Groupes

Table des matières

1 Groupe

1.1 Loi de composition interne

Définition 1.1

Soit E un ensemble. On appelle loi de *composition interne* toute application $\star$ de $E \times E$ dans E.

$$\begin{array}{rccc} \star : & E \times E & \longrightarrow & E \\ & (x, y) & \longmapsto & x \star y \end{array}$$

Définition 1.2

La loi $\star$ est dite

— *associative* lorsque

$$\forall x, y, z \in E, \quad (x \star y) \star z = x \star (y \star z)\,.$$

— *commutative* lorsque

$$\forall x, y \in E, \quad x \star y = y \star x.$$

Exemples

⇨ L'addition et la multiplication sont des lois de composition interne sur $\mathbb{Z}$, associatives et commutatives.

⇨ L'exponentiation est une loi de composition interne sur $\mathbb{N}$ qui n'est ni associative, ni commutative.

⇨ Si X est un ensemble, la composition est une loi de composition interne associative sur $E \coloneqq \mathcal{F}(X, X)$. Elle n'est pas commutative dès que X possède au moins deux éléments.

⇨ Le produit matriciel est une loi de composition interne associative sur $\mathcal{M}_n(\mathbb{C})$. Elle est n'est pas commutative dès que $n \geqslant 2$.

Remarques

⇨ Soit $\star$ une loi *associative*. Quels que soient $x, y, z, t \in E$, les 5 expressions suivantes sont égales :

$$(x \star y) \star (z \star t), \quad ((x \star y) \star z) \star t,$$

$$(x \star (y \star z)) \star t, \quad x \star ((y \star z) \star t), \quad x \star (y \star (z \star t)).$$

On admettra plus généralement que toute expression de n éléments construite à l'aide de la loi $\star$ ne dépend pas de l'emplacement des parenthèses. C'est pourquoi on se permettra de les omettre.

⇨ On dit que deux éléments $x, y \in E$ *commutent* lorsque $x \star y = y \star x$.

Définition 1.3

Une partie A de E est dite *stable* par $\star$ lorsque

$$\forall x, y \in A, \quad x \star y \in A.$$

Remarque

⇨ Si $\star$ est une loi de composition interne sur E et $A \in \mathcal{P}(E)$ est stable par $\star$, alors la loi

$$\begin{array}{rccc} \star_A : & A \times A & \longrightarrow & A \\ & (x, y) & \longmapsto & x \star y \end{array}$$

est une loi de composition interne sur A. On continuera à la noter $\star$.

Définition 1.4

On dit que $\star$ admet un *élément neutre* $e \in E$ lorsque

$$\forall x \in E, \quad x \star e = x \quad \text{et} \quad e \star x = x.$$

Si tel est le cas, il est unique et on l'appelle *élément neutre* de $\star$. Lorsque la loi est notée additivement, l'élément neutre est noté 0.

Remarque

⇨ Par convention, lorsqu'une loi est notée additivement, elle sera toujours commutative.

Exercice 1

⇨ Parmi les lois de composition interne citées plus haut, lesquelles admettent un élément neutre ?

Dans toute la suite de ce cours, on supposera, sauf mention explicite du contraire, que les lois sont associatives et admettent un élément neutre.

Définition 1.5

Soit $x \in E$. On définit par récurrence x^n pour tout $n \in \mathbb{N}$ en posant :
- $x^0 := e$
- $\forall n \in \mathbb{N}, \quad x^{n+1} := x^n \star x$.

Remarque

⇨ Lorsque la loi est notée additivement, on n'utilise pas la notation x^n mais plutôt la notation $n \cdot x$. On a donc :
- $0 \cdot x = 0$
- $\forall n \in \mathbb{N}, \quad (n+1) \cdot x = n \cdot x + x$.

