Chapitre 33

Groupe Symétrique

1 Permutations

Définition 1

Une bijection de $[\![1,n]\!]$ dans lui-même est appelée une **permutation** de $[\![1,n]\!]$.

L'ensemble des permutations de $[\![1,n]\!]$ 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}.

Preuve :

On a :

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

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

Proposition 3

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

Preuve :

$\boxed{1}$ Cours sur les structures algébriques.

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

$\boxed{3}$ S_3 n'est pas abélien car $\tau :=$ ... et $\tau' =$ ... ne commutent pas.

Soient $\sigma, \sigma' \in S_n \mid \sigma_{|\{1,2,3\}} = \tau$ et $\sigma'_{|\{1,2,3\}} = \tau'$, fixes sur $[\![4,n]\!]$, alors $\sigma\sigma' \neq \sigma'\sigma$.

Définition 4: Vocabulaire

Soit $\sigma \in S_n$.

1. Si $x \in [\![1,n]\!]$, l'ensemble $\{\sigma^k(x), k \in \mathbb{Z}\}$ est appelé **orbite** de x.
2. On dit que x est un **point fixe** de σ si $\sigma(x) = x$.
3. On appelle **support** de σ l'ensemble des éléments de $[\![1,n]\!]$ qui ne sont pas des points fixes.
4. 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 $S(\sigma) = \{x \in [\![1, n]\!] \mid \sigma(x) \neq x\}$.

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

Soit $x \in [\![1, n]\!]$.

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

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

2 Cycles.

Définition 6

Soit p un entier supérieur à 2.

Une permutation γ est appellée un p-**cycle** s'il existe p éléments distincts $a_1, ..., a_p$ de $[\![1, n]\!]$ tels que

$$a_1 \overset{\gamma}{\mapsto} a_2 \overset{\gamma}{\mapsto} ... \overset{\gamma}{\mapsto} a_p \overset{\gamma}{\mapsto} a_1.$$

$$\text{et} \quad \forall b \in [\![1, n]\!] \setminus \{a_1, ..., a_p\} \ \gamma(b) = b.$$

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

Exemple 7: Conjugué d'un cycle

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

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

Preuve :

Soit $b \in [\![1, n]\!] \setminus \{\sigma(a_1), ..., \sigma(a_p)\}$.

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

Soit $j \in [\![1, p]\!]$.

Alors $\sigma\gamma\sigma^{-1}(\sigma(a_j)) = \sigma\gamma(a_j) = \sigma(a_{j+1})$ avec $a_{p+1} := a_1$.

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

[0.2cm] **Remarque:** Ceci démontre que tous les p-cycles sont conjugués.

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

Posons $\sigma \in S_n$ telle que :

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

On pose alors $\forall i \in [\![1, n-p]\!] \ \sigma(a'_i) = b'_i$.

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

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

Exemple 8: Calculs sur un cycle

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

Preuve :

La réciproque γ^{-1} :

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

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

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

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

[0.2cm] **La puissance γ^p :**

On a $\gamma = (a, \gamma(a), ..., \gamma^{p-1}(a))$ pour un $a \in [\![1, n]\!]$.

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

Ainsi, $\forall x \in [\![1, n]\!], \ \gamma^p(x) = x$ 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 $[\![1, n]\!]$.

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

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

Preuve :

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

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

Donc $\forall x \in [\![1, n]\!] \ \gamma(x) = \pi(x)$

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 $\gamma_1, ..., \gamma_r$ r cycles à supports disjoints tels que

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

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

Preuve :

Soit $\sigma \in S_n$.

Une relation d'équivalence sur $[\![1, n]\!]$.

Pour $i, j \in [\![1, n]\!]$, on note $i \sim j$ si $\exists k \in \mathbb{Z} \mid j = \sigma^k(i)$.

- Soit $i \in [\![1, n]\!]$. $i = \sigma^0(i)$ donc $i \sim i$.
- Soient $i, j \in [\![1, n]\!] \mid i \sim j$. Alors $\exists k \in \mathbb{Z} \mid j = \sigma^k(i)$: $i = \sigma^{-k}(j)$ et $j \sim i$.
- Soient $h, i, j \in [\![1, n]\!] \mid h \sim i$ 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 $[\![1, n]\!]$ en classes d'équivalences.

