

Groupes

1. Généralités

Définition

Un magma est un couple $(M, *)$ où M est un ensemble et $*$ est une loi de composition interne c'est-à-dire une application de $M \times M$ dans M .

Dans un magma, on note $x * y$ l'image d'un couple (x, y) de $M \times M$ par l'application $*$.

Remarque

On dit qu'un sous-ensemble N d'un magma $(M, *)$ est stable pour $*$ si et seulement si, $\forall a, b \in N, a * b \in N$. Dans ce cas, on peut définir une loi de composition interne sur N (appelée loi induite par $*$ sur N) en considérant la restriction de $*$ à $N \times N$.

Définition

Soit $(M, *)$ un magma et soit e un élément de M .

On dit que e est un élément neutre à droite si et seulement si $\forall a \in M, a * e = a$.

On dit que e est un élément neutre à gauche si et seulement si $\forall a \in M, e * a = a$.

On dit que e est un élément neutre si c'est un élément neutre à droite et à gauche.

Propriété

Soit $(M, *)$ un magma.

Si M possède un élément neutre à droite e_1 et un élément neutre à gauche e_2 alors $e_1 = e_2$.

En particulier, l'élément neutre d'un magma s'il existe est unique.

Démonstration

On a $e_2 * e_1 = e_2$ car e_1 est un élément neutre à droite
et $e_2 * e_1 = e_1$ car e_2 est un élément neutre à gauche.

Définition

Soit $(M, *)$ un magma.

On dit que deux éléments a et b de M sont permutables ou commutent si et seulement si $a * b = b * a$.

Le centre de M noté $Z(M)$ est l'ensemble des éléments de M qui commutent avec tous les autres c'est-à-dire $Z(M) = \{c \in M / \forall a \in M, a * c = c * a\}$.

On dit que la loi $*$ est commutative si et seulement si tous les éléments de M sont 2 à 2 permutables i.e. $Z(M) = M$ ou encore, $\forall x, y \in M, x * y = y * x$. On dit alors que $(M, *)$ un magma commutatif.

Définition

Soit $(M,*)$ un magma.

On dit que la loi $*$ est associative si et seulement si, $\forall x,y,z \in M, x * (y * z) = (x * y) * z$.

Dans ce cas, on dit que $(M,*)$ un magma associatif.

Remarque

Dans un magma associatif, on peut utiliser la notation $x * y * z$ pour l'un des deux produits précédents. Il en est de même pour la composition de plus de trois facteurs.

Définition

Un monoïde est un magma associatif possédant un élément neutre.

Définition

Soit $(M,*)$ un monoïde d'élément neutre e .

Soit x un élément de M .

On dit que x est symétrisable à gauche si et seulement si $\exists x_1 \in M / x_1 * x = e$.

L'élément x_1 est appelé symétrique de x à gauche.

On dit que x est symétrisable à droite si et seulement si $\exists x_2 \in M / x * x_2 = e$.

L'élément x_2 est appelé symétrique de x à droite.

Propriété

Soit $(M,*)$ un monoïde d'élément neutre e et soit x un élément de M .

Si x est symétrisable à gauche et à droite de symétriques x_1 et x_2 à gauche et à droite respectif, on a $x_1 = x_2$.

Dans ce cas, on dit que x est symétrisable et l'unique élément $\tilde{x} \in M$ tel que $x * \tilde{x} = \tilde{x} * x = e$ est appelé le symétrique de x .

Démonstration

$$\begin{aligned} \text{On a : } x_1 * x * x_2 &= (x_1 * x) * x_2 = e * x_2 = x_2 \\ &= x_1 * (x * x_2) = x_1 * e = x_1. \end{aligned}$$

Remarque

Soient a, b et c trois éléments d'un magma $(M,*)$.

On a : $a = b \Rightarrow a * c = b * c$ et

$$a = b \Rightarrow c * a = c * b.$$

Mais, en général, $a = b \not\Rightarrow c * a = b * c$

Définition

Soit $(M,*)$ un magma.

Soit x un élément de M .

On dit que x est simplifiable (ou régulier) à gauche si et seulement si, $\forall a,b \in M, x * a = x * b \Rightarrow a = b$.

On dit que x est simplifiable (ou régulier) à droite si et seulement si, $\forall a,b \in M, a * x = b * x \Rightarrow a = b$.

On dit que x est simplifiable (ou régulier) s'il est simplifiable (ou régulier) à gauche et à droite.

Propriété

Soit $(M,*)$ un monoïde d'élément neutre e . Soit x un élément de M .

Si x est symétrisable à gauche alors x est simplifiable à gauche.

Si x est symétrisable à droite alors x est simplifiable à droite.

Démonstration

Supposons que x soit symétrisable à gauche et soit $x_1 \in G$ tel que $x_1 * x = e$.

$\forall a, b \in M, x * a = x * b$

$$\Rightarrow x_1 * (x * a) = x_1 * (x * b)$$

$$\Rightarrow (x_1 * x) * a = (x_1 * x) * b$$

$$\Rightarrow e * a = e * b$$

$$\Rightarrow a = b$$

Remarque

La réciproque est fautive.

Par exemple, dans (\mathbb{Z}, \times) d'élément neutre 1, 2 n'est pas symétrisable ($\frac{1}{2} \notin \mathbb{Z}$), et pourtant 2 est simplifiable.

Définition

Un magma $(S,*)$ est un semi-groupe si et seulement si :

- i) La loi $*$ est associative.
- ii) Tout élément est simplifiable (ou régulier).

Exemples

Les magmas suivants sont des semi-groupes :

- $(\mathbb{N}, +)$ où $+$ est l'addition usuelle.
- (\mathbb{Z}^*, \times) où \times est la multiplication usuelle.

Définition

Un magma $(G,*)$ est un groupe si et seulement si :

- i) La loi $*$ est associative.
- ii) La loi $*$ admet un élément neutre.
- iii) Tout élément est symétrisable.

Si, de plus, la loi est commutative, on dit que le groupe est commutatif ou abélien.

Exemples et contre-exemples

Les magmas suivants sont des groupes :

- $(\mathbb{Z}, +)$ où $+$ est l'addition usuelle.
- (\mathbb{C}^*, \times) où \times est la multiplication usuelle.
- Soit E un ensemble et soit $S(E) = \{\text{bijections de } E \text{ dans } E\} = \{\text{permutations de } E\}$
 $(S(E), o)$ est un groupe appelé groupe symétrique de E .
- $(E, +)$ où $E = \{\text{fonctions numériques définies sur } \mathbb{R}\}$ et $+$ est la somme usuelle des fonctions.
C'est-à-dire, f et g étant deux éléments de E , $f + g$ est définie, pour tout réel x , par :
 $(f + g)(x) = f(x) + g(x)$.

- $(\{0,1\}, +)$ où $+$ est la loi définie par le tableau suivant :

+	0	1
0	0	1
1	1	0

- Soit $(G_i, *_i)_{i \in I}$ une famille finie de groupe.
L'ensemble produit $\prod_{i \in I} G_i$ muni de la loi produit usuelle est un groupe.

Les magmas suivants ne sont pas des groupes :

- (\mathbb{Z}^*, \times) où \times est la multiplication usuelle.
- (\mathbb{R}, \times) où \times est la multiplication usuelle.

Remarques

- On dit que l'ensemble G est l'ensemble sous-jacent au groupe $(G, *)$.
- Lorsqu'il n'y a pas de confusion possible sur la loi, on dit simplement que G est un groupe sans préciser celle-ci. Ce qui a pour conséquence d'identifier un groupe à son ensemble sous-jacent.
- Puisqu'un élément symétrisable est simplifiable, un groupe est donc un semi-groupe.
- $(\mathbb{R}, +)$ est un groupe et donc $a + c = b + c \Leftrightarrow a = b \quad (\forall a, b, c \in \mathbb{R})$.
- (\mathbb{R}, \times) n'est pas un groupe (car 0 n'est pas inversible) et donc $a \times c = b \times c \not\Leftrightarrow a = b \quad (\forall a, b, c \in \mathbb{R})$.

Propriété

Tout semi-groupe fini est un groupe.

Démonstration

Rappel : Soient E et F deux ensembles finis de même cardinal et f une application de E vers F .

On a : f injective $\Leftrightarrow f$ surjective $\Leftrightarrow f$ bijective.

Soit $(S, *)$ un semi-groupe fini et soit a un élément de S .

On considère les applications d_a et g_a de S dans S définies par, $\forall x \in S, d_a(x) = x * a$ et $g_a(x) = a * x$.

Puisque a est simplifiable, d_a et g_a sont injectives donc surjectives (et bijectives).

Soient e_1 l'antécédent de a par d_a et e_2 l'antécédent de a par g_a i.e. $d_a(e_1) = a$ et $g_a(e_2) = a$.

Autrement dit, $e_1 * a = a$ et $a * e_2 = a$.

Pour tout b de S , soit b_1 l'antécédent de b par d_a et b_2 l'antécédent de b par g_a i.e. $d_a(b_1) = b$ et $g_a(b_2) = b$ ou encore $b_1 * a = b$ et $a * b_2 = b$.

On a donc $e_1 * b = e_1 * (a * b_2) = (e_1 * a) * b_2 = a * b_2 = b$

et $b * e_2 = (b_1 * a) * e_2 = b_1 * (a * e_2) = b_1 * a = b$.

D'où e_1 est un élément neutre à gauche et e_2 est un élément neutre à droite.

Ce qui signifie que $e_1 = e_2$ est l'élément neutre de S .

Puisque, pour tout c de S , d_c et g_c sont surjectives, les antécédents de e par d_c et g_c donnent un symétrique à droite et à gauche à c donc c est symétrisable.

Propriété

Soit $(S, *)$ un semi-groupe.

S est un groupe si et seulement si S possède un élément neutre à droite e_1 et $\forall x \in S, \exists \tilde{x} \in S / x * \tilde{x} = e_1$.

Démonstration

(\Rightarrow) Trivial.

(\Leftarrow) Soit $a \in S$.

Il existe $b \in S / a * b = e_1$ et il existe $c \in S / b * c = e_1$.

On a : $a = a * e_1 = a * (b * c) = (a * b) * c = e_1 * c$

puis $e_1 = b * c = (b * e_1) * c = b * (e_1 * c) = b * a$

et $e_1 * a = (a * b) * a = a * (b * a) = a * e_1 = a$.

Donc e_1 est un élément neutre à droite et à gauche : c'est un élément neutre.

Par suite, b est le symétrique de a .

Propriété

Soit $(S, *)$ un semi-groupe.

S est un groupe si et seulement si S possède un élément neutre à gauche e_2 et $\forall x \in S, \exists \tilde{x} \in S / \tilde{x} * x = e_2$.

Remarques

- Rappel : L'élément neutre d'un groupe est unique. En particulier, un groupe est toujours non vide.
Le symétrique d'un élément d'un groupe est unique.
Tout élément d'un groupe est simplifiable.
- *Notation additive de la loi d'un groupe.*
 $(G, *) = (G, +)$
On note 0_G l'élément neutre de G .
On parle d'opposé à la place de symétrique et on note $-x$ le symétrique d'un élément x i.e. l'élément qui vérifie $x * (-x) = (-x) * x = e = 0_G$. Par convention, on pose $0_G.x = 0_G, 1.x = x$ et, pour tout entier $n \geq 2, n.x = x * x * \dots * x$ (n fois) et $(-n)x = -(n.x)$.
- *Notation multiplicative de la loi d'un groupe.*
 $(G, *) = (G, \times)$
On note 1_G l'élément neutre de G .
On parle d'inverse à la place de symétrique et on note x^{-1} le symétrique d'un élément x i.e. l'élément qui vérifie $x * x^{-1} = x^{-1} * x = e = 1_G$. Par convention, on pose $x^0 = 1_G, x^1 = x$ et, pour tout entier $n \geq 2, x^n = x * x * \dots * x$ (n fois) et $x^{-n} = (x^n)^{-1}$.
- La notation additive est plus souvent utilisée pour les groupes commutatifs.
Dans le reste du cours, nous utiliserons de préférence la notation multiplicative.
Dans ce cas, nous noterons xy la composition de deux éléments x et y d'un groupe (G, \times) .

Propriété

Soit $(G, *)$ un groupe.

Pour tous les éléments a et b de G , on a : $(a * b)^{-1} = b^{-1} * a^{-1}$ et $(a^{-1})^{-1} = a$.

Démonstration

Soit e l'élément neutre de G .

$(a * b)^{-1}$ est, par définition, l'unique élément de G qui vérifie $(a * b)^{-1} * (a * b) = (a * b) * (a * b)^{-1} = e$.

Or $(b^{-1} * a^{-1}) * (a * b) = b^{-1} * (a^{-1} * a) * b = b^{-1} * e * b = b^{-1} * b = e$

et $(a * b) * (b^{-1} * a^{-1}) = a * (b * b^{-1}) * a^{-1} = a * e * a^{-1} = a * a^{-1} = e$.

$(a^{-1})^{-1}$ est, par définition, l'unique élément de G qui vérifie $a^{-1} * (a^{-1})^{-1} = (a^{-1})^{-1} * a^{-1} = e$.

On a bien, à nouveau par définition, $a^{-1} * a = a * a^{-1} = e$.

Remarques

- Si a, b et c sont trois éléments d'un groupe G , on a : $(a * b * c)^{-1} = c^{-1} * b^{-1} * a^{-1}$.
- Si une loi $*$ est commutative, pour vérifier qu'un élément e est l'élément neutre, il suffit de vérifier que, $\forall x \in G$, on a $x * e = x$ (ou $e * x = x$). L'autre relation étant obtenue par la commutativité. De même, pour vérifier qu'un élément \tilde{x} est le symétrique de x , il suffit que l'on ait soit $x * \tilde{x} = e$ soit $\tilde{x} * x = e$.

