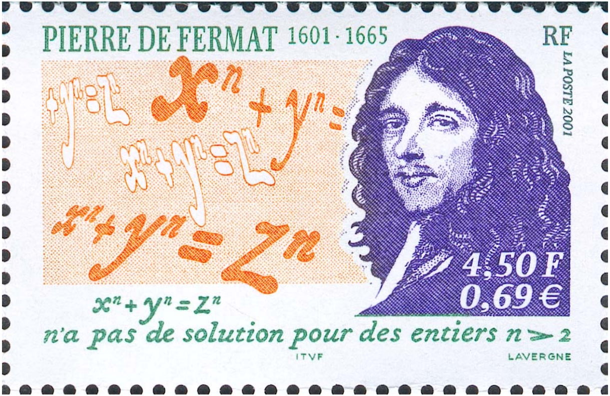

Leçon 64 - Groupes symétriques

7 & 11 février 2025

⇒ Décomposition en produit de cycles/de transpositions

⇒ Séparation en deux parties, selon la signature

⇒ Décomposition en produit de cycles/de transpositions

⇒ Séparation en deux parties, selon la signature

Transpositions

Défnition - Transposition

Soit $(a,b) \in [\![1,n]\!]^2$, $a \neq b$. La permutation $\tau_{a,b}$ définie par

$$\tau_{a,b}(a) = b,\ \tau_{a,b}(b) = a, \qquad \forall x \in [\![1,n]\!] \setminus \{a,b\},\ \tau_{a,b}(x) = x$$

s'appelle la transposition de a et b.

Cycles

Définition - Cycle

Soient $a_1, \ldots, a_p$ $(p \leqslant n)$ des éléments distincts de $[\![1, n]\!]$.
La permutation σ telle que

$$\sigma(a_1) = a_2, \sigma(a_2) = a_3, \ldots, \sigma(a_{p-1}) = a_p, \sigma(a_p) = a_1$$

$$\text{et } \forall x \notin \{a_1, a_2, \ldots, a_p\}, \sigma(x) = x$$

s'appelle un cycle de longueur p ou p-cycle, on le note $(a_1\, a_2\, \ldots\, a_p)$.
L'ensemble $\{a_1, a_2, \ldots, a_p\}$ s'appelle le support du cycle.
Deux cycles sont dits disjoints si leurs supports sont disjoints.

Classe de conjugaison

Proposition - Classe de conjugaison

Soit σ une permutation de $\mathbb{N}_n$ et $c = (a_1 \dots a_k)$ un cycle.
Alors $\sigma \circ c \circ \sigma^{-1}$ est le cycle $\big(\sigma(a_1) \dots \sigma(a_k)\big)$.

Classe de conjugaison

Proposition - Classe de conjugaison

Soit σ une permutation de $\mathbb{N}_n$ et $c = (a_1 \dots a_k)$ un cycle.
Alors $\sigma \circ c \circ \sigma^{-1}$ est le cycle $\big(\sigma(a_1) \dots \sigma(a_k)\big)$.

Démonstration

Classe de conjugaison

Proposition - Classe de conjugaison

Soit σ une permutation de $\mathbb{N}_n$ et $c = (a_1 \dots a_k)$ un cycle.
Alors $\sigma \circ c \circ \sigma^{-1}$ est le cycle $\big(\sigma(a_1) \dots \sigma(a_k)\big)$.

Démonstration

Remarque Nom arbitraire

Ordre d’un élément dans un groupe

Analyse Ordre d’un élément.

Ordre d'un élément dans un groupe

Analyse Ordre d'un élément.

Définition - Ordre d'un élément / ordre d'une permutation

Soit σ une permutation de E et $x \in E$.
On appelle ordre de x (pour σ), le nombre
$k = \min\{i \in \mathbb{N}^* \mid \sigma^i(x) = x\}$.
On appelle ordre de σ, le nombre
$k = \min\{i \in \mathbb{N}^* \mid \forall\ x \in E, \sigma^i(x) = x\}$.