On fixe $x \in [\![1, n]\!]$.

Prouvons qu'il existe $p \in \mathbb{N}^*$ tel que $[x] = \{x, \sigma(x), ..., \sigma^{p-1}(x)\}$.

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

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

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 $\{k \in \mathbb{N}^* \mid \sigma^k(x) = x\} \neq \varnothing$.

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

$\boxed{\supset}$ est trivial.

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

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

$$\forall j \in [\![1, r]\!] \ \exists x_j \in [\![1, n]\!] \ \exists p_j \in \mathbb{N}^* \mid A_j = \{x_j, \sigma(x_j), ..., \sigma^{p_j - 1}(x_j)\}.$$

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

Exemple 13: Une décomposition

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

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

Preuve :

$\boxed{1}$ $\sigma = (1 \ 5 \ 8 \ 3)(2 \ 4 \ 7)$

$\boxed{2}$

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

Corrolaire 14

Toute permutation est un produit de transpositions.

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

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.

En effet si

$\gamma = (a_1 a_2 ... a_p)$

Alors $\gamma = (a_1 a_2)(a_3 a_4)...(a_{p-1} a_p)$

σ s'écrit donc comme un produit de produit de transpositions.

Exemple 15

Décomposer en produit de transpositions la permutation

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

Preuve :

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

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

5 Signature

Définition 16

Soit $\sigma \in S_n$

1. Une paire $\{i, j\}$ de $[\![1, n]\!]$ est une **inversion** pour σ si $i - j$ et $\sigma(i) - \sigma(j)$ sont de signe opposé.
2. Le nombre d'inversion de σ est noté $Inv(\sigma)$
3. 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

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

Preuve :

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

Il y a $\binom{5}{2}$ paires dans $[\![1, 5]\!]$

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: TODO PRUVE PROPRE

1. L'identité a pour signature 1.

2. Les transpositions ont pour signature -1.

Preuve :

$\boxed{1}$ Il est clair (?)

que $Inv(id_{[\![1,n]\!]}) = 0$ donc $\varepsilon(\sigma) = 1^0 = 1$.

$\boxed{2}$ Soit $\{1, j\}$ une paire de $[\![1, n]\!]$,

$\tau \in S_n$: $\exists (a, b) \in [\![1, n]\!] \mid \tau = (a\ b)$ où $a \leq b$.

- Cas $\{i, j\} \cap \{a, b\} = \varnothing$: $\tau(i) = i$ et $\tau(j) = j$ donc $i - j$ est de même signe.
- Cas $i = a$ et $j \neq b$: $\tau(a) = b$ et $\tau(j) = j$: $|[\![a + 1, b - 1]\!]$.
- Cas $i \neq a, j = b$: $\tau(i) = i$ et $\tau(b) = a$: $|[\![a + 1, b - 1]\!]$.
- Cas $\{i, j\} = \{a, b\}$

  Alors $\tau(a) = b$ et $\tau(b) = a$, c'est une inversion.

Bilan : $Inv(\tau) = 2|[\![a + 1, b - 1]\!]| + 1 = 2(b - a) - 1$, impair.

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

Proposition 19: La signature comme un produit

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

Preuve :

Fixons $\{i, j\} \in \mathcal{P}_2([\![1, n]\!])$ (ensembles des paires)

On a $\frac{\sigma(i)-\sigma(j)}{i-j} = (-1)^{x_{\{i,j\}}} |\frac{\sigma(i)-\sigma(j)}{i-j}|$

où $x_{\{i,j\}} = \begin{cases} 0 & \text{si i, j n'est pas une inversion} \\ 1 & \text{sinon.} \end{cases}$