Propriété

Soit $(G, *)$ un groupe. $\forall n \in \mathbb{Z}, \forall x \in G, (x^{-n})^{-1} = (x^{-1})^{-n} = x^n$.

Démonstration

- Si n est nul, le résultat est évident.
- Si n est négatif, $(x^{-n})^{-1} = \underbrace{(x * x * \dots * x)^{-1}}_{-n \text{ fois}} = \underbrace{(x^{-1} * x^{-1} * \dots * x^{-1})}_{-n \text{ fois}} = (x^{-1})^{-n}$.
Par définition, $x^n = (x^{-1})^{-n}$.
- Si n est positif, $(x^{-n})^{-1} = ((x^{-1})^n)^{-1} = ((x^{-1})^{-1})^n = x^n$ et $(x^{-1})^{-n} = ((x^{-1})^{-1})^{-(-n)} = x^n$.

Remarque

En notation additive, cela donne :

$$\forall n \in \mathbb{Z}, \forall x \in G, -(-n.x) = -n.(-x) = n.x.$$

Propriété

Soit $(G, *)$ un groupe. $\forall n, p \in \mathbb{Z}, \forall x \in G, x^{n \times p} = (x^n)^p$ et $x^{n+p} = x^n * x^p$.

Démonstration

Remarquons en premier lieu que n et p ont des rôles symétriques.

- Si n est nul, $x^{n \times p} = x^0 = e$ et $(x^n)^p = (x^0)^p = (e)^p = e$.
 $x^{n+p} = x^p = e * x^p = x^0 * x^p = x^n * x^p$.
- Si n et p sont strictement positifs,
$$x^{n \times p} = \underbrace{(x * x * \dots * x)}_{n \times p \text{ fois}} = \underbrace{\underbrace{(x * x * \dots * x)}_{n \text{ fois}} * \dots * \underbrace{(x * x * \dots * x)}_{n \text{ fois}}}_{p \text{ fois}} = \underbrace{x^n * \dots * x^n}_{p \text{ fois}} = (x^n)^p.$$
$$x^n * x^p = \underbrace{(x * x * \dots * x)}_{n \text{ fois}} * \underbrace{(x * x * \dots * x)}_{p \text{ fois}} = x^{n+p}.$$
- Si n et p sont strictement négatifs,
$$x^{n \times p} = x^{(-n) \times (-p)} = (x^{-n})^{-p} = (((x^n)^{-1})^{-1})^p = (x^n)^p.$$
$$x^n * x^p = \underbrace{((x^{-1}) * (x^{-1}) * \dots * (x^{-1}))}_{-n \text{ fois}} * \underbrace{((x^{-1}) * (x^{-1}) * \dots * (x^{-1}))}_{-p \text{ fois}}$$
$$= \underbrace{(x^{-1}) * (x^{-1}) * \dots * (x^{-1})}_{-p+(-n) \text{ fois c\`ad } -(p+n) \text{ fois}} = x^{n+p}.$$

- Si n est positif et p est négatif (si n est négatif et p est positif : idem),

$$x^{n \times p} = x^{-(n \times (-p))} = (x^{-1})^{n \times (-p)} = ((x^{-1})^n)^{-p} = ((x^n)^{-1})^{-p} = (x^n)^p$$

$$x^n * x^p = \underbrace{x * x * \dots * x}_n * \underbrace{(x^{-1}) * (x^{-1}) * \dots * (x^{-1})}_{-p}$$
 - $n > -p$ $x^n * x^p = \underbrace{x * x * \dots * x}_{n-(-p)} = x^{n+p}$
 - $n < -p$ $x^n * x^p = \underbrace{(x^{-1}) * (x^{-1}) * \dots * (x^{-1})}_{-p-n} = x^{n+p}$
 - $n = -p$ $x^n * x^p = e = 1_G = x^0 = x^{n+p}$

Remarque

En notation additive, cela donne :

$$\forall n, p \in \mathbb{Z}, \forall x \in G, (n + p)x = (nx) + (px) \text{ et } (n \times p)x = n(px).$$

2. Sous-groupes

Définition

Soit $(G, *)$ un groupe.

Soit $H \subset G$ et $H \neq \emptyset$.

On dit que H est un sous-groupe de $(G, *)$ si et seulement si H est un groupe pour la loi $*$ induite.

Exemples et contre-exemple

- $(\mathbb{Z}, +)$ est un sous-groupe de $(\mathbb{R}, +)$.
- $2\mathbb{Z} = \{2k ; k \in \mathbb{Z}\}$ est un sous-groupe de $(\mathbb{Z}, +)$.
- (\mathbb{Z}^*, \times) n'est pas un sous-groupe de (\mathbb{R}^*, \times) .

Propriété

Soit (G, \cdot) un groupe noté multiplicativement.

Soit $H \subset G$.

Les propriétés suivantes sont équivalentes :

- (1) H est un sous-groupe de (G, \cdot) .
- (2) $H \neq \emptyset$.
 H est stable par composition (par la loi de G) i.e., $\forall x, y \in H$, on a $xy \in H$.
 H est stable par inverse i.e., $\forall x \in H$, on a $x^{-1} \in H$.
- (3) $H \neq \emptyset$ et, $\forall x, y \in H$, on a $xy^{-1} \in H$.

Démonstration

(1) \Rightarrow (2) : évident.

(2) \Rightarrow (3) : évident.

- (3) \Rightarrow (1) Associativité : découle de celle de G .
 Élément neutre : $\forall x \in H, xx^{-1} \in H \Rightarrow e \in H$.
 Symétrique : $\forall x \in H, ex^{-1} \in H \Rightarrow x^{-1} \in H$.
 Loi de composition interne : $\forall x, y \in H$, on a $y^{-1} \in H$
 et donc $xy = x(y^{-1})^{-1} \in H$.

Remarques

- Si H est un sous-groupe de G , l'élément neutre de H et le même que celui de G et le symétrique d'un élément de H est le même dans H que dans G .
- Si la loi de G est une loi notée additivement, on a :
 - (2') $H \neq \emptyset$, H est stable par la loi de G et, $\forall x \in H$, on a $-x \in H$.
 - (3') $H \neq \emptyset$ et, $\forall x, y \in H$, on a $x - y \in H$.
- Il existe d'autres propriétés équivalentes à (1) :
 - (4) H est stable par la loi de G , $e \in H$ et, $\forall x \in H$, on a $x^{-1} \in H$.
 - (5) $H \neq \emptyset$ et, $\forall x, y \in H$, on a $x^{-1}y \in H$.

Exemples importants

Si (G, \cdot) est un groupe, alors $\{e\}$ et G sont des sous-groupes de (G, \cdot) .
Tous les autres sous-groupes sont dits propres.

Propriété

Si K est un sous-groupe de $(H, *)$ et si H est un sous-groupe de $(G, *)$ alors K est un sous-groupe de $(G, *)$.

Démonstration

Trivial + remarque sur la loi.

Exemples

Soit \mathcal{P} l'ensemble des points du plan. L'ensemble T des transformations (bijections du plan) de \mathcal{P} muni de la loi de composition usuelle des fonctions est un groupe.

L'ensemble I des isométries est un sous-groupe de T .

L'ensemble des translations est un sous-groupe de I .

L'ensemble des rotations d'un centre commun est un sous-groupe de I .

L'ensemble des déplacements (conserve les angles orientés) est un sous-groupe de I .

Propriété

Soit (G, \cdot) un groupe et soit $(H_i)_{i \in I}$ une famille non vide de sous-groupes de G .

Alors $\bigcap_{i \in I} H_i$ est un sous-groupe de G .

Démonstration

- $\forall i \in I$ ($\neq \emptyset$), $e \in H_i$ donc $e \in \bigcap_{i \in I} H_i$. D'où $\bigcap_{i \in I} H_i \neq \emptyset$.
- Soient x et y deux éléments de $\bigcap_{i \in I} H_i$. On a, $\forall i \in I$, x et $y \in H_i$ donc $xy^{-1} \in H_i$.
D'où $xy^{-1} \in \bigcap_{i \in I} H_i$.

Remarque

En général, la réunion de 2 sous-groupes n'est pas un sous-groupe.

Par exemple, on a : $2\mathbb{Z}$ est un sous-groupe de $(\mathbb{Z}, +)$ et $3\mathbb{Z}$ est un sous-groupe de $(\mathbb{Z}, +)$.

Si $2\mathbb{Z} \cup 3\mathbb{Z}$ était un sous-groupe de $(\mathbb{Z}, +)$, on devrait avoir $5 = 2 + 3 \in 2\mathbb{Z} \cup 3\mathbb{Z}$.

Propriété

Soit (G, \cdot) un groupe et soit X une partie de G . Il existe un plus petit sous-groupe de G (au sens de l'inclusion) contenant X . Ce sous-groupe est appelé groupe engendré par X et est noté $\text{gr}(X)$ ou $\langle X \rangle$.

Démonstration

Soit $(H_i)_{i \in I}$ l'ensemble des sous-groupes de G qui contiennent X .

Cette famille n'est pas vide car G appartient à cette famille et on vérifie aisément que $\text{gr}(X) = \bigcap_{i \in I} H_i$.

Remarques

- X est appelé un système générateur de $\langle X \rangle$.
- $\text{gr}(\emptyset) = \{e\}$.
- En particulier, si a est un élément d'un groupe G , on note $\text{gr}(a)$ le groupe engendré par $\{a\}$.

Propriété

Soit G un groupe dont la loi est notée multiplicativement et soit a un élément de G .

On a $\text{gr}(a) = \{a^i \text{ où } i \in \mathbb{Z}\} = \{ \dots, a^{-2}, a^{-1}, 1, a, a^2, \dots \}$.

Remarque

En notation additive, on obtient $\text{gr}(a) = \{ka \text{ où } k \in \mathbb{Z}\} = \{ \dots, -2a, -a, 0, a, 2a, \dots \}$.

Démonstration

On pose $E = \{ \dots, a^{-2}, a^{-1}, 1, a, a^2, \dots \}$. On veut montrer que $\text{gr}(a) = E$.

(\subset) Il suffit de montrer que E est un sous-groupe de G (qui contient $\{a\}$).

- Puisque l'on a bien E qui contient a , $E \neq \emptyset$.
- $\forall x, y \in E, \exists n, p \in \mathbb{Z} / x = a^n$ et $y = a^p$. On a : $xy^{-1} = a^{n-p} \in E$.

(\supset) Puisque $\text{gr}(a)$ est un sous-groupe qui contient a , $\text{gr}(a)$ doit être stable par inverse et composition.

Donc $a^{-1} \in \text{gr}(a)$ et, $\forall n \in \mathbb{Z}, a^n \in \text{gr}(a)$.

Exemples

- $(2\mathbb{Z}, +)$ est le sous-groupe de $(\mathbb{Z}, +)$ engendré par 2.
- $(\mathbb{Z}, +)$ est le sous-groupe de $(\mathbb{R}, +)$ engendré par 1.
- Dans (\mathbb{C}^*, \times) , $\text{gr}(i) = \{1, i, -1, -i\}$.

Propriété

Soit G un groupe dont la loi est notée multiplicativement et soit A une partie non vide de G .

On note $A^{-1} = \{x^{-1} \text{ où } x \in A\}$. On a $\text{gr}(A) = \{a_1 a_2 \dots a_n \text{ où } n \in \mathbb{N}^* \text{ et } a_i \in A \cup A^{-1}, \forall i = 1, n\}$.

Démonstration

On pose $E = \{a_1 a_2 \dots a_n \text{ où } n \in \mathbb{N}^* \text{ et } a_i \in A \cup A^{-1}, \forall i = 1, n\}$.

On veut montrer que $\text{gr}(A) = E$.

- (\subset) Il suffit de montrer que E est un sous-groupe de G (qui contient A).
- Puisque l'on a bien E qui contient A , $E \neq \emptyset$.
 - $\forall x, y \in E, \exists n, p \in \mathbb{N}^*$ et $\exists a_1, a_2, \dots, a_n, b_1, b_2, \dots, b_p \in A \cup A^{-1}$ tels que :
 $x = a_1 a_2 \dots a_n$ et $y = b_1 b_2 \dots b_p$. D'où $xy^{-1} = a_1 a_2 \dots a_n b_p^{-1} b_{p-1}^{-1} \dots b_1^{-1}$.
On a bien $xy^{-1} \in E$ car $b_i^{-1} \in A \cup A^{-1} \forall i = 1, p$.
- (\supset) Puisque $\text{gr}(A)$ est un sous-groupe qui contient A , $\text{gr}(A)$ doit être stable par inverse et composition.
Donc $A^{-1} \subset \text{gr}(A)$, $A \cup A^{-1} \subset \text{gr}(A)$ et, $\forall n \in \mathbb{N}^*$, $a_1 a_2 \dots a_n \in \text{gr}(A)$ si $a_i \in A \cup A^{-1}$.

Exemple

Dans $(\mathbb{Z}, +)$, on considère $A = \{2, 3\}$. On a $\text{gr}(A) = \mathbb{Z}$ car $1 = 3 - 2 \in \text{gr}(A)$.

Définition

Soit G un groupe et soit A une partie de G .

On dit que A est une partie génératrice de G si et seulement si $\text{gr}(A) = G$.

Si, de plus, $\text{card}(A) = 1$, on dit que le groupe est monogène.

Exemple

$(\mathbb{Z}, +)$ est monogène car $\text{gr}(1) = \mathbb{Z}$ et (\mathbb{R}^*, \times) n'est pas monogène.

Définition

Soit (G, \cdot) un groupe d'élément neutre 1 et soit x un élément de G .

