$ sont égaux en tout point.

Remarque: Ceci démontre que tous les p -cycles sont conjugués.

Soient $\gamma = (a_1 \ \dots \ a_p)$ et $\gamma' = (b_1 \ \dots \ b_p)$ deux p -cycles.

Posons $\sigma \in S_n$ telle que :

- $\forall j \in \llbracket 1, p \rrbracket \quad \sigma(a_j) = b_j$.
- Notons $\llbracket 1, n \rrbracket \setminus \{a_1, \dots, a_p\} := \{a'_1, \dots, a'_{n-p}\}$ et $\llbracket 1, n \rrbracket \setminus \{b_1, \dots, b_p\} := \{b'_1, \dots, b'_{n-p}\}$.

On pose alors $\forall i \in \llbracket 1, n-p \rrbracket \quad \sigma(a'_i) = b'_i$.

Alors σ est bien une bijection de $\llbracket 1, n \rrbracket$ dans lui-même car injective et de même cardinal.

On a donc $\gamma' = (b_1 \ \dots \ b_p) = (\sigma(a_1) \ \dots \ \sigma(a_p)) = \sigma\gamma\sigma^{-1}$ donc γ et γ' sont conjugués.

Exemple 8: Calculs sur un cycle

Soit $\gamma = (a_1 \ \dots \ a_p)$. Déterminer γ^{-1} et γ^p .

Solution :

La réciproque γ^{-1} :

Si $\gamma(b) = b$ alors $\gamma^{-1}(b) = b$ car c'est un point fixe.

Soit $j \in \llbracket 1, p-1 \rrbracket$, $\gamma(a_j) = a_{j+1}$ donc $a_j = \gamma^{-1}(a_{j+1})$.

Alors $\forall k \in \llbracket 2, p \rrbracket$, $\gamma^{-1}(a_k) = a_{k-1}$, et $\gamma^{-1}(a_1) = a_p$.

Ainsi, $\gamma^{-1} = (a_p \ a_{p-1} \ \dots \ a_2 \ a_1)$.

La puissance γ^p :

On a $\gamma = (a, \gamma(a), \dots, \gamma^{p-1}(a))$ pour un $a \in \llbracket 1, n \rrbracket$.

- $\gamma^p(a) = \gamma(\gamma^{p-1}(a)) = a$.
- Soit $j \in \llbracket 1, p-1 \rrbracket$, $\gamma^p(\gamma^j(a)) = \gamma^j(\gamma^p(a)) = \gamma^j(a)$.
- Soit $b \in \llbracket 1, n \rrbracket \setminus \{a, \gamma(a), \dots, \gamma^{p-1}(a)\}$, alors $\gamma^p(b) = b$ car point fixe.

Ainsi, $\forall x \in \llbracket 1, n \rrbracket$, $\gamma^p(x) = x$ donc $\gamma^p = id$.

Remarque: On pourrait aussi prouver que $p = \min\{j \in \mathbb{N}^* \mid \gamma^j = id\}$.

3 Transpositions

Définition 9

Une permutation τ qui est un 2-cycle est appelé une **transposition**.

Une transposition est donc une permutation de la forme (a, b) où $\{a, b\}$ est une paire de $\llbracket 1, n \rrbracket$.

Proposition 10: Involutivité

Si τ est une transposition, alors

$$\tau^2 = id \quad \text{et} \quad \tau^{-1} = \tau$$

Preuve :

C'est un 2-cycle donc $\tau^2 = id$.

On en déduit que $\tau^{-1} = \tau$.

Lemme 11: Décomposition d'un cycle en produit de transpositions

Soit $\gamma = (a_1 \ \dots \ a_p)$. Alors

$$\gamma = (a_1 \ a_2)(a_2 \ a_3) \dots (a_{p-1} \ a_p) \quad \text{ou} \quad \gamma = (a_1 \ a_p)(a_1 \ a_{p-1}) \dots (a_1 \ a_2)$$

Preuve :

Notons $\pi = (a_1 \ a_2)(a_2 \ a_3) \dots (a_{p-1} \ a_p)$. Montrons que $\gamma = \pi$.

- Soit $b \in \llbracket 1, n \rrbracket \setminus \{a_1, \dots, a_p\} : \gamma(b) = b$ et $\forall j \in \llbracket 1, p-1 \rrbracket$, $(a_j \ a_{j+1})(b) = b$ car $b \notin \{a_j, a_{j+1}\}$.
Alors $\gamma(b) = \pi(b) = b$.
- Soit $j \in \llbracket 1, p-1 \rrbracket$. Alors $\pi(a_j) = [\dots(a_{j-1} \ a_j)(a_j \ a_{j+1}) \dots](a_j) = [\dots(a_{j-1} \ a_j)](a_{j+1}) = a_{j+1}$.
- $\pi(a_p) = [(a_1 \ a_2) \dots (a_{p-1} \ a_p)](a_p) = [(a_1 \ a_2) \dots (a_{p-2} \ a_{p-1})](a_{p-1}) = \dots = a_1$

Donc $\forall x \in \llbracket 1, n \rrbracket \quad \gamma(x) = \pi(x)$

Remarque: On retrouve que $(1 \ 2)(2 \ 3) = (1 \ 2 \ 3)$ et $(2 \ 3)(1 \ 2) = (3 \ 2)(2 \ 1) = (3 \ 2 \ 1) = (1 \ 3 \ 2)$

On a $(1 \ 2)(2 \ 3) \neq (2 \ 3)(1 \ 2)$.