Proposition 1.6

- Soit $x \in E$. Alors

$$\begin{aligned} \forall m, n \in \mathbb{N}, \quad & x^{m+n} = x^m \star x^n \\ & (x^m)^n = x^{mn}. \end{aligned}$$

- Soit $x, y \in E$ tels que $x \star y = y \star x$. Alors, pour tout $n, m \in \mathbb{N}$, x^n et y^m commutent. De plus

$$\forall n \in \mathbb{N}, \quad (x \star y)^n = x^n \star y^n.$$

Remarque

⇨ Si la loi est notée additivement, on a donc :

$$\begin{aligned} \forall x \in E, \quad \forall m, n \in \mathbb{N}, \quad & (m+n) \cdot x = m \cdot x + n \cdot x \\ & n \cdot (m \cdot x) = (nm) \cdot x \\ \forall x, y \in E, \quad \forall n \in \mathbb{N}, \quad & n \cdot (x + y) = n \cdot x + n \cdot y. \end{aligned}$$

Définition 1.7

Soit $x \in E$. On dit que x est *symétrisable* pour la loi $\star$ lorsqu'il existe $y \in E$ tel que

$$x \star y = y \star x = e.$$

Si tel est le cas, y est unique et est appelé *symétrique* de x. On l'appelle *inverse* de x et on le note x^{-1} lorsque la loi est notée multiplicativement. On l'appelle *opposé* de x et on le note $-x$ lorsque la loi est notée additivement.

Proposition 1.8

— Si x est symétrisable, x^{-1} l'est et

$$\left(x^{-1}\right)^{-1} = x.$$

— Si x et y sont symétrisables, $x \star y$ l'est et

$$(x \star y)^{-1} = y^{-1} \star x^{-1}.$$

Définition 1.9

Soit $x \in E$. Si x est symétrisable, on étend la définition de x^n en posant :

$$\forall n \in \mathbb{Z}, \quad x^n := \begin{cases} x^n & \text{si } n \geqslant 0 \\ \left(x^{-n}\right)^{-1} & \text{si } n < 0. \end{cases}$$

Proposition 1.10

— Soit $x \in E$. Si x est symétrisable

$$\forall m, n \in \mathbb{Z}, \qquad x^{m+n} = x^m \star x^n$$
$$\left(x^m\right)^n = x^{mn}.$$

— Si $x, y \in E$ sont symétrisables et commutent, alors

$$\forall n \in \mathbb{Z}, \quad (x \star y)^n = x^n \star y^n.$$

Remarque

⇨ Lorsque la loi est notée additivement, on a donc :

$$\begin{aligned} \forall x \in E, \quad \forall m, n \in \mathbb{Z}, \qquad & (m+n) \cdot x = m \cdot x + n \cdot x \\ & n \cdot (m \cdot x) = (nm) \cdot x \\ \forall x, y \in E, \quad \forall n \in \mathbb{Z}, \qquad & n \cdot (x+y) = n \cdot x + n \cdot y. \end{aligned}$$

Définition 1.11

On dit qu'un élément x de E est *régulier* lorsque

$$\begin{aligned} \forall y, z \in E, \quad x \star y = x \star z \quad &\Longrightarrow \quad y = z \\ y \star x = z \star x \quad &\Longrightarrow \quad y = z. \end{aligned}$$

Proposition 1.12

Les éléments symétrisables sont réguliers.

1.2 Groupe

Définition 1.13

Soit G un ensemble muni d'une loi de composition interne $\star$. On dit que $(G, \star)$ est un *groupe* lorsque
— $\star$ est associative
— $\star$ admet un élément neutre
— tout élément de G est symétrisable.
Le groupe $(G, \star)$ est dit commutatif (ou *abélien*) lorsque la loi $\star$ est commutative.

Remarques

⇨ $(\mathbb{C}, +)$ et $(\mathbb{C}^*, \times)$ sont des groupes commutatifs.