On définit l'ordre de x (noté $\text{ordre}(x)$, $\text{ord}(x)$ ou encore $\omega(x)$) par :

si $\forall n \in \mathbb{N}^*$, $x^n \neq 1$ alors $\text{ordre}(x) = +\infty$

sinon $\text{ordre}(x)$ est le plus petit entier strictement positif p tel que $x^p = 1$.

Remarque

En notation additive, cela donne : si $\forall n \in \mathbb{N}^*$, $nx \neq 0$ alors $\text{ordre}(x) = +\infty$

sinon $\text{ordre}(x)$ est le plus petit entier strictement positif n tel que $nx = 0$.

Exemples

- Dans (\mathbb{C}^*, \times) , on a $\text{ordre}(1) = 1$, $\text{ordre}(-1) = 2$, $\text{ordre}(i) = 4$ et $\text{ordre}(-i) = 4$.
- Dans $(\mathbb{Z}, +)$, $\text{ordre}(1) = +\infty$, $\text{ordre}(3) = +\infty$ et $\text{ordre}(0) = 1$.

Définition

Le cardinal d'un groupe fini est appelé l'ordre du groupe.

Remarques

- L'ordre d'un élément a d'un groupe est égal à l'ordre de $\text{gr}(a)$ si celui-ci est fini. C'est-à-dire $\text{ordre}(a) = \text{Card}(\text{gr}(a))$ où $\text{gr}(a) = \{a^i \text{ où } i \in \mathbb{Z}\} = \{\dots, a^{-2}, a^{-1}, 1, a, a^2, \dots\}$.
Si $\text{ord}(a) = p$ alors, $\forall i \in \mathbb{Z}$, $i = pq + r$ avec $0 \leq r < p$ et $a^i = a^{pq+r} = a^{pq} a^r = (a^p)^q a^r = a^r$.
D'où $\text{gr}(a) = \{a^r \text{ où } 0 \leq r < p\}$.
- Si un élément x d'un groupe est d'ordre infini, alors $\text{gr}(x)$ est isomorphe à $(\mathbb{Z}, +)$.

Définition

Un groupe est dit cyclique si et seulement si il est monogène et de cardinal fini.

Exemples

- $(\{1, i, -1, -i\}, \times)$ est cyclique.
- $\mathbb{Z}/p\mathbb{Z}$ est cyclique.
- Soit p un entier non nul.
Dans le plan cartésien muni d'un repère orthonormal (O, \vec{i}, \vec{j}) , l'ensemble des rotations de centre O et d'angle $\frac{2k\pi}{p}$ ($k \in \mathbb{Z}$) muni de la loi de composition usuelle des fonctions est un groupe cyclique.

Remarque

Un groupe cyclique est donc un ensemble de la forme $\{1, a, a^2, \dots, a^p\}$.

Propriété

Soit (G, \times) un groupe et soit H un sous-groupe de G . On définit sur G les relations suivantes : $\forall x, y \in G$, $x {}_H\mathcal{R}y \Leftrightarrow x^{-1}y \in H$ et $x \mathcal{R}_H y \Leftrightarrow xy^{-1} \in H$. Ces deux relations sont des relations d'équivalence. On note $(G/H)_g$ et $(G/H)_d$ les ensembles quotients respectifs selon ${}_H\mathcal{R}$ et \mathcal{R}_H .

Remarque

En notation additive, les relations sont : $x {}_H\mathcal{R}y \Leftrightarrow -x + y \in H$ et $x \mathcal{R}_H y \Leftrightarrow x - y \in H$.

Démonstration

Soit e l'élément neutre de G .

Réflexive : $\forall x \in G$, $x^{-1}x = e \in H$ car H sous groupe. Donc $x {}_H\mathcal{R}x$.

Symétrique : $\forall x, y \in G$, $x {}_H\mathcal{R}y \Leftrightarrow x^{-1}y \in H \Rightarrow (x^{-1}y)^{-1} \in H$ car H sous-groupe.
 $\Leftrightarrow y^{-1}x \in H \Leftrightarrow x {}_H\mathcal{R}y$.

Transitive : $\forall x, y, z \in G$, $x {}_H\mathcal{R}y \Leftrightarrow x^{-1}y \in H$
 $y {}_H\mathcal{R}z \Leftrightarrow y^{-1}z \in H \Rightarrow (x^{-1}y)(y^{-1}z) \in H$ car H sous-groupe.
 $\Rightarrow x^{-1}z \in H \Leftrightarrow x {}_H\mathcal{R}z$.

Remarques

Avec les notations de la propriété précédente :

- Soit a un élément de G .

$$\text{On a : } \{x \in G / a {}_H\mathcal{R}x\} = \{x \in G / a^{-1}x \in H\} = \{x \in G / \exists h \in H / a^{-1}x = h\} = \{x \in G / \exists h \in H / x = ah\} \\ = \{ah / h \in H\}$$

$$\text{et } \{x \in G / a \mathcal{R}_H x\} = \{x \in G / x \mathcal{R}_H a\} = \{x \in G / xa^{-1} \in H\} = \{x \in G / \exists h \in H / xa^{-1} = h\} \\ = \{x \in G / \exists h \in H / x = ha\} = \{ha / h \in H\}$$

On note donc aH et Ha les classes respectives de a selon ${}_H\mathcal{R}$ et \mathcal{R}_H .

- $eH = H$ et $He = H$.
- $xy \in H \Leftrightarrow \exists h \in H / xy = h \Leftrightarrow \exists h \in H / y = x^{-1}h \Leftrightarrow y \in x^{-1}H$
 $xy \in H \Leftrightarrow \exists h \in H / xy = h \Leftrightarrow \exists h \in H / x = hy^{-1} \Leftrightarrow x \in Hy^{-1}$

Propriété

Soit (G, \times) un groupe et soit H un sous-groupe de G .

L'ensemble $(G/H)_g$ est fini si et seulement si $(G/H)_d$ est fini. Dans ce cas, on a $\text{card}(G/H)_g = \text{card}(G/H)_d$. Cette valeur commune notée $(G:H)$ est appelée indice de H dans G .

Démonstration

Soit $\varphi : (G/H)_d \rightarrow (G/H)_g$
 $Ha \mapsto a^{-1}H$

- φ surjective par définition de $(G/H)_g$ et $(G/H)_d$.
- $\varphi(Ha) = \varphi(Hb)$
 $\Rightarrow a^{-1}H = b^{-1}H$
 $\Rightarrow a^{-1} \in b^{-1}H$
 $\Rightarrow \exists h \in H / a^{-1} = b^{-1}h.$
 $\Rightarrow \exists h \in H / a = h^{-1}b.$
 $\Rightarrow \exists h' \in H / a = h'b.$
 $\Rightarrow a \in Hb$
 $\Rightarrow Ha = Hb$

Il y a donc une bijection entre $(G/H)_g$ et $(G/H)_d$.

Remarque

Si G est fini, alors les conditions sont trivialement réalisées.
De plus, $(G : \{e\})$ est le cardinal de G .

Propriété

Si (G, \times) est un groupe fini et si H est un sous-groupe de G , alors $\text{card } G = (G:H) \times \text{card } H$.

Démonstration

Soient $A \in (G/H)_d$ et $a \in A$ i.e. $A = Ha = \{ha / h \in H\} = \{x \in G / a \mathcal{B}_H x\}$.

Soit l'application $\varphi_a : H \rightarrow A$
 $h \mapsto ha$

- φ surjective par définition de A .
- $\varphi(h) = \varphi(h')$
 $\Rightarrow ha = h'a$
 $\Rightarrow h = h'$ donc φ injective.

D'où φ_a est bijective.

Toutes les classes de $(G/H)_d$ ont donc le même nombre d'éléments. Celui-ci étant égal à $\text{card } H$.

Remarque

En particulier, puisque l'ordre d'un sous-groupe H d'un groupe fini G divise l'ordre de celui-ci, si $\text{card } G$ est une puissance d'un nombre premier, il en est de même de $\text{card } H$.

Corollaire

Soit (G, \cdot) un groupe d'ordre $n \in \mathbb{N}^*$ d'élément neutre e .

Soit a un élément de G .

i) L'ordre de a est fini et divise n .

ii) $a^n = e$.

iii) Si n est premier, G est cyclique et tout élément de G différent de e engendre G .

Démonstration

On pose $H = \text{gr}(a)$ donc $\text{card} H = \text{ord}(a)$.

i) D'après la propriété précédente avec $H = \text{gr}(a)$.

ii) Par définition de l'ordre de a , $a^{\text{ord}(a)} = e$.

D'où $a^n = a^{(\text{ord}(a)) \times (G:H)} = e^{(G:H)} = e$.

iii) L'ordre de tout élément $b \neq e$ de G est différent de 1 et divise n et donc est égal à n .

Propriété

Soient (G, \cdot) un groupe, H un sous-groupe de G et K un sous-groupe de H .

Les ensembles $(G/H)_g \times (H/K)_g$ et $(G/K)_g$ sont équipotents.

Si ces ensembles sont finis, on a $(G:K) = (G:H) \times (H:K)$.

Démonstration

Puisque les applications $\alpha : G \rightarrow (G/H)_g$ et $\beta : H \rightarrow (H/K)_g$ sont surjectives (surjections canoniques), on

$$x \mapsto xH \quad y \mapsto yK$$

peut trouver deux ensembles $G_1 \subset G$ et $H_1 \subset H$ tels que les restrictions de α et β respectivement à G_1 et H_1 soient bijectives.

Les ensembles $(G/H)_g$ et G_1 sont équipotents. De même pour $(H/K)_g$ et H_1 .

Considérons l'application $\gamma : G_1 \times H_1 \rightarrow (G/K)_g$

$$(x, y) \mapsto (xy)K$$

Pour obtenir le résultat, il suffit de montrer que γ est bijective.

γ est injective.

Soient $(x, y), (x', y')$ deux couples de $G_1 \times H_1$.

$$\gamma(x, y) = \gamma(x', y') \Rightarrow xyK = x'y'K \Rightarrow (x^{-1}x')yK = y'K$$

Puisque yK et $y'K$ sont deux parties de H , $(x^{-1}x')H \cap H \neq \emptyset$.

D'où $x^{-1}x' \in H$, $x \in x'H$ et $xH = x'H$.

Par définition de G_1 , on obtient $x = x'$.

D'où $x^{-1}x = e$ et $yK = y'K$.

Par définition de H_1 , on obtient $y = y'$.

γ est surjective.

Soit $lK \in (G/K)_g$.

Par définition de G_1 , il existe $g \in G_1$ tel que $lH = gH$. Autrement dit, $g^{-1}l \in H$.

Par définition de H_1 , il existe $h \in H_1$ tel que $g^{-1}lK = hK$.

C'est-à-dire $lK = (gh)K = \gamma(g, h)$.

Définition

Soient $(G,*)$ un groupe et \mathcal{R} une relation d'équivalence sur G .

On dit que \mathcal{R} est compatible à gauche avec $*$ si et seulement si, $\forall a,b,c \in G, a \mathcal{R} b \Rightarrow c * a \mathcal{R} c * b$.

On dit que \mathcal{R} est compatible à droite avec $*$ si et seulement si, $\forall a,b,c \in G, a \mathcal{R} b \Rightarrow a * c \mathcal{R} b * c$.

On dit que \mathcal{R} est compatible avec $*$ si elle est compatible à gauche et à droite avec $*$.

Propriété

Soient $(G,*)$ un groupe et \mathcal{R} une relation d'équivalence sur G .

\mathcal{R} est compatible avec $*$ si et seulement si, $\forall a,b,c,d \in G, a \mathcal{R} b$ et $c \mathcal{R} d \Rightarrow a * c \mathcal{R} b * d$.

Démonstration

(\Leftarrow) On a \mathcal{R} réflexive donc, $\forall x \in G, x \mathcal{R} x$.

(\Rightarrow) $\forall a,b,c,d \in G, a \mathcal{R} b \Rightarrow a * c \mathcal{R} b * c$
 $c \mathcal{R} d \Rightarrow b * c \mathcal{R} b * d \Rightarrow a * c \mathcal{R} b * d$

Propriété

Soit (G,\times) un groupe.

Les relations d'équivalence compatibles à gauche (resp. à droite) avec la loi \times sont les relations de la forme ${}_H \mathcal{R}$ (resp. \mathcal{R}_H) où H est un sous-groupe de G .

Démonstration

(Uniquement pour la comptabilité "à gauche" : idem pour "à droite")

- Soit \mathcal{R} une relation d'équivalence compatible à gauche avec la loi \times .

Soit H la classe de l'élément neutre de G .

On a $a \mathcal{R} b \Rightarrow a^{-1} a \mathcal{R} a^{-1} b \Rightarrow e \mathcal{R} a^{-1} b \Rightarrow a^{-1} b \in \text{cl}(e) \Rightarrow a^{-1} b \in H$.
et $a^{-1} b \in H \Rightarrow a^{-1} b \in \text{cl}(e) \Rightarrow e \mathcal{R} a^{-1} b \Rightarrow a e \mathcal{R} a a^{-1} b \Rightarrow a \mathcal{R} b$.

C'est-à-dire $a \mathcal{R} b \Leftrightarrow a^{-1} b \in H$.

H est un sous-groupe.

* $e \in H$ donc $H \neq \emptyset$.

* $\forall x,y \in H$, puisque x et y appartiennent à la même classe, on a $x \mathcal{R} y$.

D'où $x^{-1} y \in H$.

- $\forall x,y,g \in G, x {}_H \mathcal{R} y \Leftrightarrow x^{-1} y \in H \Leftrightarrow x^{-1} g^{-1} g y \in H \Leftrightarrow (gx)^{-1} (gy) \in H \Leftrightarrow gx {}_H \mathcal{R} gy$.

3. Morphismes

Définition

Soient $(G,*)$ et $(G',*)$ deux groupes.

On dit qu'une application f de G vers G' est un homomorphisme de groupes ou simplement un morphisme de groupes si et seulement si : $\forall x,y \in G, f(x * y) = f(x) *' f(y)$.