4 Théorème de décomposition.

Théorème 12: Décomposition en produit de cycles à supports disjoints

Soit $\sigma \in S_n$. Il existe $\gamma_1, \dots, \gamma_r$ r cycles à supports disjoints tels que

$$\sigma = \gamma_1 \gamma_2 \dots \gamma_r.$$

Les γ_i commutent et cette décomposition est unique à l'ordre près.

Preuve :

Soit $\sigma \in S_n$.

Pour **relation d'équivalence** sur $\llbracket 1, n \rrbracket$.

On écrit $i, j \in \llbracket 1, n \rrbracket$, on note $i \sim j$ si $\exists k \in \mathbb{Z} \mid j = \sigma^k(i)$.

- Soit $i \in \llbracket 1, n \rrbracket$, $i = \sigma^0(i)$ donc $i \sim i$.
- Soient $i, j \in \llbracket 1, n \rrbracket \mid i \sim j$. Alors $\exists k \in \mathbb{Z} \mid j = \sigma^k(i) : i = \sigma^{-k}(j)$ et $j \sim i$.
- Soient $h, i, j \in \llbracket 1, n \rrbracket \mid h \sim i$ et $i \sim j : \exists k, l \in \mathbb{Z} \mid i = \sigma^k(h)$ et $j = \sigma^l(i)$ donc $j = \sigma^{l+k}(h)$ et $j \sim h$.

Il existe alors une partition de $\llbracket 1, n \rrbracket$ en classes d'équivalences.

On fixe $x \in \llbracket 1, n \rrbracket$, prouvons qu'il existe $p \in \mathbb{N}^*$ tel que $[x] = \{x, \sigma(x), \dots, \sigma^{p-1}(x)\}$.

On pose $p = \min\{k \in \mathbb{N}^* \mid \sigma^k(x) = x\}$. Cet ensemble est minoré et non-vidé car :

$$S : \begin{cases} \mathbb{Z} \rightarrow \llbracket 1, n \rrbracket \\ k \mapsto \sigma^k(x) \end{cases} \quad \text{n'est pas injective.}$$

Ainsi, $\exists k, k' \in \mathbb{Z} \mid k < k'$ et $\sigma^k(x) = \sigma^{k'}(x)$ donc $\sigma^{k'-k}(x) = x$.

Or $k' - k \in \mathbb{N}^*$, donc $\{k \in \mathbb{N}^* \mid \sigma^k(x) = x\} \neq \emptyset$.

Il faut montrer que $[x] = \{x, \sigma(x), \dots, \sigma^{p-1}(x)\}$.

[\supseteq] est trivial.

[\subset] Soit $y \in [x] : \exists k \in \mathbb{Z} \mid y = \sigma^k(x)$.

Par division euclidienne : $\exists!(q, r) \in \mathbb{Z}^2 \mid k = qp + r$ et $0 \leq r \leq p-1$.

Donc $y = \sigma^k(x) = \sigma^{qp+r}(x) = \sigma^r(\sigma^{pq}(x)) = \sigma^r(x) = y : y \in \{x, \sigma(x), \dots, \sigma^{p-1}(x)\}$.

Notons A_1, \dots, A_r les classes d'équivalences non triviales de \sim . On a prouvé que :

$$\forall j \in \llbracket 1, r \rrbracket \quad \exists x_j \in \llbracket 1, n \rrbracket \quad \exists p_j \in \mathbb{N}^* \mid A_j = \{x_j, \sigma(x_j), \dots, \sigma^{p_j-1}(x_j)\}.$$

On pose alors $\gamma_j = (x_j \ \sigma(x_j) \ \dots \ \sigma^{p_j-1}(x_j))$, il est clair que $\sigma = \gamma_1 \gamma_2 \dots \gamma_r$.

Exemple 13: Une décomposition

$$\text{Soit } \sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 5 & 4 & 1 & 7 & 8 & 6 & 2 & 3 \end{pmatrix}.$$

- Décomposer σ en produit de cycles à supports disjoints.
- Déterminer σ^4 , σ^{12} et σ^{666} .