Ordre d'un élément dans un groupe

Analyse Ordre d'un élément.

Définition - Ordre d'un élément / ordre d'une permutation

Soit σ une permutation de E et $x \in E$.
On appelle ordre de x (pour σ), le nombre $k = \min\{i \in \mathbb{N}^* \mid \sigma^i(x) = x\}$.
On appelle ordre de σ, le nombre $k = \min\{i \in \mathbb{N}^* \mid \forall\ x \in E, \sigma^i(x) = x\}$.

<u>Exercice</u>

Montrer que l'ordre de σ est le ppcm des ordres de tous les x de E.

Ordre d'une permutation

Proposition - Ordre d'un cycle

Si c est un cycle de longueur p, alors $c^p = \mathrm{id}$.
Mieux : p est l'ordre du cycle

Ordre d'une permutation

Proposition - Ordre d'un cycle

Si c est un cycle de longueur p, alors $c^p = \mathrm{id}$.
Mieux : p est l'ordre du cycle

Démonstration

⇒ Décomposition en produit de cycles/de transpositions

⇒ Séparation en deux parties, selon la signature

Sous-groupe engendré par une partie

Nous rappelons du vocabulaire valable pour toute la théorie des groupes.

Sous-groupe engendré par une partie

Nous rappelons du vocabulaire valable pour toute la théorie des groupes.

Sous-groupe engendré par une partie

Soit $(G,\star)$ un groupe et S, une partie de G.
On appelle sous-groupe de G, engendré par S, le plus petit sous-groupe de G (au sens de l'inclusion) qui contient S.
On le note $<S>$.
On a donc la caractéristique suivante :

$$<S> < G \text{ et } (S \subset H, H < G) \Rightarrow <S> \subset H$$

Description explicite

Comme pour les espaces vectoriels, on dispose d'une description explicite.

Description explicite

Comme pour les espaces vectoriels, on dispose d'une description explicite.

Sous-groupe engendré par une partie

Soit $(G, \star)$ un groupe et S, une partie de G.

$$< S >= \{x_1^{\epsilon_1} \star \ldots x_n^{\epsilon_n} ; n \in \mathbb{N}, \forall\ i \in \mathbb{N}_n, x_i \in S, \epsilon_i \in \{-1, 1\}\}$$

Description explicite

Comme pour les espaces vectoriels, on dispose d'une description explicite.

Sous-groupe engendré par une partie

Soit $(G, \star)$ un groupe et S, une partie de G.

$$< S >= \{x_1^{\epsilon_1} \star \ldots x_n^{\epsilon_n} ; n \in \mathbb{N}, \forall\ i \in \mathbb{N}_n, x_i \in S, \epsilon_i \in \{-1, 1\}\}$$

Démonstration

Description explicite

Comme pour les espaces vectoriels, on dispose d'une description explicite.

Sous-groupe engendré par une partie

Soit $(G, \star)$ un groupe et S, une partie de G.

$$< S >= \{x_1^{\epsilon_1} \star \dots x_n^{\epsilon_n}; n \in \mathbb{N}, \forall\ i \in \mathbb{N}_n, x_i \in S, \epsilon_i \in \{-1,1\}\}$$

Démonstration

Exercice :

Dans $G = \frac{\mathbb{Z}}{n\mathbb{Z}}$, avec la loi $\overline{+}$, montrer que $< r >= G \iff r \wedge n = 1$

⇒ Décomposition en produit de cycles/de transpositions

⇒ Séparation en deux parties, selon la signature

« Chasles »

Analyse - Quelques exemples

« Chasles »

Analyse - Quelques exemples

Si les cycles ne sont pas à supports disjoints :

« Chasles »

Analyse - Quelques exemples

Si les cycles ne sont pas à supports disjoints :

Proposition - Pseudo-Chasles

Soient $a_i, a_j a_k$ distincts.