Exemples

- $f : (\mathbb{R}, +) \rightarrow (\mathbb{R}^*, \times)$
 $x \mapsto \exp x$
- $g : (\mathbb{R}^*, \times) \rightarrow (\mathbb{R}, +)$
 $x \mapsto \ln|x|$
- $h : (\mathbb{C}^*, \times) \rightarrow (\mathbb{C}^*, \times)$
 $z \mapsto \bar{z}$
- Soient $(G, *)$ et $(G', *')$ deux groupes d'éléments neutres respectifs e et e' .
 $i : (G, *) \rightarrow (G', *')$
 $x \mapsto e'$
- Soit $(G_i, *_i)_{i \in I}$ une famille de groupe.
On munit l'ensemble produit $\prod_{i \in I} G_i$ de la loi produit usuelle.
Chaque projection canonique $p_j : \prod_{i \in I} G_i \rightarrow G_j$ est un morphisme.

Remarques

Un morphisme d'un ensemble dans lui-même est appelé un endomorphisme.

Un morphisme bijectif est appelé un isomorphisme.

Un endomorphisme bijectif est appelé un automorphisme.

Deux ensembles sont dits isomorphes s'il existe un isomorphisme de l'un vers l'autre.

Exemples fondamentaux

- Pour tout groupe G , Id_G est un automorphisme de G .
- Soit (G, \times) un groupe et soit x un élément de G .
 $f_x : (\mathbb{Z}, +) \rightarrow (G, \times)$ est un homomorphisme de groupes.
 $n \mapsto x^n$
- Soit $(G, +)$ un groupe et soit x un élément de G .
 $f_x : (\mathbb{Z}, +) \rightarrow (G, +)$ est un homomorphisme de groupes.
 $n \mapsto nx$

Propriété

Soient $(G, *)$ et $(G', *')$ deux groupes d'éléments neutres respectif e et e' .

Soit f un morphisme de groupe de G vers G' .

Alors $f(e) = e'$.

Démonstration

Soit $x \in G$, $f(x) = f(x * e) = f(x) *' f(e)$
 $\Rightarrow [f(x)]^{-1} *' f(x) = [f(x)]^{-1} *' f(x) *' f(e)$
 $\Rightarrow e' = f(e)$

Propriété

Soient $(G,)$ et $(H,)$ deux groupes. Soit f un morphisme de groupes de G vers H .

Alors on a : (i) $\forall x \in G, f(x^{-1}) = [f(x)]^{-1}$
(ii) $\forall x \in G, \forall n \in \mathbb{Z}, f(x^n) = [f(x)]^n$.

Démonstration

- (i)
- $$\begin{aligned} f(x * x^{-1}) &= f(e) = e' \\ \Rightarrow f(x) \nabla f(x^{-1}) &= e' \\ \Rightarrow [f(x)]^{-1} \nabla f(x) \nabla f(x^{-1}) &= [f(x)]^{-1} \nabla e' \\ \Rightarrow e' \nabla f(x^{-1}) &= [f(x)]^{-1} \\ \Rightarrow f(x^{-1}) &= [f(x)]^{-1} \end{aligned}$$
- (ii) 1ère étape : Si $n \geq 0$, on utilise une démonstration par récurrence :
- vrai au rang 0 : par convention $x^0 = e$
 - on suppose vrai au rang n
- $$\begin{aligned} f(x^{n+1}) &= f(x^n * x) \\ &= f(x^n) * f(x) \\ &= [f(x)]^n \nabla f(x) \\ &= [f(x)]^{n+1} \end{aligned}$$
- 2ème étape : Si $n < 0$, alors $f(x^n) = f[(x^{-1})^{-n}] = [f(x^{-1})]^{-n} = [f(x)^{-1}]^{-n} = [f(x)]^n$.

Remarque

En notation additive, cela donne :

- (i') $\forall x \in G, f(-x) = -f(x)$.
(ii') $\forall x \in G, \forall n \in \mathbb{Z}$, on a $f(nx) = nf(x)$.

Propriété

Soient $(G, *)$ un groupe, H un sous-groupe de G et j l'injection canonique de H dans G .

Alors :

1. j est un morphisme.
2. L'élément neutre de H est le même que celui de G .
3. Le symétrique d'un élément de H dans H est le même que dans G .

Démonstration

1. Trivial car H est un groupe pour la loi induite de G .
2. Si on note e_H l'élément neutre de H et e_G celui de G , on a $e_H = j(e_H) = e_G$.
3. Si on note a_H le symétrique d'un l'élément a de H dans H et a_G celui dans G , on a :
 $a_H = j(a_H) = [j(a)]^{-1} = a^{-1} = a_G$.

Propriété

La composée de deux morphismes est un morphisme.

La composée de deux isomorphismes est un isomorphisme.

Démonstration

Soient $(G_1, *_1)$, $(G_2, *_2)$ et $(G_3, *_3)$ trois groupes.

Soit f un morphisme de groupe de G_1 vers G_2 et soit g un morphisme de groupe de G_2 vers G_3 .

$$\begin{aligned} \forall a, b \in G_1, (g \circ f)(a *_1 b) &= g[f(a *_1 b)] \\ &= g[f(a) *_2 f(b)] \quad \text{car } f \text{ est un morphisme} \\ &= g[f(a)] *_3 g[f(b)] \quad \text{car } g \text{ est un morphisme.} \end{aligned}$$

Propriété

La réciproque d'un isomorphisme est un isomorphisme.

Démonstration

Soient $(G_1, *_1)$ et $(G_2, *_2)$ deux groupes et soit f un isomorphisme de G_1 vers G_2 .

On doit montrer que f^{-1} est un morphisme.

Puisque f est bijectif, $\forall y, y' \in G_2, \exists x, x' \in G_1 / y = f(x)$ et $y' = f(x')$ c'est-à-dire $x = f^{-1}(y)$ et $x' = f^{-1}(y')$

$$\begin{aligned} \text{On a } f^{-1}(y *_2 y') &= f^{-1}(f(x) *_2 f(x')) \\ &= f^{-1}(f(x *_1 x')) \\ &= x *_1 x' = f^{-1}(y) *_1 f^{-1}(y'). \end{aligned}$$

Remarque

On note $\text{Aut}(G)$ l'ensemble des automorphismes d'un groupe G . $\text{Aut}(G)$ est un sous-groupe de $(S(G), \circ)$.

Définition

Soit $(G_1, *_1)$ un groupe d'élément neutre e_1 et soit $(G_2, *_2)$ un groupe d'élément neutre e_2 .

Soit f un morphisme de groupe de G_1 vers G_2 .

On appelle image de f et on note $\text{Im } f$ l'ensemble image de f c'est-à-dire :

$$\text{Im } f = \{y \in G_2 / \exists x \in G_1; y = f(x)\}.$$

On appelle noyau de f et on note $\text{Ker } f$ l'image réciproque de $\{e_2\}$ c'est-à-dire :

$$\text{Ker } f = \{x \in G_1 / f(x) = e_2\}.$$

Exemples

- Soit $f: (\mathbb{R}, +) \rightarrow (\mathbb{R}^*, \times)$. On a $\text{Ker } f = \{0\}$ et $\text{Im } f = \mathbb{R}_+^*$.
 $x \mapsto \exp x$
- Soit $f: (\mathbb{Z}, +) \rightarrow (\mathbb{Z}/2\mathbb{Z}, +)$. On a $\text{Ker } f = 2\mathbb{Z}$ et $\text{Im } f = \mathbb{Z}/2\mathbb{Z}$.
 $p \mapsto \bar{p}$

Propriété

Soient $(G_1, *_1)$ et $(G_2, *_2)$ deux groupes et d'éléments neutres respectifs e_1 et e_2 .

Soit f un morphisme de groupe de G_1 vers G_2 .

On a : f injective $\Leftrightarrow \text{Ker } f = \{e_1\}$.

Démonstration

(\Rightarrow) Soit $x \in \text{Ker } f$. On a $f(x) = e_2 = f(e_1)$.

Puisque f est injective, on obtient $x = e_1$.

(\Leftarrow) Soient $x, x' \in G_1$.

$$\begin{aligned} \text{On a } f(x) = f(x') &\Rightarrow f(x) *_2 [f(x')]^{-1} = e_2 \\ &\Rightarrow f(x) *_2 f(x'^{-1}) = e_2 \\ &\Rightarrow f(x *_1 x'^{-1}) = e_2 \\ &\Rightarrow x *_1 x'^{-1} \in \text{Ker } f \\ &\Rightarrow x *_1 x'^{-1} = e_1 \quad \Rightarrow x = x'. \end{aligned}$$

Propriété

Soit H_1 un sous-groupe d'un groupe $(G_1, *_1)$ d'élément neutre e_1 .

Soit H_2 un sous-groupe d'un groupe $(G_2, *_2)$ d'élément neutre e_2 .

Soit f un morphisme de groupe de G_1 vers G_2 .

Alors $f(H_1)$ est un sous-groupe de G_2 et $f^{-1}(H_2)$ est un sous-groupe de G_1 .

En particulier, $\text{Im} f$ est un sous-groupe de G_2 et $\text{Ker} f$ est un sous-groupe de G_1 .

Démonstration

◇ $f(H_1)$ sous-groupe de G_2 .

- $e_1 \in H_1$ donc $f(e_1) = e_2 \in f(H_1)$ et $f(H_1) \neq \emptyset$.

- Soient b_1 et b_2 deux éléments de $f(H_1)$.

$\exists a_1 \in H_1 / b_1 = f(a_1)$ et $\exists a_2 \in H_1 / b_2 = f(a_2)$.

On a $b_1 *_2 (b_2)^{-1} = f(a_1) *_2 (f(a_2))^{-1} = f(a_1) *_2 f(a_2^{-1}) = f(a_1 *_1 a_2^{-1})$.

Or $a_1 *_1 a_2^{-1} \in H_1$ car H_1 est un sous-groupe de G_1 . Donc $b_1 *_2 (b_2)^{-1} \in f(H_1)$.

◇ $f^{-1}(H_2)$ sous-groupe de G_1 .

- $e_2 \in H_2$ et $f(e_1) = e_2$ donc $e_1 \in f^{-1}(H_2)$ et $f^{-1}(H_2) \neq \emptyset$.

- Soient a_1 et a_2 deux éléments de $f^{-1}(H_2)$.

On a $f(a_1) \in H_2$ et $f(a_2) \in H_2$ et donc $f(a_1) *_2 (f(a_2))^{-1} \in H_2$ car H_2 est un sous-groupe de G_2 .

Or $f(a_1 *_1 a_2^{-1}) = f(a_1) *_2 f(a_2^{-1}) = f(a_1) *_2 (f(a_2))^{-1} \in H_2$

Donc $a_1 *_1 a_2^{-1} \in f^{-1}(H_2)$.

Remarques

- Soit f un morphisme de groupes de G vers G' . Si f est injective, $\text{Im} f$ est isomorphe à G .

- Soit $(G_1, *_1)$ un groupe d'élément neutre e_1 et soit $(G_2, *_2)$ un groupe d'élément neutre e_2 .

Soit f un morphisme de groupes de G_1 vers G_2 .

Alors, $\forall x \in G_1, \forall a \in \text{Ker} f, x *_1 a *_1 x^{-1} \in \text{Ker} f$.

Propriété

Soit $(G, *)$ un groupe d'élément neutre e .

Pour tout élément a de G , on définit une application $i_a : G \rightarrow G$

$$x \mapsto a * x * a^{-1}.$$

On a : i) $i_e = \text{Id}_G$

ii) $i_a \circ i_b = i_{a*b}$

iii) $(i_a)^{-1} = i_{a^{-1}}$

i_a est un automorphisme de G appelé automorphisme intérieur.

On note $\text{Int}(G)$ l'ensemble des automorphismes intérieurs de G .

L'application $i : G \rightarrow \text{Aut}(G)$ est un morphisme de groupes.

$$a \mapsto i_a$$

On a $\text{Ker} i = Z(G)$ et, par définition, $\text{Im} i = \text{Int}(G)$.

Démonstration

- i) Trivial

ii) $\forall x \in G, (i_a \circ i_b)(x) = i_a(i_b(x)) = i_a(b * x * b^{-1}) = a * (b * x * b^{-1}) * a^{-1}$
 $= (a * b) * x * (a * b)^{-1} = i_{a*b}(x)$.

iii) On a : $i_{a^{-1}} \circ i_a = i_{a^{-1}*a} = i_e = \text{Id}_G$ et de même $i_a \circ i_{a^{-1}} = \text{Id}_G$. C'est-à-dire $i_{a^{-1}} = (i_a)^{-1}$.

- Il reste à montrer que, pour tout $a \in G$, i_a est un morphisme car on a déjà l'application réciproque.

$$\begin{aligned} \forall x, y \in G, i_a(x * y) &= a * (x * y) * a^{-1} \\ &= a * x * e * y * a^{-1} \\ &= a * x * (a^{-1} * a) * y * a^{-1} \\ &= (a * x * a^{-1}) * (a * y * a^{-1}) \\ &= i_a(x) * i_a(y) \end{aligned}$$
- D'après ii), i est un morphisme.

$$\begin{aligned} a \in \text{Ker } i &\Leftrightarrow i_a = \text{Id}_G \\ &\Leftrightarrow \forall x \in G, i_a(x) = \text{Id}_G(x) \\ &\Leftrightarrow \forall x \in G, a * x * a^{-1} = x \\ &\Leftrightarrow \forall x \in G, a * x = x * a \\ &\Leftrightarrow a \in Z(G). \end{aligned}$$

Remarques

- $\text{Int}(G)$ est sous-groupe de $\text{Aut}(G)$.
- G commutatif ($\Leftrightarrow Z(G) = G$) $\Leftrightarrow \text{Int}(G) = \{\text{Id}_G\}$.