⇨ Si $(G, \star)$ est un groupe et $a, b \in G$, alors

$$\forall x \in G, \quad a \star x = b \quad \Longleftrightarrow \quad x = a^{-1} \star b.$$

De même

$$\forall x \in G, \quad x \star a = b \quad \Longleftrightarrow \quad x = b \star a^{-1}.$$

⇨ Si $(G,\star)$ est un groupe fini, on appelle table de $(G,\star)$ le tableau à deux entrées dont les lignes et les colonnes sont indexées par les éléments de G et qui contient les produits $x\star y$. Puisque $(G,\star)$ est un groupe, chaque ligne et chaque colonne contient une et une seule fois chaque élément de G.

Exercice 2

⇨ Montrer qu'il n'existe qu'une seule table de groupe à 3 éléments.

Définition 1.14

Soit $(G,\star)$ un groupe et H une partie de G. On dit que H est un *sous-groupe* de $(G,\star)$ lorsque
- $e\in H$
- $\forall x,y\in H,\quad x\star y\in H$
- $\forall x\in H,\quad x^{-1}\in H$.

Si tel est le cas, alors $(H,\star)$ est un groupe.

Remarques

⇨ Si H est un sous-groupe de G, alors : $\forall x\in H,\quad \forall n\in\mathbb{Z},\quad x^n\in H$.

⇨ En pratique, pour montrer que $(H,\star)$ est un groupe, on le fera presque toujours apparaître comme sous-groupe d'un groupe connu.

Exemples

⇨ Si $(G,\star)$ est un groupe, G et $\{e\}$ sont des sous-groupes de G. Le sous-groupe $\{e\}$ est appelé groupe *trivial*.

⇨ $\mathbb{R}$ et $\mathbb{Z}$ sont des sous-groupes de $(\mathbb{C},+)$. De même, $\mathbb{R}^*$ et $\mathbb{U}$ sont des sous-groupes de $(\mathbb{C}^*,\times)$.

Proposition 1.15

Si $n\in\mathbb{N}^*$, $(\mathbb{U}_n,\times)$ est un groupe dont l'élément neutre est 1.

Proposition 1.16

Soit E un ensemble. On note $\sigma(E)$ l'ensemble des bijections de E dans E. Alors $(\sigma(E),\circ)$ est un groupe, appelé groupe des *permutations* de E, dont l'élément neutre est Id_E.

Exercice 3

⇨ Montrer que l'ensemble des bijections strictement croissantes de $\mathbb{R}$ dans $\mathbb{R}$ est un sous-groupe de $(\sigma(\mathbb{R}),\circ)$.

Proposition 1.17

L'intersection d'une famille de sous-groupes est un sous-groupe.

Remarque

⇨ Contrairement à l'intersection, l'union de deux sous-groupes n'est en général pas un sous-groupe.

Définition 1.18

Soit $(G,\star)$ un groupe et A une partie de G. Alors, au sens de l'inclusion, il existe un plus petit sous-groupe de G contenant A ; on l'appelle *groupe engendré* par A et on le note $\mathrm{Gr}(A)$.

Remarque

⇨ Si $(G,\star)$ est un groupe et x est un élément de G, le groupe engendré par $\{x\}$, appelé aussi groupe engendré par x, est $\left\{x^k : k\in\mathbb{Z}\right\}$.

Définition 1.19

Soit $(G_1,\star_1)$ et $(G_2,\star_2)$ deux groupes. On dit qu'une application φ de G_1 dans G_2 est un *morphisme de groupe* lorsque

$$\forall x,y\in G_1,\quad \varphi\left(x\star_1 y\right)=\varphi(x)\star_2\varphi(y).$$

Plus précisément, on dit que φ est un
- *endomorphisme* lorsque $(G_1,\star_1)=(G_2,\star_2)$
- *isomorphisme* lorsque φ est bijective
- *automorphisme* lorsque φ est un endomorphisme et un isomorphisme.