Alors $(a_j\, a_i) \circ (a_i\, a_k) = (a_j\, a_i\, a_k)$

« Chasles »

Analyse - Quelques exemples
Si les cycles ne sont pas à supports disjoints :

Proposition - Pseudo-Chasles

Soient $a_i, a_j a_k$ distincts.
Alors $(a_j\, a_i) \circ (a_i\, a_k) = (a_j\, a_i\, a_k)$

Démonstration

« Chasles »

Analyse - Quelques exemples

Si les cycles ne sont pas à supports disjoints :

Proposition - Pseudo-Chasles

Soient $a_i, a_j a_k$ distincts.

Alors $(a_j\, a_i) \circ (a_i\, a_k) = (a_j\, a_i\, a_k)$

Démonstration

Plus largement :

Exercice : Montrer que $(a_1\, a_2\, a_3) \circ (a_3\, a_4\, a_1) = (a_2\, a_3\, a_4)$

Orbite

Définition - Orbite de x

Soit σ une permutation de $[\![1,n]\!]$.
La relation définie sur $[\![1,n]\!]$ par

$$x\mathscr{R}_\sigma y \Longleftrightarrow \exists k \in \mathbb{Z}, y = \sigma^k(x)$$

est une relation d'équivalence.
Pour $x \in [\![1,n]\!]$, il existe un unique $p \in \mathbb{N}^*$ tel que $x, \sigma(x), \dots, \sigma^{p-1}(x)$ soient deux à deux distincts et $\sigma^p(x) = x$.
La classe d'équivalence de x pour la relation $\mathscr{R}_\sigma$ est alors l'ensemble $\{x, \sigma(x), \dots, \sigma^{p-1}(x)\}$, appelé **orbite** de x.

Orbite

Définition - Orbite de x

Soit σ une permutation de $[\![1,n]\!]$.
La relation définie sur $[\![1,n]\!]$ par

$$x \mathscr{R}_\sigma y \iff \exists k \in \mathbb{Z}, y = \sigma^k(x)$$

est une relation d'équivalence.
Pour $x \in [\![1,n]\!]$, il existe un unique $p \in \mathbb{N}^*$ tel que $x, \sigma(x), \ldots, \sigma^{p-1}(x)$ soient deux à deux distincts et $\sigma^p(x) = x$.
La classe d'équivalence de x pour la relation $\mathscr{R}_\sigma$ est alors l'ensemble $\{x, \sigma(x), \ldots, \sigma^{p-1}(x)\}$, appelé **orbite** de x.

Démonstration

Orbite

Définition - Orbite de x

Soit σ une permutation de $[\![1,n]\!]$.
La relation définie sur $[\![1,n]\!]$ par

$$x\mathscr{R}_\sigma y \iff \exists k \in \mathbb{Z}, y = \sigma^k(x)$$

est une relation d'équivalence.
Pour $x \in [\![1,n]\!]$, il existe un unique $p \in \mathbb{N}^*$ tel que $x, \sigma(x), \ldots, \sigma^{p-1}(x)$ soient deux à deux distincts et $\sigma^p(x) = x$.
La classe d'équivalence de x pour la relation $\mathscr{R}_\sigma$ est alors l'ensemble $\{x, \sigma(x), \ldots, \sigma^{p-1}(x)\}$, appelé **orbite** de x.

Démonstration

Exercice

Montrer qu'il s'agit bien d'une relation d'équivalence

Décomposition en produit de cycles

Théorème - Décomposition en produit de cycles à supports disjoints

Toute permutation autre que l'identité se décompose, de manière unique à l'ordre près des facteurs, en un produit de cycles à supports deux à deux disjoints.
Plus précisément, ces cycles sont entièrement déterminés par σ : leur nombre est égal au nombre d'orbites non réduites à un élément de σ et ils sont égaux aux restrictions de σ à chacune des orbites.