Définition

Soient x et y deux éléments d'un groupe $(G,)$.

On dit que y est un conjugué de x s'il existe un élément g de G tel que $y = g x g^{-1}$.

Propriété

Soit G un groupe.

La relation \mathcal{R} définie par $x \mathcal{R} y$ si et seulement si y est un conjugué de x est une relation d'équivalence.

Démonstration

- $\forall x \in G, x = e x e^{-1}$ donc $x \mathcal{R} x$.
- $\forall x, y \in G, x \mathcal{R} y \Rightarrow \exists g \in G / y = g x g^{-1}$
Donc $x = g^{-1} y g = g^{-1} y (g^{-1})^{-1}$
Puisque $g^{-1} \in G$, on obtient bien $y \mathcal{R} x$.
- $\forall x, y, z \in G, x \mathcal{R} y \Rightarrow \exists g \in G / y = g x g^{-1}$
 $y \mathcal{R} z \Rightarrow \exists g' \in G / z = g' y g'^{-1}$
Donc $z = g' y g'^{-1} = g' (g x g^{-1}) g'^{-1} = (g'g) x (g'g)^{-1}$
Puisque $g'g \in G$, on obtient bien $x \mathcal{R} z$.

Remarque

- On peut donc dire que x et y sont conjugués.
- Les classes d'équivalence (qui forment une partition de G) sont appelées classes d'éléments conjugués et parfois simplement classes conjuguées.

Propriété

Soient G un groupe, H un sous-groupe de G et g un élément de G .

L'ensemble $\{g h g^{-1} / h \in H\}$ noté $g H g^{-1}$ est un sous-groupe de G appelé groupe conjugué de H par g .

Démonstration

- $e \in H \Rightarrow g e g^{-1} \in g H g^{-1}$
 $\Rightarrow g g^{-1} \in g H g^{-1}$
 $\Rightarrow e \in g H g^{-1}$ donc $g H g^{-1} \neq \emptyset$.
- Soient $h_1, h_2 \in H$.
 $(g h_1 g^{-1})(g h_2 g^{-1})^{-1} = (g h_1 g^{-1})((g^{-1})^{-1} h_2^{-1} g^{-1})$
 $= g h_1 g^{-1} g h_2^{-1} g^{-1}$
 $= g h_1 h_2^{-1} g^{-1}$ avec $h_1 h_2^{-1} \in H$.

Propriété

Soit G un groupe.

La relation \mathcal{R} sur les sous-groupes de G définie par $H \mathcal{R} K \Leftrightarrow \exists g \in G / K = g H g^{-1}$ est une relation d'équivalence. Deux groupes qui sont dans la même classe d'équivalence sont dits conjugués.

Démonstration

- Réflexive : Il suffit de prendre $g = e$.
- Symétrique : (Si $g \in G$, alors $g^{-1} \in G$)
 $H \mathcal{R} K \Rightarrow \exists g \in G / K = g H g^{-1} \Rightarrow H = g^{-1} K g = g^{-1} K (g^{-1})^{-1} \Rightarrow H \mathcal{R} K$.
- Transitive : (Si $g, g' \in G$, alors $g' g \in G$)
 $H \mathcal{R} K \Rightarrow \exists g \in G / K = g H g^{-1}$
 $K \mathcal{R} L \Rightarrow \exists g' \in G / L = g' K g'^{-1}$
Donc $L = g' K g'^{-1} = g'(g H g^{-1})g'^{-1} = (g'g)H(g'g)^{-1}$.

4. Sous-groupes distingués

Définition

Soit $(G, *)$ un groupe et soit H un sous-groupe de G .

On dit que H est un sous-groupe distingué (ou normal) et on note $H \triangleleft G$ si et seulement si $\forall x \in G, \forall a \in H, x * a * x^{-1} \in H$.

Remarques

Avec les notations de la définition :

- Autrement dit, $H \triangleleft G \Leftrightarrow \forall x \in G, x H x^{-1} \subset H$.
- Si e est l'élément neutre de G , alors G et $\{e\}$ sont des sous-groupes normaux de G .
- Si G est abélien, tous les sous-groupes sont distingués.
- L'intersection de deux sous-groupes distingués est un sous-groupe distingué.
- On a aussi : $H \triangleleft G$ si et seulement si $i(H) \subset H$ pour tout $i \in \text{Int}(G)$.
- On dit qu'un sous-groupe H d'un groupe G est caractéristique si et seulement si $j(H) \subset H$ pour tout $j \in \text{Aut}(G)$.

Propriété

Soit $(G, *)$ un groupe et soit $H \triangleleft G$. On a $i(H) = H$ pour tout $i \in \text{Int}(G)$.

Démonstration

$\forall i \in \text{Int}(G)$, on a $i^{-1} \in \text{Int}(G)$. Donc $i^{-1}(H) \subset H$. Or $H = (i \circ i^{-1})(H) = i(i^{-1}(H)) \subset i(H)$.
Puisque $i(H) \subset H$, on a bien $i(H) = H$.

Propriété

Soient $(G_1, *_1)$ et $(G_2, *_2)$ deux groupes. Soient $H_1 \triangleleft G_1$ et $H_2 \triangleleft G_2$ et soit f un morphisme de G_1 dans G_2 .
Alors $f(H_1) \triangleleft f(G_1)$ et $f^{-1}(H_2) \triangleleft G_1$. En particulier, $\text{Ker } f \triangleleft G_1$.

Démonstration

Cela découle directement du fait que, $\forall a \in G_1, \forall x \in H_1, f(a *_1 x *_1 a^{-1}) = f(a) *_2 f(x) *_2 f(a)^{-1}$.

Remarques

- En général, $f(H_1)$ n'est pas un sous-groupe normal de G_2 .
- $Z(G)$ le centre d'un groupe G est un sous-groupe distingué de ce groupe.
Cela peut être montré directement ou en utilisant la propriété précédente avec l'application $i : G \rightarrow \text{Aut}(G)$ puisque $\text{Ker } i = Z(G)$.
 $a \mapsto i_a$
En particulier, cela signifie que le centre est non vide.

Propriété

Soit (G, \times) un groupe et soit H un sous-groupe de G .

On a $H \triangleleft G \Leftrightarrow {}_H\mathcal{R} = \mathcal{R}_H$ et, dans ce cas, $aH = Ha \forall a \in G$ i.e. $(G/H)_g = (G/H)_d$.

Démonstration

- (\Rightarrow) On suppose $H \triangleleft G$.
 $\forall x \in G, \forall h \in H, xhx^{-1} \in H$. C'est-à-dire qu'il existe $h' \in H$ tel que $xhx^{-1} = h'$ ou encore $xh = h'x$.
 $\forall x, y \in G, x {}_H\mathcal{R} y \Leftrightarrow x^{-1}y \in H$
 $\Leftrightarrow \exists h \in H / x^{-1}y = h$
 $\Leftrightarrow \exists h \in H / y = xh$
 $\Leftrightarrow \exists h' \in H / y = h'x$
 $\Leftrightarrow \exists h' \in H / yx^{-1} = h'$
 $\Leftrightarrow yx^{-1} \in H$
 $\Leftrightarrow y \mathcal{R}_H x \Leftrightarrow x \mathcal{R}_H y$.

- (\Leftarrow) On suppose ${}_H\mathcal{R} = \mathcal{R}_H$.
 $\forall x \in G$, on a donc $xH = Hx$ c'est-à-dire $xHx^{-1} = H$.

Remarques

- Si e est l'élément neutre de G , on a $eH = H = He$.
- Si $H \triangleleft G$, l'ensemble quotient est noté G/H .
Pour tout x de G , on note aussi \bar{x} la classe de x selon ${}_H\mathcal{R}$ (ou \mathcal{R}_H).
C'est-à-dire $\text{cl}(x) = \{y \in H / x {}_H\mathcal{R} y\} = xH$.

Corollaire

Soit (G, \times) un groupe. Les relations d'équivalence compatibles avec la loi \times sont les relations de la forme ${}_H\mathcal{R}$ ou \mathcal{R}_H où H est un sous-groupe distingué de G .

Démonstration

Soit \mathcal{R} une relation d'équivalence compatible avec la loi de G . Soit H la classe de l'élément neutre de G .

\mathcal{R} compatible à gauche $\Rightarrow \mathcal{R} = {}_H\mathcal{R}$

\mathcal{R} compatible à droite $\Rightarrow \mathcal{R} = \mathcal{R}_H$

D'où $\mathcal{R}_H = {}_H\mathcal{R}$.

Remarques

- Si G est un groupe et si H est un sous-groupe de G , alors $\bigcap_{g \in G} gHg^{-1}$ est le plus grand sous-groupe normal de G inclus dans H .
- Dans une structure quotient, si on veut pouvoir définir simplement $\bar{x} \bar{\times} \bar{y} = \overline{x \times y}$, il faut que, si x' est un autre représentant de \bar{x} et si y' est un autre représentant de \bar{y} , alors $\overline{x' \times y'} = \overline{x \times y}$. C'est-à-dire $x' \mathcal{R} x$ et $y' \mathcal{R} y \Rightarrow x' * y' \mathcal{R} x * y$.

Propriété

Soit (G, \times) un groupe et soit H un sous-groupe normal de G .

L'opération $\bar{\times}$ sur l'ensemble quotient G/H définie par $\forall \bar{x}, \bar{y} \in G/H, \bar{x} \bar{\times} \bar{y} = \overline{x \times y}$ donne une structure de groupe à G/H .

Démonstration

Loi de composition interne : évident.

$\forall \bar{x}, \bar{y}, \bar{z} \in G/H, (\bar{x} \bar{\times} \bar{y}) \bar{\times} \bar{z} = \overline{(x \times y) \times z} = \overline{x \times (y \times z)} = \bar{x} \bar{\times} \overline{y \times z} = \bar{x} \bar{\times} (\bar{y} \bar{\times} \bar{z})$.

$\forall \bar{x} \in G/H, \bar{x} \bar{\times} \bar{e} = \overline{x \times e} = \bar{x}$ et $\bar{e} \bar{\times} \bar{x} = \overline{e \times x} = \bar{x}$.

$\forall \bar{x} \in G/H, \bar{x} \bar{\times} \bar{x}^{-1} = \overline{x \times x^{-1}} = \bar{e}$ et $\bar{x}^{-1} \bar{\times} \bar{x} = \overline{x^{-1} \times x} = \bar{e}$ c'est-à-dire $\bar{x}^{-1} = (\bar{x})^{-1}$.

Remarques

Soit (G, \times) un groupe et $H \triangleleft G$.

• $\bar{\times}$ est simplement noté " \times " ou "." ou "" et est appelée loi quotient.

• G/H est alors appelé le groupe quotient de G par H .

• $\bar{e} = H$ est l'élément neutre du groupe quotient G/H .

• La surjection canonique $p : G \rightarrow G/H$

$$x \mapsto \bar{x}$$

est un morphisme de groupes.

On a $\text{Ker } p = H$.

On note $p(g) = \bar{g} = \{gh \mid h \in H\} = gH$.

• Si G est un groupe commutatif, il en est de même du groupe quotient.

• L'opération $\forall \bar{x}, \bar{y} \in G/H, \bar{x} \bar{\times} \bar{y} = \overline{x \times y}$ peut aussi s'écrire $\forall gH, g'H \in G/H, gHg'H = (gg')H$.

Exemple

Cas particulier $(G, \times) = (\mathbb{Z}, +)$ et $H = 3\mathbb{Z}$.

$\forall x, y \in \mathbb{Z}, x \mathcal{R} y \Leftrightarrow x - y \in 3\mathbb{Z}$.

On a : $\bar{0} = \{x \in \mathbb{Z} / x \mathcal{R} 0\} = \{x \in \mathbb{Z} / x - 0 \in 3\mathbb{Z}\} = \{x \in \mathbb{Z} / x = 0 + 3p \text{ où } p \in \mathbb{Z}\}$

$\bar{1} = \{x \in \mathbb{Z} / x \mathcal{R} 1\} = \{x \in \mathbb{Z} / x - 1 \in 3\mathbb{Z}\} = \{x \in \mathbb{Z} / x = 1 + 3p \text{ où } p \in \mathbb{Z}\}$

$\bar{2} = \{x \in \mathbb{Z} / x \mathcal{R} 2\} = \{x \in \mathbb{Z} / x - 2 \in 3\mathbb{Z}\} = \{x \in \mathbb{Z} / x = 2 + 3p \text{ où } p \in \mathbb{Z}\}$

On a alors les opérations :

+	$\bar{0}$	$\bar{1}$	$\bar{2}$
$\bar{0}$	$\bar{0}$	$\bar{1}$	$\bar{2}$
$\bar{1}$	$\bar{1}$	$\bar{2}$	$\bar{0}$
$\bar{2}$	$\bar{2}$	$\bar{0}$	$\bar{1}$

Remarque

Soient E, F deux groupes et f un morphisme de E dans F .

On définit une relation d'équivalence sur E dite associée à f en posant, $\forall x, y \in E, x \mathcal{R} y \Leftrightarrow f(x) = f(y)$.

Cette relation est compatible avec les lois car $x \mathcal{R} y \Leftrightarrow f(xy^{-1}) = e_F \Leftrightarrow xy^{-1} \in \text{Ker } f \triangleleft E$.

Soient ϕ la surjection canonique associée à E/\mathcal{R} et j l'injection canonique de $f(E)$ dans F .

Il existe une unique bijection \tilde{f} de E/\mathcal{R} dans $f(E)$ telle que $f = j \circ \tilde{f} \circ \phi$ (décomposition canonique de f).

Plus précisément, \tilde{f} est un isomorphisme.

Autrement dit, $\text{Im } f$ est isomorphe à $E/\text{Ker } f$.