Solution :

[1] $\sigma = (1 \ 5 \ 8 \ 3)(2 \ 4 \ 7)$

[2] On a :

- $\sigma^{12} = (\gamma_1 \gamma_2)^{12} = \gamma_1^4 \gamma_2^4 = \gamma_2$ car $\gamma_1^4 = id$ et $\gamma_2^4 = \gamma_2^3 \gamma_2 = \gamma_2$.
- $\sigma^{666} = (\gamma_1^3)(\gamma_2^3)^{11} = id$
- $\sigma^{666} = (1 \ 8)(3 \ 5)$ car $\sigma^{666} = \sigma^{12 \times 55 \times 6} = id^{55} \sigma^6$.

Corrolaire 14

Toute permutation est un produit de transpositions.

La décomposition n'est pas unique et les transpositions ne commutent pas nécessairement.

Preuve :

Soit $\sigma \in S_n$.

Le théorème 12 nous dit que : σ s'écrit comme un produit de cycles. (à supports disjoints)

Or tout cycle s'écrit comme un produit de transpositions.

Donc, si $\gamma = (a_1 a_2 \dots a_p)$, alors $\gamma = (a_1 a_2) \dots (a_{p-1} a_p)$ et σ s'écrit comme produit de produit de transpositions.

Exemple 15

Décomposer en produit de transpositions la permutation :

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 7 & 5 & 1 & 2 & 4 & 6 & 3 \end{pmatrix}$$

Solution :

$\sigma = (173)(254)$ (produit de cycles)

$\sigma = (17)(73)(25)(54)$

5 Signature

Définition 16

Soit $\sigma \in S_n$.

- Une paire $\{i, j\}$ de $\llbracket 1, n \rrbracket$ est une **inversion** pour σ si $i < j$ et $\sigma(i) > \sigma(j)$ sont de signe opposé.
- Le nombre d'inversion de σ est noté $Inv(\sigma)$
- On appelle **signature** de σ le nombre $\varepsilon(\sigma) = (-1)^{Inv(\sigma)}$

Exemple 17

Après avoir calculé son nombre d'inversions, donner la signature de

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 1 & 2 & 5 & 3 \end{pmatrix}$$

Solution :

On va calculer $\varepsilon(\sigma)$ en comptant le nombre d'inversions.

Il y a $\binom{5}{2}$ paires dans $\llbracket 1, 5 \rrbracket$.

| paire | $\{1, 2\}$ | $\{1, 3\}$ | $\{1, 4\}$ | $\{1, 5\}$ | $\{2, 3\}$ | $\{2, 4\}$ | $\{2, 5\}$ | $\{3, 4\}$ | $\{3, 5\}$ | $\{4, 5\}$ |
|-----------|------------|------------|------------|------------|------------|------------|------------|------------|------------|------------|
| inversion | ✓ | ✓ | ✗ | ✓ | ✗ | ✗ | ✗ | ✗ | ✗ | ✓ |

Ainsi on a $Inv(\sigma) = 4$ donc $\varepsilon(\sigma) = (-1)^4 = 1$

Proposition 18

- L'identité id pour signature 1.
- Les transpositions ont pour signature -1 .

Preuve :

[1] Il est clair que $Inv(id_{\llbracket 1, n \rrbracket}) = 0$ donc $\varepsilon(\sigma) = 1^0 = 1$.

[2] Soit $\{i, j\}$ une paire de $\llbracket 1, n \rrbracket$, $\tau \in S_n : \exists(a, b) \in \llbracket 1, n \rrbracket \mid \tau = (a, b)$ où $a \leq b$.

- Cas $\{i, j\} \cap \{a, b\} = \emptyset : \tau(i) = i$ et $\tau(j) = j$ donc $i < j$ est de même signe.
- Cas $i = a$ et $j \neq b : \tau(a) = b$ et $\tau(j) = j : \llbracket a+1, b-1 \rrbracket$.
- Cas $i \neq a, j = b : \tau(i) = i$ et $\tau(b) = a : \llbracket a+1, b-1 \rrbracket$.
- Cas $\{i, j\} = \{a, b\} : \tau(a) = b$ et $\tau(b) = a$, c'est une inversion.

Bilan : $Inv(\tau) = 2\llbracket a+1, b-1 \rrbracket + 1 = 2(b-a) - 1$, impair.

Donc $\varepsilon(\tau) = -1$.

Proposition 19: La signature comme un produit

$$\forall \sigma \in S_n \quad \varepsilon(\sigma) = \prod_{\{i,j\}} \frac{\sigma(i) - \sigma(j)}{i - j}$$

Preuve :

Fixons $\{i, j\} \in \mathcal{P}_2(\llbracket 1, n \rrbracket)$ (ensembles des paires)

On a

$$\frac{\sigma(i) - \sigma(j)}{i - j} = (-1)^{x_{\{i,j\}}} \left| \frac{\sigma(i) - \sigma(j)}{i - j} \right| \quad \text{où} \quad x_{\{i,j\}} = \begin{cases} 0 & \text{si } i, j \text{ n'est pas une inversion.} \\ 1 & \text{sinon.} \end{cases}$$

Alors :