Remarque

⇨ L'application φ de $\mathbb{R}$ dans $\mathbb{U}$ qui à θ associe $e^{i\theta}$ est un morphisme du groupe $(\mathbb{R},+)$ dans le groupe $(\mathbb{U},\times)$. L'application exp de $\mathbb{R}$ dans $\mathbb{R}_+^*$ est un isomorphisme du groupe $(\mathbb{R},+)$ dans le groupe $(\mathbb{R}_+^*,\times)$.

Proposition 1.20

Soit φ un morphisme du groupe de $(G_1,\star_1)$ dans $(G_2,\star_2)$. Alors

$$\begin{aligned} & & \varphi(e_1) = e_2 \\ \forall x \in G_1, & & \varphi\left(x^{-1}\right) = [\varphi(x)]^{-1} \\ \forall x \in G_1, \quad \forall n \in \mathbb{Z}, & & \varphi\left(x^n\right) = [\varphi(x)]^n . \end{aligned}$$

Remarque

⇨ Si φ est un morphisme de groupe et que les lois sont notées additivement, alors

$$\forall x \in G_1, \quad \forall n \in \mathbb{Z}, \quad \varphi(n \cdot x) = n \cdot \varphi(x).$$

Exercice 4

⇨ Déterminer les endomorphismes, puis les automorphismes de $(\mathbb{Z},+)$.

Proposition 1.21

Soit φ un morphisme de $(G_1,\star_1)$ dans $(G_2,\star_2)$. Alors
- l'image réciproque d'un sous-groupe de G_2 est un sous-groupe de G_1.
- l'image directe d'un sous-groupe de G_1 est un sous-groupe de G_2.

Définition 1.22

Soit φ un morphisme de $(G_1,\star_1)$ dans $(G_2,\star_2)$. On appelle *noyau* de φ et on note $\operatorname{Ker}\varphi$ l'ensemble

$$\operatorname{Ker}\varphi := \{x \in G_1 \mid \varphi(x) = e_2\}.$$

C'est un sous-groupe de G_1.

Proposition 1.23

Un morphisme φ de $(G_1,\star_1)$ dans $(G_2,\star_2)$ est injectif si et seulement si

$$\operatorname{Ker}\varphi = \{e_1\}.$$

Remarque

⇨ Pour montrer l'injectivité d'un morphisme, montrer que $\operatorname{Ker}\varphi = \{e_1\}$ doit devenir un réflexe. Pour cela, il est naturel de procéder par double inclusion. Mais comme l'inclusion $\{e_1\} \subset \operatorname{Ker}\varphi$ est toujours vraie, puisque $\varphi(e_1) = e_2$, il est essentiel de se concentrer sur l'inclusion $\operatorname{Ker}\varphi \subset \{e_1\}$.

Exercice 5

⇨ Soit $(G,\star)$ un groupe et φ l'application de G dans $\sigma(G)$ définie par

$$\begin{array}{rccl} \varphi : & G & \longrightarrow & \sigma(G) \\ & x & \longmapsto & \varphi(x) : \begin{array}{ccc} G & \longrightarrow & G \\ g & \longmapsto & x \star g \end{array} \end{array}$$

Montrer que φ est bien définie et que c'est un morphisme injectif de groupe. En déduire que $(G,\star)$ est isomorphe à un sous-groupe du groupe de ses permutations.

Proposition 1.24

- La composée de deux morphismes de groupe est un morphisme de groupe.
- La bijection réciproque d'un isomorphisme de groupe est un isomorphisme de groupe.

Proposition 1.25

Si $(G,\star)$ est un groupe, on note $\operatorname{Aut}(G)$ l'ensemble des automorphismes de G. $(\operatorname{Aut}(G),\circ)$ est un groupe.