Décomposition en produit de cycles

Théorème - Décomposition en produit de cycles à supports disjoints

Toute permutation autre que l'identité se décompose, de manière unique à l'ordre près des facteurs, en un produit de cycles à supports deux à deux disjoints.
Plus précisément, ces cycles sont entièrement déterminés par σ : leur nombre est égal au nombre d'orbites non réduites à un élément de σ et ils sont égaux aux restrictions de σ à chacune des orbites.

Démonstration

Cycles (Savoir-faire)

Savoir-faire. Comment décrire une permutation en produit de cycles

On suppose que la permutations sous la forme d'une liste double.

On peut imaginer que $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & \dots \\ s_1 & s_2 & s_3 & s_4 & \dots \end{pmatrix}$

On procède, en plusieurs temps, en suivant les chemins ....

- On est choisit librement premier élément du cycle : il ne doit pas être un point fixe.
  On le note k $\Longrightarrow (k, \qquad)$
- On se dirige alors en s_k. $\Longrightarrow (k, s_k \qquad)$
- On se dirige ensuite en $s(s_k)$. $\Longrightarrow (k, s_k, s(s_k) \qquad)$
- $\dots$
- On continue ainsi jusqu'à trouver à nouveau k.

Cycles (Savoir-faire)

Savoir-faire. Comment décrire une permutation en produit de cycles

On suppose que la permutations sous la forme d'une liste double.

On peut imaginer que $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & \dots \\ s_1 & s_2 & s_3 & s_4 & \dots \end{pmatrix}$

On procède, en plusieurs temps, en suivant les chemins $\dots$

Si la permutation considérée est un cycle, l'écriture est terminée.

Sinon, on continue avec les nombres qui n'était pas dans le 1er cycle.

Exercices

<u>Exercice</u>

Soit $A \in \mathscr{M}_n(\mathbb{K})$ une matrice qui possède exactement un 1 par ligne et par colonne et que des zéros sinon.

Montrer qu'il existe k tel que $A^k = I_n$.

⇒ Décomposition en produit de cycles/de transpositions

⇒ Séparation en deux parties, selon la signature

Transpositions quelconques

On commence par une proposition :

Proposition - Décomposition

Un p-cycle est un produit (i.e. une composée) de $p-1$ transpositions :

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

Transpositions quelconques

On commence par une proposition :

Proposition - Décomposition

Un p-cycle est un produit (i.e. une composée) de $p-1$ transpositions :

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

Démonstration

Décomposition d’une permutation

On en déduit, associé avec la partie précédente

Théorème - Engendrement par transpositions

Toute permutation se décompose en produit de transpositions.
Autrement écrit, si on note T_n l’ensemble des transpositions de S_n,

alors $S_n = < T_n >$

⇒ Décomposition en produit de cycles/de transpositions

⇒ Séparation en deux parties, selon la signature

Décomposition d’une permutation

On en déduit, associé avec la partie précédente

Théorème - Engendrement par transpositions

Toute permutation se décompose en produit de transpositions. Autrement écrit, si on note T_n l’ensemble des transpositions de S_n,

alors $S_n =< T_n >$

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

Décomposition d'une permutation

On en déduit, associé avec la partie précédente

Théorème - Engendrement par transpositions

Toute permutation se décompose en produit de transpositions. Autrement écrit, si on note T_n l'ensemble des transpositions de S_n,

alors $S_n = < T_n >$

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

Exercice

Déterminer la permutation $(a_1\, a_p) \circ (a_1\, a_{p-1}) \circ \cdots \circ (a_1\, a_2)$ où les a_i sont des entiers tous distincts compris entre 1 et n, ainsi que la permutation $(a_1\, a_2 \ldots a_q) \circ (a_q\, a_{q+1} \ldots a_p)$ où $1 < q < p$.

Exercices

<u>Exercice</u>

Soit $\tau = (a\,b) \in S_n$ et $\sigma = (a\,a_1\,a_2\,\dots a_p) \in S_n$ un cycle de longueur $p+1$. Donner la décomposition en produit de cycles à supports disjoints de $\tau\sigma$. Comparer le nombre d'orbites de σ et celui de $\tau\sigma$.