$\prod_{\{i,j\}} \frac{\sigma(i)-\sigma(j)}{i-j} = \prod_{\{i,j\}} (-1)^{x_{\{i,j\}}} |\frac{\sigma(i)-\sigma(j)}{i-j}| = (-1)^{\sum_{\{i,j\}} x_{\{i,j\}}} \times \prod_{\{i,j\}} |\frac{\sigma(i)-\sigma(j)}{i-j}|$

Or $\sum_{\{i,j\}} x_{\{i,j\}} = Inv(\sigma)$ donc $(-1)^{\sum_{\{i,j\}}} = \varepsilon(\sigma)$

Reste à prouver $\prod_{\{i,j\}} |\frac{\sigma(i)-\sigma(j)}{i-j}| = 1$

Le produit vaut 1 car

$\varphi : \begin{cases} \mathcal{P}_2([\![1, n]\!]) \to \mathcal{P}_2([\![1, n]\!]) \\ \{i, j\} \mapsto \{\sigma(i), \sigma(j)\} \end{cases}$ est une bijection.

On pose alors le changement d'indice $\{u, v\} = \{\sigma(i), \sigma(j)\}$

$\prod_{\{i,j\}} |\sigma(i) - \sigma(j)| = \prod_{\{u,v\}} |u - v| = \prod_{\{i,j\}} |i - j|$

Théorème 20: TODO PREUVE PROPRE

La signature est l'unique application $\varepsilon : S_n \to \{-1, 1\}$ telle que

1. $\forall \sigma, \sigma' \in S_n \quad \varepsilon(\sigma\sigma') = \varepsilon(\sigma)\varepsilon(\sigma')$
2. Pour toute transposition $\tau \in S_n,\ \varepsilon(\tau) = -1$

Preuve :

$\boxed{1}$ TODO

$\boxed{2}$ On le sait déjà (proposition 18)

Unicité : Soit $\delta : S_n \to \{-1, 1\}$ une fonction qui vérifie 1. et 2.

Montrons que $\gamma = \varepsilon$ (ε la signature)

Soit $\sigma \in S_n$, $\exists r \in \mathbb{N}^*\ \exists \tau_1, \tau_2, ..., \tau_r$ transpositions : $\sigma = \tau_1\tau_2...\tau_r$.

Alors

$$\begin{aligned}\delta(s) &= \prod_{i=1}^{r}(-1)\\ &= \varepsilon(\tau_1)\varepsilon(\tau_2)...\varepsilon(\tau_r)\\ &= \varepsilon(\tau_1\tau_2...\tau_r)(1)\\ &= \varepsilon(\sigma)\end{aligned}$$

Corrolaire 21

La signature est l'unique morphisme de groupes non trivial de $(S_n, \circ)$ dans $(\mathbb{C}^*, \times)$

Preuve :

- La fonction constante
  $\mathbb{1} : \begin{cases} S_n \to \mathbb{C}^* \\ \sigma \mapsto 1 \end{cases}$ est un morphisme de groupes dit morphisme trivial
- La signature ε est un morphisme de groupes de S_n dans $\mathbb{C}^*$. Il est non trivial car si τ est une transposition $\varepsilon(\tau) = -1$
- Unicité Soit $f : S_n \to \mathbb{C}^*$ un morphisme de groupes.

  Soit τ transpositions fixée. $\tau^2 = id$

  Appliquons f :

  $f(\tau^2) = f(id) = 1 \Longrightarrow f(\tau)^2 = -1$ ou 1
- 1^{er} cas : $f(\tau) = 1$

  Soit τ', conjuguée à τ

  $\exists \alpha \in S_n,\ \tau' = \alpha\tau\alpha^{-1}$ (on a prouvé plutôt que 2 p-cycles sont conjugués)

  $f(\tau') = f(\alpha\tau\alpha^{-1}) = f(\alpha)\cancel{f(\tau)}f(\alpha)^{-1} = 1$

  or toute permutation est produit de transpositions $\Longrightarrow\ \forall \sigma \in S_n f(\sigma) = 1$.
- 2ème cas $f(\tau) = -1$

  Par conjugaison, $\forall \tau'$ transpositions $f(\tau') = -1$

  f est un morphisme de groupe envoyant sur -1.