Définition 1.26

Soit $(G_1, \star_1)$ et $(G_2, \star_2)$ deux groupes. On définit la loi $\star$ sur $G_1 \times G_2$ par

$$\forall (x_1, x_2), (y_1, y_2) \in G_1 \times G_2, \quad (x_1, x_2) \star (y_1, y_2) = (x_1 \star_1 y_1, x_2 \star_2 y_2).$$

Alors $(G_1 \times G_2, \star)$ est un groupe d'élément neutre (e_1, e_2) et

$$\forall (x_1, x_2) \in G_1 \times G_2, \quad (x_1, x_2)^{-1} = \left(x_1^{-1}, x_2^{-1}\right).$$

Exercice 6

⇨ Montrer que $(\mathbb{R}_+^* \times \mathbb{U}, \times)$ est isomorphe à $(\mathbb{C}^*, \times)$.

1.3 Ordre d'un élément

Proposition 1.27

Pour tout $n \in \mathbb{N}$, on pose

$$n\mathbb{Z} \coloneqq \{kn : k \in \mathbb{Z}\}.$$

C'est un sous-groupe de $(\mathbb{Z}, +)$.

Proposition 1.28

Une partie H de $\mathbb{Z}$ est un sous-groupe de $(\mathbb{Z}, +)$ si et seulement si il existe $n \in \mathbb{N}$ tel que $H = n\mathbb{Z}$. De plus, si tel est le cas, l'entier n est unique.

Remarque

⇨ Si H est un sous-groupe de $(\mathbb{Z}, +)$ non réduit à $\{0\}$, alors H admet un plus petit élément strictement positif $n \in \mathbb{N}^*$. On a alors $H = n\mathbb{Z}$.

Définition 1.29

Soit $(G, \star)$ un groupe et $x \in G$.

— On dit que x est d'*ordre fini* lorsqu'il existe $n \in \mathbb{N}^*$ tel que $x^n = e$. Dans ce cas, il existe un unique $\omega \in \mathbb{N}^*$ tel que

$$\forall n \in \mathbb{Z}, \quad x^n = e \iff \omega | n.$$

On l'appelle *ordre* de x. C'est le plus petit entier $n \in \mathbb{N}^*$ tel que $x^n = e$.

— Sinon, on dit que x est d'*ordre infini*. On a alors

$$\forall n \in \mathbb{Z}, \quad x^n = e \iff n = 0.$$

Remarques

⇨ Dans $(\mathbb{C}^*, \times)$, si $n \in \mathbb{N}^*$, $\omega \coloneqq \mathrm{e}^{\mathrm{i}\frac{2\pi}{n}}$ est d'ordre n.

⇨ Dans un groupe, e est l'unique élément d'ordre 1.

⇨ Dans un groupe fini, tout élément est d'ordre fini.

⇨ Soit $x \in G$ un élément d'ordre $\omega \in \mathbb{N}^*$. Alors le groupe engendré par x est $\left\{e, x, x^2, \ldots, x^{\omega-1}\right\}$, ces éléments étant deux à deux distincts. En particulier, l'ordre de x est le cardinal du groupe qu'il engendre.

Théorème 1.30: Théorème de Lagrange

Soit $(G, \star)$ un groupe fini et x un élément de G. Alors l'ordre de x divise le cardinal de G.

Remarques

⇨ Si $(G, \star)$ est un groupe fini, le cardinal de G est aussi appelé ordre de G. La version faible du théorème de Lagrange nous dit donc que dans un groupe fini, l'ordre d'un élément divise l'ordre du groupe.

⇨ La version forte du théorème de Lagrange dit que si $(G, \star)$ est un groupe fini et H est un sous-groupe de $(G, \star)$, alors le cardinal de H divise le cardinal de G. De cette version forte découle la version faible : si $x \in G$, il suffit de remarquer que le cardinal du groupe H engendré par x est l'ordre de x.

Exercice 7

⇨ Déterminer les sous-groupes finis de $(\mathbb{U}, \times)$.

2 Groupe symétrique

2.1 Groupe symétrique

Définition 2.1

Soit $n \in \mathbb{N}$. On appelle *groupe symétrique* et on note $(\mathcal{S}_n, \circ)$ l'ensemble des bijections de $[\![1, n]\!]$ dans lui-même muni de la loi de composition.