Si f est surjective, on a donc F isomorphe à $E/\text{Ker } f$.

Application

Soit $i : G \rightarrow \text{Aut}(G)$ où $i_a : G \rightarrow G$
 $a \mapsto i_a$ $x \mapsto a * x * a^{-1}$.

On obtient :

$Z(G)$ est un sous-groupe normal de G et $G/Z(G)$ est isomorphe à $\text{Int}(G)$.

Propriété

Soit (G, \times) un groupe et soit H un sous-groupe normal de G .

Soit L un groupe et ϕ un morphisme de groupes de G vers L tel que $H \subset \text{Ker } \phi$.

Alors il existe un seul morphisme ϕ' de G/H dans L tel que $\phi = \phi' \circ p$ où p est la projection canonique.

De plus, $\text{Im } \phi = \text{Im } \phi'$ et $\text{Ker } \phi' = \text{Ker } \phi/H$.

Remarque

Si $H = \text{Ker } \phi$, alors $\text{Ker } \phi' = \{e\}$ et ϕ' est injective.

Démonstration

- Il faut donc que l'opération qui, pour tout g de G , consiste à associer à la classe gH l'élément $\phi(g)$ de L soit bien une application uniquement déterminée et un morphisme de groupes.

Si $gH = g'H$ alors il existe $h \in H$ tel que $g' = gh$.
 D'où $\varphi(g') = \varphi(gh) = \varphi(g)\varphi(h)$ or $H \subset \text{Ker } \varphi$ donc $\varphi(h) = e'$ où e' est l'élément neutre de L .
 $= \varphi(g)e' = \varphi(g)$.

On définit bien une application en considérant $\varphi' : G/H \rightarrow L$
 $gH \mapsto \varphi(g)$

Par hypothèse φ' est uniquement déterminée.

Soient $\bar{x}, \bar{y} \in G/H$. On a : $\varphi'(\bar{x}\bar{y}) = \varphi'(\overline{xy}) = \varphi(xy) = \varphi(x)\varphi(y) = \varphi'(\bar{x})\varphi'(\bar{y})$.

- L'égalité $\text{Im } \varphi = \text{Im } \varphi'$ est triviale.
- Soit $K = \text{Ker } \varphi$.

Par hypothèse, $H \subset K$. Puisque H est un sous-groupe normal de G , c'en est un de K .

D'où K/H est bien défini et c'est un sous-groupe de G/H .

$gH \in \text{Ker } \varphi' \Leftrightarrow \varphi'(gH) = e' \Leftrightarrow \varphi(g) = e' \Leftrightarrow g \in K \Leftrightarrow gH \in K/H$.

Corollaire

Soient G et L deux groupes.

Soient φ un morphisme de groupes de G vers L surjectif et $H = \text{Ker } \varphi$.

Alors il existe un seul isomorphisme φ' de G/H dans L tel que $\varphi = \varphi' \circ p$ où p est la projection canonique.

On a alors $L = \text{Im } \varphi \simeq G/H = G/\text{Ker } \varphi$.

Propriété

Soient H et K deux sous-groupes d'un groupe G .

Si $K \triangleleft G$, alors le sous-groupe engendré par $H \cup K$ est l'ensemble $HK = \{hk \text{ où } h \in H \text{ et } k \in K\}$.

Démonstration

Il suffit de montrer que HK est un sous-groupe de G .

Soit 1 l'élément neutre de G .

$1 \times 1 = 1 \in HK$.

Soient h_1k_1 et h_2k_2 deux éléments de HK avec $h_1, h_2 \in H$ et $k_1, k_2 \in K$.

$$h_1k_1(h_2k_2)^{-1} = h_1k_1k_2^{-1}h_2^{-1} = h_1h_2^{-1}(h_2k_1k_2^{-1}h_2^{-1})$$

Or $h_1h_2^{-1} \in H$ et $k_1k_2^{-1} \in K$ car H et K sont des sous-groupes.

De plus, $h_2k_1k_2^{-1}h_2^{-1} \in K$ car K est normal.

Propriété

Soient H et K deux sous-groupes d'un groupe G . On suppose que $K \triangleleft G$.

Alors i) $H \cap K \triangleleft H$

ii) $H/H \cap K \simeq HK/K$

Démonstration

i) # $H \cap K$ sous-groupe de G donc c'est un groupe et $H \cap K \subset H$.

Soit $x \in H \cap K$ et $h \in H$.

$hxh^{-1} \in K$ car $x \in K$ et K normal.

$hxh^{-1} \in H$ car $x \in H$ et H sous-groupe.

ii) Soit p la projection canonique de G dans G/K . On pose $p_0 = p|_H$ (la restriction de p à H).

p_0 est un morphisme de groupes de H dans G/K .

On a $\text{Ker } p_0 = H \cap \text{Ker } p = H \cap K$ donc $\text{Im } p_0 \simeq H/\text{Ker } p_0 = H/H \cap K$

Or $\text{Im } p_0 = \{hK / h \in H\}$ donc $\text{Im } p_0 = HK/K$.

Propriété

Soient H et K deux sous-groupes d'un groupe G . On suppose que $H \triangleleft G$, $K \triangleleft G$ et $K \subset H$.

Alors $H/K \triangleleft G/K$ et $(G/K)/(H/K) \simeq G/H$.

De plus, l'application $f: G/K \rightarrow G/H$ est un morphisme de groupes.

$$gK \mapsto gH$$

Démonstration

Montrons, dans un premier temps, que f est bien une application uniquement définie : si $gK = g'K$ alors il existe $k \in K$ tel que $g' = gk$. Puisque $K \subset H$, on a bien $gH = g'H$.

Soient $gK, g'K \in G/K$.

$$f(gK \ g'K) = f(gg'K) = gg'H = (gH) (g'H) = f(gK) f(g'K).$$

$$\text{Ker } f = \{gK / f(gK) = H\} = \{gK / gH = H\} = \{gK / g \in H\} = H/K$$

On a donc $H/K \triangleleft G/K$ et $\text{Im } f = \{gH / g \in G\} = G/H$.

Définition

Soient $(G_i)_{i=1,n}$ une famille finie de groupes.

Pour tout entier i compris entre 1 et $n-1$, soit f_i un morphisme de G_i dans G_{i+1} .

On peut représenter cette situation par : $G_1 \xrightarrow{f_1} G_2 \xrightarrow{f_2} G_3 \xrightarrow{f_3} \dots \xrightarrow{f_{n-2}} G_{n-1} \xrightarrow{f_{n-1}} G_n$.

Cette suite est dite exacte si et seulement si $\text{Im } f_i = \text{Ker } f_{i+1}$ pour tout $i = 1, n-1$.

Remarque

Il existe, à un isomorphisme près, un seul groupe à un unique élément que l'on peut noter 1 et un seul morphisme de 1 dans G ou de G dans 1.

Dire que la suite $1 \rightarrow G \xrightarrow{f} G'$ est exacte signifie que f est injective.

Dire que la suite $G \xrightarrow{g} G \rightarrow 1$ est exacte signifie que g est surjective.

Propriété

Soient G un groupe et $H \triangleleft G$.

Soient i l'injection canonique de H dans G et φ la surjection canonique de G dans G/H .

La suite $1 \rightarrow H \xrightarrow{i} G \xrightarrow{\varphi} G/H \rightarrow 1$ est exacte.

Définition

Soit G un groupe et soient a et b deux éléments de G .

On appelle commutateur de a et b l'élément $[a, b] = aba^{-1}b^{-1} = ab(ba)^{-1}$.

On appelle groupe dérivé de G le sous-groupe $D(G) = \langle [a, b] / (a, b) \in G \times G \rangle$.

Remarque

L'ensemble des commutateurs n'est pas en général un groupe.

Propriété

Soit G un groupe et soient a, b et c trois éléments de G .

- $[a, b] = 1 \Leftrightarrow a$ et b commutent
- $[a, b]^{-1} = [b, a]$
- $[a, bc] = [a, b] b [a, c] b^{-1}$
- $[ab, c] = a [b, c] a^{-1} [a, c]$

Démonstration

- $ab(ba)^{-1} = 1 \Leftrightarrow ab = ba$
- $[a, b]^{-1} = (aba^{-1}b^{-1})^{-1} = bab^{-1}a^{-1}$
- $[a, b] b [a, c] b^{-1} = aba^{-1}b^{-1} b aca^{-1}c^{-1} b^{-1} = abca^{-1}c^{-1}b^{-1} = a(bc)a^{-1}(bc)^{-1}$
- $a [b, c] a^{-1} [a, c] = a bcb^{-1}c^{-1} a^{-1} aca^{-1}c^{-1} = abcb^{-1}a^{-1}c^{-1} = (ab)c(ab)^{-1}c^{-1}$

Propriété

Soit G un groupe.

- $D(G) \triangleleft G$ et $G/D(G)$ est commutatif
- Soit $H \triangleleft G$ tel que G/H soit commutatif alors $D(G) \subset H$.
- Soit H un sous-groupe de G tel que $D(G) \subset H$ alors $H \triangleleft G$ et G/H est commutatif.
- Soit $f: G \rightarrow G'$ un morphisme de groupes alors $f(D(G)) \subset D(G')$.
De plus, si f est surjective, alors $f(D(G)) = D(G')$.

Démonstration

- $\forall g, a, b \in G, g[a, b]g^{-1} = [gag^{-1}, gbg^{-1}]$
Soient $c_1, c_2, \dots, c_k \in D(G)$.
 $\forall g \in G, gc_1c_2c_3\dots c_kg^{-1} = (gc_1g^{-1})(gc_2g^{-1})(gc_3g^{-1}) \dots (gc_kg^{-1}) \in D(G)$.
 - Soit $p: G \rightarrow G/D(G)$ la projection canonique.
 $\forall a, b \in G, p(a)p(b) = p(b)p(a) \Leftrightarrow [p(a), p(b)] = 1 = p([a, b])$.
- Soit $H \triangleleft G$.
Soit $p: G \rightarrow G/H$ la projection canonique.
On a p est surjective.
Par hypothèses, $\forall a, b \in G, p(a)p(b) = p(b)p(a)$
C'est-à-dire $p([a, b]) = 1 \Leftrightarrow [a, b] \in \text{Ker } p$.
 $\Leftrightarrow D(G) = \text{Ker } p = H$.
- $\forall g \in G, \forall h \in H, ghg^{-1} = ghg^{-1}h^{-1}h = [g, h]h \in H$.
Donc $H \triangleleft G$.
Soit $p: G \rightarrow G/H$ la projection canonique.
On a $[p(a), p(b)] = 1$ car $D(G) \subset \text{Ker } p = H$.
- $\forall a, b \in G, f([a, b]) = [f(a), f(b)]$.
D'où l'inclusion.

Définition

Soit G un groupe.

La suite de groupes $(D_n(G))_{n \in \mathbb{N}}$ définie par $D_0(G) = G$ et $D_{n+1}(G) = D(D_n(G))$ pour tout entier $n \geq 0$, est appelée suite dérivée de G .

Propriété

Soient G un groupe et H un sous-groupe de G

Soit f un morphisme de G vers H .

Pour tout entier n , $f(D_n(G)) \subset D_n(H)$.

De plus, si f est surjective, alors $f(D_n(G)) = D_n(H)$.

Démonstration

Récurrence trivial via le 4° de la propriété précédente.

Remarque

Cette propriété reste vraie, en particulier, lorsque $H = G$ et que f est un automorphisme de G .

Définition

Un groupe G est dit résoluble si et seulement si il existe un entier n tel que $D_n(G) = \{e\}$.

Définition

On appelle suite normale d'un groupe G toute suite finie de $m \in \mathbb{N}^*$ sous-groupes de G vérifiant :

$$G_m \triangleleft G_{m-1} \triangleleft \dots \triangleleft G_1 \triangleleft G_0 = G.$$

Propriété

Soit G un groupe.

Les trois propriétés suivantes sont équivalentes :

- (1) G est résoluble
- (2) Il existe une suite de $m \in \mathbb{N}^*$ sous-groupes distingués de G , $\{e\} = G_m \subset G_{m-1} \subset \dots \subset G_1 \subset G_0 = G$ tels que G_k/G_{k+1} soit abélien pour tout entier k compris entre 0 et $m - 1$.
- (3) Il existe une suite de $m \in \mathbb{N}^*$ sous-groupes de G , $\{e\} = G_m \triangleleft G_{m-1} \triangleleft \dots \triangleleft G_1 \triangleleft G_0 = G$ tels que G_k/G_{k+1} soit abélien pour tout entier k compris entre 0 et $m - 1$.

Démonstration

$$(1) \Rightarrow (2) \quad G_k = D_k(G).$$

$$(2) \Rightarrow (3) \quad \text{Trivial.}$$

$$(3) \Rightarrow (1) \quad \text{On a } D(G_k) \subset G_{k+1}.$$

Donc, on obtient par récurrence que $D^k(G) \subset G_k$ pour tout k .

5. Groupes symétriques

Définition

Soit E un ensemble non vide.

On appelle permutation de E toute bijection de E et on note $S(E)$ l'ensemble des permutations de E .

En particulier, S_n est l'ensemble des permutations de $\mathbb{N}_n^* = \{1, 2, \dots, n\}$ où $n \geq 1$.

Rappel

$\text{Card}(S_n) = n!$.

Propriété

Pour tout ensemble non vide E , $(S(E), \circ)$ est un groupe.

Démonstration

En effet,

- La composée de deux bijections est une bijection.
- La loi \circ est associative.
- Id_E est bijective.
- Toute application bijective ρ admet une réciproque ρ^{-1} qui vérifie $\rho \circ \rho^{-1} = \rho^{-1} \circ \rho = \text{Id}_E$.