Exercices

<u>Exercice</u>

Soit $\tau = (a\, b) \in S_n$ et $\sigma = (a\, a_1\, a_2 \ldots a_p) \in S_n$ un cycle de longueur $p+1$. Donner la décomposition en produit de cycles à supports disjoints de $\tau\sigma$. Comparer le nombre d'orbites de σ et celui de $\tau\sigma$.

<u>Exercice</u>

Pour $(i,j) \in [\![2,n]\!]^2$, calculer $\tau_{1i} \circ \tau_{1j} \circ \tau_{1i}$ et montrer que les transpositions de la forme τ_{1i} engendrent le groupe symétrique S_n (c'est-à-dire que toute permutation se décompose comme produit de transpositions de la forme τ_{1i}).

Transposition $\tau_{i,i+1}$

Analyse Un deuxième algorithme ?

Transposition $\tau_{i,i+1}$

Analyse Un deuxième algorithme ?

Exercice

Appliquer la méthode présentée pour exprimer à nouveau $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 2 & 3 & 1 & 6 & 4 & 5 & 7 \end{pmatrix}$ en produit de transpositions.

Décomposition avec des transposition $(i\ i+1)$

Proposition - Décomposition par transposition simple

Toute permutation est le produit de transpositions de la forme $\tau_{i,i+1}$.
Autrement écrit :
Pour tout $\sigma \in S_n$, il existe $r \in \mathbb{N}$, $i_1, i_2, \ldots i_r \in \mathbb{N}_{n-1}$ tel que $\sigma = \tau_{i_1,i_1+1} \circ \cdots \circ \tau_{i_r,i_r+1}$.

Décomposition avec des transposition $(i\, i+1)$

Proposition - Décomposition par transposition simple

Toute permutation est le produit de transpositions de la forme $\tau_{i,i+1}$.
Autrement écrit :
Pour tout $\sigma \in S_n$, il existe $r \in \mathbb{N}$, $i_1, i_2, \dots i_r \in \mathbb{N}_{n-1}$ tel que $\sigma = \tau_{i_1,i_1+1} \circ \dots \circ \tau_{i_r,i_r+1}$.

Exercice

A démontrer

Conclusion

Objectifs

$\Rightarrow$ Décomposition en produit de cycles/de transpositions

Conclusion

Objectifs

$\Rightarrow$ Décomposition en produit de cycles/de transpositions

- Toute permutation se décompose en produit de cycles disjoints

Conclusion

Objectifs

⇒ Décomposition en produit de cycles/de transpositions

- Toute permutation se décompose en produit de cycles disjoints
  Comment l'obtenir ? L'algorithme des orbites.

Conclusion

Objectifs

⇒ Décomposition en produit de cycles/de transpositions

- Toute permutation se décompose en produit de cycles disjoints
  Comment l'obtenir ? L'algorithme des orbites.
- Toute permutation est un produit de transpositions

Conclusion

Objectifs

⇒ Décomposition en produit de cycles/de transpositions

- Toute permutation se décompose en produit de cycles disjoints
  Comment l'obtenir ? L'algorithme des orbites.
- Toute permutation est un produit de transpositions
  Comment l'obtenir ? Décomposition des orbites, ou avec la vision graphe

Conclusion

Objectifs

⇒ Décomposition en produit de cycles/de transpositions

- Toute permutation se décompose en produit de cycles disjoints
  Comment l'obtenir ? L'algorithme des orbites.
- Toute permutation est un produit de transpositions
  Comment l'obtenir ? Décomposition des orbites, ou avec la vision graphe
- Toute permutation est un produit de transpositions $\tau_{i,i+1}$

Conclusion

Objectifs

⇒ Décomposition en produit de cycles/de transpositions

Pour le prochain cours

- Lecture du cours : Signature
- Exercice n° 611