Remarques

⇨ Si $\sigma \in \mathcal{F}([\![1, n]\!], [\![1, n]\!])$, l'application σ est aussi notée

$$\sigma = \begin{pmatrix} 1 & 2 & \cdots & n \\ \sigma(1) & \sigma(2) & \cdots & \sigma(n) \end{pmatrix}.$$

Puisque $[\![1, n]\!]$ est fini, σ est bijective si et seulement si elle est injective ou surjective. Autrement dit, σ est bijective si et seulement si l'une des deux conditions suivantes est vérifiée :

1. Les entiers $\sigma(1), \ldots, \sigma(n)$ sont deux à deux distincts.
2. $\{\sigma(1), \ldots, \sigma(n)\} = [\![1, n]\!]$.

⇨ Si E est un ensemble fini de cardinal n, l'ensemble des bijections de E muni de la loi de composition est un groupe isomorphe à $(\mathcal{S}_n, \circ)$.

Proposition 2.2

$(\mathcal{S}_n, \circ)$ est un groupe fini de cardinal $n!$.

Définition 2.3

Soit $n \in \mathbb{N}$.

— Soit $p \in [\![2, n]\!]$. On appelle *cycle* de longueur p (ou p-cycle) toute permutation σ tel qu'il existe $x_0, \ldots, x_{p-1} \in [\![1, n]\!]$ deux à deux distincts tels que
  — $\sigma(x_0) = x_1, \sigma(x_1) = x_2, \ldots, \sigma(x_{p-1}) = x_0$
  — $\forall x \in [\![1, n]\!] \setminus \{x_0, \ldots, x_{p-1}\}, \quad \sigma(x) = x$
  On note $\sigma = (x_0 \quad x_1 \quad \cdots \quad x_{p-1})$.

— On appelle *transposition* tout cycle de longueur 2.

Remarques

⇨ Si $n \geqslant 3$, $(\mathcal{S}_n, \circ)$ n'est pas commutatif.

⇨ Si σ est une transposition, alors $\sigma^2 = \mathrm{Id}$. On en déduit que $\sigma^{-1} = \sigma$.

⇨ Si $i \in \mathbb{Z}$ et $p \in \mathbb{N}^*$, on note $i \bmod p$, le reste de la division euclidienne de i par p. Si $\sigma = (x_0 \quad x_1 \quad \cdots \quad x_{p-1})$ est un p-cycle, on a donc

$$\forall i \in [\![0, p[\![, \quad \sigma(x_i) = x_{i+1 \bmod p}.$$

⇨ Les p-cycles sont des éléments d'ordre p.

Exercices 8

⇨ Soit τ un p-cycle et $\sigma \in \mathcal{S}_n$. Montrer que $\sigma\tau\sigma^{-1}$ est un p-cycle.

⇨ Montrer que si $\sigma_1, \sigma_2 \in \mathcal{S}_n$ sont deux p-cycles, il existe $\sigma \in \mathcal{S}_n$ tel que $\sigma_2 = \sigma\sigma_1\sigma^{-1}$.

2.2 Décomposition en cycles à supports disjoints

Définition 2.4

Soit $\sigma \in \mathcal{S}_n$. On définit la relation $\mathcal{R}$ sur $[\![1, n]\!]$ par

$$\forall x, y \in [\![1, n]\!], \quad x \mathcal{R} y \iff \left[\exists k \in \mathbb{Z}, \quad \sigma^k(x) = y\right].$$

Alors $\mathcal{R}$ est une relation d'équivalence. Si $x \in [\![1, n]\!]$, la classe de x est notée $\mathcal{O}(x)$ et est appelée orbite de x.

Remarques

⇨ Les orbites étant des classes d'équivalence, elles forment une partition de $[\![1, n]\!]$.