Remarques

- Le groupe $(S(E), \circ)$ est appelé groupe symétrique (ou groupe des permutations). En particulier, (S_n, \circ) est appelé groupe symétrique d'ordre n ou de degré n .
- De plus, si deux ensembles E et E' sont équipotents et si φ est une bijection de E dans E' , alors, l'application qui, à toute bijection σ de E , associe l'application $\varphi \circ \sigma \circ \varphi^{-1}$ est un isomorphisme de groupes de $S(E)$ dans $S(E')$. Cette dernière remarque permet de ramener l'étude du groupe des permutations d'un ensemble fini E à celle de S_n où n est le cardinal de E .

Notation

Soit l'application $\varphi : \{1, 2, 3, 4, 5, 6\} \rightarrow \{1, 2, 3, 4, 5, 6\}$

définie par : $\varphi(1) = 5, \varphi(2) = 2, \varphi(3) = 1, \varphi(4) = 6, \varphi(5) = 3$ et $\varphi(6) = 4$.

On peut représenter φ des façons suivantes :

- $\varphi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 5 & 2 & 1 & 6 & 3 & 4 \end{pmatrix}$.
- $\varphi = (1\ 5\ 3)(2)(4\ 6)$: on dit que l'on a décomposé la permutation en cycles.

Remarques

- L'objet $(1\ 5\ 3)$ est le même que $(5\ 3\ 1)$.
- Soit $\varphi = (1\ 5\ 3)(2)(4\ 6)$ et $\tau = (1\ 6\ 3\ 4)(2\ 5)$.
On a $\varphi \circ \tau = (1\ 4\ 5\ 2\ 3\ 6)$.
- On note aussi $\varphi \tau$ pour $\varphi \circ \tau$ et l'on parle de produit à la place de composition.
Mais attention, ce produit n'est pas en général commutatif.

Définition

Soient $n \in \mathbb{N}^*$, $\rho \in S_n$ et $k \in \mathbb{N}_n^*$.

On appelle orbite de k pour ρ et on note $\text{Orb}_\rho(k)$, $\text{Orb}(k)$ ou simplement $O_\rho(k)$ l'ensemble $\{\rho^p(k) / p \in \mathbb{N}\}$ avec la convention $\rho^0 = \text{Id}$.

Exemple

Soit $\varphi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 5 & 2 & 1 & 6 & 3 & 4 \end{pmatrix} \in S_6$.

On a : $\text{Orb}(1) = \{1, 3, 5\} = \text{Orb}(3) = \text{Orb}(5)$,

$\text{Orb}(2) = \{2\}$ et

$\text{Orb}(4) = \{4, 6\} = \text{Orb}(6)$.

Propriété

Soient $n \in \mathbb{N}^*$, $\rho \in S_n$ et $k \in \mathbb{N}_n^*$.

On a $\text{Orb}(k) = \{\rho^p(k) / p \in \mathbb{N}_{n-1}\}$.

Remarque

Cela signifie qu'il suffit de calculer un nombre fini de $\rho^p(k)$ pour avoir $\text{Orb}(k)$.

Ce nombre est au maximum n (de 0 à $n-1$), mais ce n'est pas forcément n (voir exemple précédent).

Démonstration

Soit l'ensemble $P = \{\rho^s(k) / s \in \mathbb{N}_{n-1}\} = \{k, \rho(k), \rho^2(k), \dots, \rho^{n-1}(k)\}$. P est un sous-ensemble de \mathbb{N}_n^* .

• Si P contient n éléments différents, alors $P = \mathbb{N}_n^*$ et $\forall r > n-1$, $\rho^r(k) \in P$.

• Si P contient au plus $n-1$ éléments différents.

Donc au moins deux éléments parmi $\{k, \rho(k), \rho^2(k), \dots, \rho^{n-1}(k)\}$ sont égaux.

Soit i le plus petit indice tel que $\rho^i(k)$ apparaisse deux fois dans $\{k, \rho(k), \rho^2(k), \dots, \rho^{n-1}(k)\}$.

Soit j le plus petit indice différent de i tel que $\rho^i(k) = \rho^j(k)$.

On a obligatoirement $i = 0$ car sinon $\rho^{i-1}(k) = (\rho^{-1} \circ \rho^i)(k) = (\rho^{-1} \circ \rho^j)(k) = \rho^{j-1}(k)$: ce qui est contraire aux hypothèses. D'où $\rho^i(k) = k$.

Pour tout entier r , on a $r = pj + q$ avec $0 \leq q < j$ et donc $\rho^r(k) = \rho^{pj+q}(k) = \rho^q(k) \circ \rho^{pj}(k) = \rho^q(k)$.

Remarque

Avec les notations de la démonstration, on a donc $\text{Orb}_\rho(k) = \{\rho^s(k) / 0 \leq s < j\}$.

Propriété

Soient $n \in \mathbb{N}^*$ et $\rho \in S_n$.

La relation \mathcal{R}_ρ définie sur \mathbb{N}_n^* par $x \mathcal{R}_\rho y \Leftrightarrow y \in \text{Orb}_\rho(x)$ est une relation d'équivalence.

Démonstration

$\forall x \in \mathbb{N}_n^*$, $x = \rho^0(x)$ donc $x \mathcal{R}_\rho x$.

$\forall x, y \in \mathbb{N}_n^*$, soit i le plus petit entier non nul tel que $x = \rho^i(x)$.

$x \mathcal{R}_\rho y \Rightarrow y \in \text{Orb}_\rho(x)$
 \Rightarrow il existe un entier $r \leq i$ tel que $y = \rho^r(x)$.
 \Rightarrow il existe un entier $r \leq i$ tel que $\rho^{i-r}(y) = \rho^{i-r}(\rho^r(x))$.
 \Rightarrow il existe un entier $r \leq i$ tel que $\rho^{i-r}(y) = \rho^i(x) = x$.
 $\Rightarrow x \in \text{Orb}_\rho(y) \Rightarrow y \mathcal{R}_\rho x$.

Soit $x, y, z \in \mathbb{N}_n^*$.
 $x \mathcal{R}_\rho y \Rightarrow y \in \text{Orb}_\rho(x) \Rightarrow$ il existe un entier r tel que $y = \rho^r(x)$.
 $y \mathcal{R}_\rho z \Rightarrow z \in \text{Orb}_\rho(y) \Rightarrow$ il existe un entier s tel que $z = \rho^s(y)$.
 On a $z = \rho^s(y) = \rho^s(\rho^r(x)) = \rho^{s+r}(x)$.

Remarques

- Soit A une orbite d'une permutation σ de S_n ($n \in \mathbb{N}^*$).
On a $\sigma(A) = A$ et la restriction de σ à A est une permutation de A .
Pour tout x de A , on a $A = \text{Orb}_\sigma(x)$.
- Soit A une orbite non réduite à un élément d'une permutation σ de S_n ($n \in \mathbb{N}^*$).
Alors $\sigma(x) \neq x$ pour tout x de A .
En effet, si $\sigma(x) = x$, alors $\text{Orb}_\sigma(x) = \{\sigma^p(x) / p \in \mathbb{N}\} = \{x\} = A$ ce qui contredit aux hypothèses.
Plus précisément, on a $A = \{x, \sigma(x), \sigma^2(x), \dots, \sigma^{p-1}(x)\}$ où p est le cardinal de A .

Définition

Soit $n \in \mathbb{N}^*$.
 Une permutation de S_n est appelée un cycle si et seulement si elle ne possède qu'une seule orbite non réduite à un élément.

Exemple

Soit $\varphi = (1) (5 \ 3 \ 2 \ 6) (4) (7) (8) \in S_8$. φ est un cycle que l'on peut noter simplement $\varphi = (5 \ 3 \ 2 \ 6)$.

Remarques

- On peut aussi considérer un cycle comme la restriction d'une permutation donnée à une orbite.
- Le nombre p d'éléments du cycle $\gamma = (a_1 \ a_2 \ \dots \ a_p)$ est appelé la longueur de γ et $\{a_1 \ a_2 \ \dots \ a_p\}$ est appelé l'orbite de γ . On dit aussi que γ est un p -cycle.

Propriété

Un cycle de longueur p est d'ordre p c'est-à-dire $\gamma^p = \text{Id}$.

Propriété

Soient φ et σ deux cycles de S_n ($n \in \mathbb{N}^*$) de même longueur p .
 Alors il existe une permutation u de S_n telle que $\varphi = u \circ \sigma \circ u^{-1}$. On dit que φ et σ sont conjugués.

Démonstration

On suppose que $\varphi = (a_1 \ a_2 \ \dots \ a_p)$ et $\sigma = (b_1 \ b_2 \ \dots \ b_p)$.
 Puisque $\text{card}\{b_1 \ b_2 \ \dots \ b_p\} = \text{card}\{a_1 \ a_2 \ \dots \ a_p\}$, il existe une bijection de $\{b_1 \ b_2 \ \dots \ b_p\}$ dans $\{a_1 \ a_2 \ \dots \ a_p\}$

Considérons une extension de cette bijection :

Soit $u : \mathbb{N}_n^* \rightarrow \mathbb{N}_n^*$

$$b_i \mapsto a_i$$

$$x \mapsto x \text{ si } x \notin \{b_1, b_2, \dots, b_p\}$$

Si $i \neq p$, $(u \circ \sigma \circ u^{-1})(a_i) = u(\sigma[u^{-1}(a_i)]) = u[\sigma(b_i)] = u[b_{i+1}] = a_{i+1} = \varphi(a_i)$.

Si $i = p$, $(u \circ \sigma \circ u^{-1})(a_p) = u(\sigma[u^{-1}(a_p)]) = u[\sigma(b_p)] = u[b_1] = a_1 = \varphi(a_p)$.

Et $(u \circ \sigma \circ u^{-1})(x) = x$ si $x \notin \{b_1, b_2, \dots, b_p\}$.

Définition

Soit $n \in \mathbb{N}^*$ et soient $i, j \in \mathbb{N}_n^*$.

On appelle transposition de i et de j et on note $\tau_{i,j}$ la permutation de S_n définie par : $\tau_{i,j}(i) = j$, $\tau_{i,j}(j) = i$ et $\tau_{i,j}(k) = k$ pour tout $k \in \mathbb{N}_n^*$ tel que $k \neq i$ et $k \neq j$.

Remarques

- Une transposition est un cycle de longueur 2. On peut noter $\tau_{i,j} = (i j)$.
- Une transposition est une involution i.e. $\tau_{i,j} \circ \tau_{i,j} = \text{Id}$.

Propriété

Soient $n, p \in \mathbb{N}^*$ avec $p \leq n$. Soient $a_1, a_2, \dots, a_p \in \mathbb{N}_n^*$ deux à deux différents.

On a $(a_1 a_2 a_3 a_4 \dots a_p) = (a_1 a_2) (a_2 a_3) (a_3 a_4) \dots (a_{p-1} a_p)$.

Exemple

Cela donne, par exemple, $(1 2) (2 3) = (1 2 3)$

Démonstration

Soit $\varphi = (a_1 a_2) (a_2 a_3) (a_3 a_4) \dots (a_{p-1} a_p)$.

On a $\varphi(a_p) = a_1$ et $\varphi(a_i) = a_{i+1}$ pour tout $1 \leq i \leq p-1$.

Définition

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

On appelle permutation circulaire de S_n toute permutation (de S_n) qui ne possède qu'une seule orbite.

Exemple

Dans S_4 , $\varphi = (1 3 4 2)$ est une permutation circulaire.

Remarque

Si $n \geq 2$, une permutation circulaire de S_n est un cycle de longueur n .

Propriété

La composition (le produit) de cycles disjoints (c'est-à-dire dont l'intersection des orbites est vide) est commutative.

Remarques

- Un cycle n'intervenant que sur une seule orbite, deux cycles disjoints n'agissent que sur des entiers différents.
Par exemple, $(1\ 3\ 4)(2\ 5) = (2\ 5)(1\ 3\ 4)$.
- Mais un produit de cycles non disjoints n'est pas commutatif.
En effet, si par exemple $\rho_1 = (1\ 2)$ et $\rho_2 = (2\ 3)$, on a $\rho_1 \circ \rho_2 = (1\ 2\ 3)$ et $\rho_2 \circ \rho_1 = (1\ 3\ 2)$.

Propriété

Toute permutation se décompose en une composition (un produit) de cycles disjoints et cette décomposition est unique à l'ordre près des cycles.

Remarque

On obtient simplement cette décomposition en considérant les cycles sur les différentes orbites en ne conservant que celles non réduites à un élément.

Exemple

Soit l'application $\varphi : \{1, 2, 3, 4, 5, 6, 7, 8\} \rightarrow \{1, 2, 3, 4, 5, 6, 7, 8\}$ définie par :
 $\varphi(1) = 5, \varphi(2) = 7, \varphi(3) = 6, \varphi(4) = 4, \varphi(5) = 8, \varphi(6) = 3, \varphi(7) = 2$ et $\varphi(8) = 1$.
On a $\varphi = (1\ 5\ 8)(2\ 7)(3\ 6)$.

Propriété

Pour tout entier $n \geq 2$, S_n est engendré par ses transpositions.

Remarques

- Cela signifie que toute permutation peut s'exprimer comme une composition (un produit) de transpositions.
- Cette décomposition n'est pas unique.

Exemples

- Soit $\rho = (1\ 3\ 4)(2\ 3)$. On a $\rho = (1\ 3)(3\ 4)(2\ 3)$.
- Soit $\rho = (1\ 2\ 3)$.
On a $\rho = (1\ 2)(2\ 3)$. Mais aussi $\rho = (1\ 3)(1\ 2)$.

Démonstration 1

On raisonne par récurrence sur le nombre n de S_n .