⇨ Si $x \in [\![1, n]\!]$, alors $\mathcal{O}(x) = \left\{\sigma^k(x) : k \in \mathbb{Z}\right\}$. De plus, il existe un plus petit $p \in \mathbb{N}^*$ tel que $\sigma^p(x) = x$. On a alors $\mathcal{O}(x) = \left\{x, \sigma(x), \ldots, \sigma^{p-1}(x)\right\}$.

Définition 2.5

Soit $\sigma \in \mathcal{S}_n$. On appelle *support* de σ et on note $\mathrm{Supp}(\sigma)$ l'ensemble des $x \in [\![1, n]\!]$ tels que $\sigma(x) \neq x$.

Remarques

⇨ Si $\sigma = (x_0 \quad x_1 \quad \cdots \quad x_{p-1})$ est un p-cycle, alors $\mathrm{Supp}(\sigma) = \{x_0, \ldots, x_{p-1}\}$.

⇨ Le support de σ est stable par σ.

⇨ Deux permutations de supports disjoints commutent. Cependant la réciproque est fausse.

Théorème 2.6

Toute permutation s'écrit comme le produit (commutatif) de cycles à supports disjoints. De plus, à l'ordre près, il y a unicité d'une telle décomposition.

Exercices 9

⇨ Déterminer tous les éléments de $\mathcal{S}_3$. Quels sont leurs ordres ?

⇨ Quels sont les entiers qui sont l'ordre d'un élément de $\mathcal{S}_4$?

⇨ Déterminer les éléments d'ordre 2 de $\mathcal{S}_n$?

2.3 Signature, groupe alterné

Proposition 2.7

Toute permutation $\sigma \in \mathcal{S}_n$ s'écrit comme le produit d'au plus $n-1$ transpositions.

Remarque

⇨ Soit $\sigma = (x_0 \quad x_1 \quad \cdots \quad x_{p-1})$ un cycle de longueur p. Alors

$$\sigma = (x_0 \quad x_1)\,(x_1 \quad x_2)\cdots(x_{p-2} \quad x_{p-1})\,.$$

Exercice 10

⇨ Dans $\mathcal{S}_3$, on pose $\sigma_1 \coloneqq (1 \quad 3)$ et $\sigma_2 \coloneqq (1 \quad 2 \quad 3)$. Décomposer $\sigma_1\sigma_2$ en produit de transpositions de deux manières distinctes.

Définition 2.8

Soit σ une permutation et

$$\sigma = \tau_1 \cdots \tau_m \quad \text{et} \quad \sigma = \tau'_1 \cdots \tau'_{m'}$$

deux décompositions de σ en produit de transpositions. Alors m et m' ont même parité ; on dit que σ est *paire* lorsque ces entiers sont pairs et que σ est *impaire* dans le cas contraire. On définit la *signature* de σ que l'on note $\epsilon(\sigma)$ par

$$\epsilon(\sigma) \coloneqq \begin{cases} +1 & \text{si } \sigma \text{ est paire} \\ -1 & \text{si } \sigma \text{ est impaire.} \end{cases}$$

Remarques

⇨ Soit $\sigma \in \mathcal{S}_n$ et $\sigma = \tau_1 \cdots \tau_m$ une décomposition de σ en produit de transpositions. Alors

$$\epsilon(\sigma) = (-1)^m\,.$$

⇨ La signature d'un p-cycle est $(-1)^{p-1}$. En particulier, les transpositions sont impaires et les 3-cycles sont pairs.

Proposition 2.9

L'application ϵ de $(\mathcal{S}_n, \circ)$ dans $(\{-1, 1\}, \times)$ est un morphisme de groupe.

Remarque

⇨ Si σ est une permutation, σ et σ^{-1} ont la même signature.

Définition 2.10

On note $\mathcal{A}_n$ l'ensemble des permutations paires. C'est un sous-groupe de $(\mathcal{S}_n, \circ)$ appelé *groupe symétrique alterné*.

Remarque

⇨ Si $n \geqslant 2$, le groupe $(\mathcal{A}_n, \circ)$ est de cardinal $n!/2$.