- Si $n = 2$, $S_2 = \{\text{Id}, \tau_{1,2}\}$ avec $\text{Id} = \tau_{1,2} \circ \tau_{1,2}$.
- On suppose la propriété vraie au rang $n - 1$ et soit $\rho \in S_n$.
Si $\rho(n) = n$ alors la restriction de ρ à $\{1, 2, \dots, n - 1\}$ appartient à S_{n-1} et ρ en a la même décomposition en transpositions.
Si $\rho(n) = m \neq n$, alors $\tau_{n,m} \circ \rho$ est une permutation de S_n qui vérifie $(\tau_{n,m} \circ \rho)(n) = n$.
Nous sommes donc dans le cas précédent et $\rho = \tau_{n,m} \circ (\tau_{n,m} \circ \rho)$ avec $\tau_{n,m} \circ \rho$ qui peut se décomposer en produit de transpositions.

Démonstration 2

Cela découle directement du fait que tout cycle peut se décomposer en un produit de transpositions.

Propriété

Soit $n \in \mathbb{N}^*$ et soient $i, j \in \mathbb{N}_n^*$.

Si $j > i$, alors $\tau_{i,j} = \tau_{i,i+1} \circ \tau_{i+1,i+2} \circ \dots \circ \tau_{j-2,j-1} \circ \tau_{j-1,j} \circ \tau_{j-2,j-1} \circ \dots \circ \tau_{i+1,i+2} \circ \tau_{i,i+1}$.

Démonstration

Si $\rho = (i \ i+1) (i+1 \ i+2) \dots (j-2 \ j-1) (j-1 \ j) (j-2 \ j-1) \dots (i+1 \ i+2) (i \ i+1)$, on a :
 $\rho(i) = j$, $\rho(j) = i$ et $\rho(k) = k$ pour tout $i < k < j$ (car k apparaît dans 2 transpositions).

Corollaire

Pour tout entier $n \geq 2$, S_n est engendré par les transpositions du type $\tau_{i, i+1}$ où $1 \leq i \leq n-1$.

Remarque

Le nombre de transpositions d'une décomposition d'une permutation peut varier. Mais nous allons voir que la parité de ce nombre reste la même.

Définition

Soit $n \in \mathbb{N}^*$ et soient $i, j \in \mathbb{N}_n^*$.

On dit que le couple (i, j) présente une inversion pour une permutation ρ de S_n si $i < j$ et $\rho(i) > \rho(j)$.

Exemple

Soit $\rho = (1 \ 4 \ 2)$ dans S_4 . On doit étudier le signe de $\rho(j) - \rho(i)$:

i	j	$\rho(j) - \rho(i)$
1	2	-3
1	3	-1
1	4	-2
2	3	2
2	4	1
3	4	-1

Il y a en tout C_4^2 couples (i, j) possibles. Quatre couples présentent une inversion.

Remarque

Soit $n \in \mathbb{N}^*$. Il y a C_n^2 couples (i, j) tels que $i, j \in \mathbb{N}_n^*$ et $i < j$. Le produit $p = \prod_{i < j} (j - i)$ est un entier positif.

Soit $\varphi \in S_n$, on s'intéresse à $p' = \prod_{i < j} (\varphi(j) - \varphi(i))$.

Si l'on reprend l'exemple précédent, $\rho = (1 \ 4 \ 2)$ dans S_4 , on a :

$$p = (2-1)(3-1)(4-1)(3-2)(4-2)(4-3) = (1)(2)(3)(1)(2)(1) \text{ et}$$

$$p' = (-3)(-1)(-2)(2)(1)(-1).$$

On remarque que p' et p ne peuvent différer que par le signe. Le nombre de soustractions qui changent de signe est égale au nombre d'inversions.

Définition

Soit $n \in \mathbb{N}^*$ et soit $\varphi \in S_n$.

On appelle signature de φ et on note $\sigma(\varphi)$ le nombre $\sigma(\varphi) = \frac{\prod_{i < j} \varphi(j) - \varphi(i)}{\prod_{i < j} (j - i)}$.

Si $\sigma(\varphi) > 0$, on dit que φ est paire.

Si $\sigma(\varphi) < 0$, on dit que φ est impaire.

Exemple

Toujours avec le même exemple, $\rho = (1\ 4\ 2)$ dans S_4 , on a $\sigma(\rho) = 1$.

Propriété

Soit l le nombre d'inversions d'une permutation φ de S_n où $n \geq 2$.

On a $\sigma(\varphi) = (-1)^l$ et donc $\prod_{i < j} (\varphi(j) - \varphi(i)) = (-1)^l \prod_{i < j} (j - i)$.

Remarque

$$\prod_{i \neq j} (\varphi(j) - \varphi(i)) = (-1)^l \prod_{i \neq j} (j - i).$$

Démonstration

Soit $\varphi \in S_n$.

On a $\varphi(\mathbb{N}_n^*) = \mathbb{N}_n^*$.

D'où $\prod_{i, j \in \{1, \dots, n\}} (\varphi(j) - \varphi(i)) = \prod_{a, b \in \{1, \dots, n\}} (b - a)$ et donc $\prod_{i < j} (|\varphi(j) - \varphi(i)|) = \prod_{i < j} (j - i)$.

Etant donné que $j - i$ est positif et que seuls les couples présentant une inversion sont tels que $\varphi(j) - \varphi(i) < 0$, le signe de $\prod_{i < j} (\varphi(j) - \varphi(i))$ dépend du nombre d'inversions de φ .

Remarques

- La parité d'une permutation est donc égale à la parité du nombre total d'inversions qu'elle produit.
- La signature d'une transposition est -1 .

Exemple

Avec $\rho = (1\ 4\ 2)$ dans S_4 , on a $\sigma(\rho) = (-1)^4$ et ρ paire.

Propriété

La signature est un morphisme de groupe de (S_n, \circ) dans $(\{-1, 1\}, \times)$ c'est-à-dire :

$\forall f, g \in S_n$, on a $\sigma(f \circ g) = \sigma(f) \times \sigma(g)$.

Démonstration

On a $\prod_{i < j} ((f \circ g)(j) - (f \circ g)(i)) = \sigma(f \circ g) \prod_{i < j} (j - i)$.

Or $\prod_{i < j} (f[g(j)] - f[g(i)]) = \sigma(f) \prod_{i < j} (g(j) - g(i)) = \sigma(f) \sigma(g) \prod_{i < j} (j - i)$.

Remarque

Le noyau de ce morphisme (c'est-à-dire l'ensemble des permutations de S_n de signature 1) est appelé groupe alterné d'ordre n et on le note A_n .

Les éléments de A_n sont appelés les permutations paires et ceux de $S_n \setminus A_n$ les permutations impaires.

Corollaire

Soit m le nombre de transpositions dans une décomposition quelconque d'une permutation φ de S_n où $n \geq 2$. On a $\sigma(\varphi) = (-1)^m$.

Remarque

Ce dernier corollaire donne une méthode plus rapide que les précédentes pour déterminer la signature d'une permutation.

Par exemple, si $\varphi = (1\ 2\ 6)(4\ 5)$ dans S_6 , on a $\varphi = (1\ 2)(2\ 6)(4\ 5)$ et $\sigma(\varphi) = -1$.

Propriété

Soit φ une permutation de S_n et m son nombre d'orbites.

On a $\sigma(\varphi) = (-1)^{n-m}$.

6. Groupes opérant sur un ensemble

Définition

Soit (G, \times) un groupe d'élément neutre 1 et E un ensemble.

- On dit que G opère sur E si et seulement si il existe un morphisme de groupes φ de G dans $S(E)$.
- On dit que G opère fidèlement sur E ou que G est un groupe de permutations de E si et seulement si $\text{Ker } \varphi = \{1\}$.
- Si $\text{card } E = n$, on dit que G est un groupe de degré n .

Notation

Si G opère sur E et si φ est un morphisme de G dans $S(E)$, pour tout g de G et pour x de E , on note $g.x$ l'élément de E défini par $\varphi(g)(x)$.

Propriété

Soit (G, \times) un groupe d'élément neutre 1.

On dit que G opère sur un ensemble E si et seulement si il existe une application de $G \times E$ dans E dont l'image du couple (g, x) est notée $g.x$ telle que :

- i) $1.x = x \quad \forall x \in E$
- ii) $a.(b.x) = (ab).x \quad \forall x \in E, \forall a, b \in G$

Démonstration

(\Rightarrow) Trivial car $\varphi(1) = \text{Id}$.

- (\Leftarrow) Pour tout g de G , soit $\sigma_g : x \mapsto g.x$ et soit $\varphi : g \mapsto \sigma_g$
- # σ_g est une bijection. En effet, l'application $x \mapsto g^{-1}.x$ est la réciproque de σ_g car, $\forall x \in E$, $(\sigma_{g^{-1}} \circ \sigma_g)(x) = \sigma_{g^{-1}}(\sigma_g(x)) = \sigma_{g^{-1}}(g.x) = g^{-1}(g.x) = (g^{-1}g).x = 1.x = x$.
 φ est donc une application de G dans $S(E)$.
 - # φ est un morphisme.
 En effet, $\forall x \in E, \forall a, b \in G, \sigma_{ab}(x) = (ab).x = a.(b.x) = a.(\sigma_b(x)) = \sigma_a(\sigma_b(x))$.
 C'est-à-dire, $\sigma_{ab} = \sigma_a \circ \sigma_b$ ou encore $\varphi(ab) = \varphi(a) \circ \varphi(b)$.

Remarques

- Si G opère sur un ensemble E , on a : $x = y \Leftrightarrow a.x = a.y \quad \forall x, y \in E, \forall a \in G$.
 Autrement dit, tout élément de G est simplifiable pour la loi externe.
- Si G opère sur un ensemble E , nous appellerons noyau de l'application de $(g, x) \mapsto g.x$ le noyau du morphisme de groupes (de G dans $S(E)$) associé c'est-à-dire l'ensemble des éléments a de G tels que $a.x = x \quad \forall x \in E$.

Exemples

- Soit E est un ensemble.
 $S(E)$ et tous ses sous-groupes opèrent sur E .
- Si G est un groupe, G opère sur lui-même par la translation à gauche :
 $\forall g \in G, \forall x \in G, g.x = gx$.
- Si G est un groupe, G opère sur lui-même par la translation à droite :
 $\forall g \in G, \forall x \in G, g.x = xg^{-1}$.
- Si G est un groupe, G opère sur lui-même par automorphisme intérieur :
 $\forall g \in G, \forall x \in G, g.x = gxg^{-1}$
 Soit $\sigma_g : x \mapsto gxg^{-1}$ et soit $\varphi : g \mapsto \sigma_g$.
 Le noyau de l'application φ est le centre de G c'est-à-dire
 $\text{Ker } \varphi = Z(G) = \{g \in G / \forall x \in G, gxg^{-1} = x\} = \{g \in G / \forall x \in G, gx = xg\}$.
- Si G opère sur un ensemble E , on peut faire opérer G de manière canonique sur $\mathcal{P}(E)$:
 $g.X = \{g.x / x \in X\}$
- Si G opère sur un ensemble E , on peut faire opérer G de manière canonique sur $E \times E$:
 $g.(a, b) = (g.a, g.b)$
- Si G opère sur un ensemble E et F est un ensemble, on peut faire opérer G de manière canonique sur $F^E = \{f : E \rightarrow F\}$ avec l'opérateur $(g.f)(x) = f(g^{-1}.x)$.

Définitions

Soit G un groupe qui opère sur un ensemble E et soit F un sous ensemble de E .

On appelle fixateur de F l'ensemble $G_F = \{g \in G / \forall x \in F, g.x = x\}$.

On dit que F est invariant par G si $G_F = G$.

On appelle stabilisateur de F l'ensemble $G(F) = \{g \in G / g.F = F\}$.

On dit que F est stable par G si $G(F) = G$.

Remarques

- Si $F = \{x\}$, on a alors $G_F = G(F)$. Le stabilisateur (ou fixateur) de F est alors noté G_x et est aussi appelé groupe d'isotropie de x dans G .
- Si G opère sur lui-même par automorphismes intérieurs et si $F = \{x\}$, alors G_x est l'ensemble des éléments de G qui commutent avec x .

Propriété

Soit G un groupe qui opère sur un ensemble E .

Soit F un sous ensemble de E .

G_F et $G(F)$ sont des sous-groupes de G .

Démonstration

- # $\forall x \in F, 1.x = x$ donc $1 \in G_F$.
- # $\forall a, b \in G_F, \forall x \in F, (ab).x = a.(b.x) = a.x = x$ donc $ab \in G_F$.
- # $\forall a \in G_F, \forall x \in F, x = 1.x = (a^{-1}a).x = a^{-1}.(a.x) = a^{-1}.x$ donc $a^{-1} \in G_F$.
- # $\forall x \in F, 1.F = F$ donc $1 \in G(F)$.
- # $\forall a, b \in G(F), (ab).F = a.(b.F) = a.F = F$ donc $ab \in G(F)$.
- # $\forall a \in G(F), \forall x \in F, a^{-1}.F = a^{-1}.(a.F) = (a^{-1}a).F = 1.F = F$ et donc $a^{-1} \in G(F)$.

Propriété

Soit G un groupe qui opère sur un ensemble E et soit F un sous ensemble de E .

$G_F \triangleleft G(F)$ et $G(F)/G_F$ est isomorphe à un sous-groupe de $S(F)$.

Démonstration

Puisque $G(F)$ est un sous-groupe de G , $G(F)$ opère sur F .

Donc il existe un morphisme $\psi : G(F) \rightarrow S(F)$.

$\text{Ker } \psi = \{g \in G(F) / \psi(g) = \text{Id}_F\} = G_F$.

Propriété

Soit G un groupe qui opère sur un ensemble E et soit x un élément de E .

Alors, pour tout élément g de G , on a $G_{g.x} = gG_xg^{-1}$.

Démonstration

$$\begin{aligned} h \in G_{g.x} &\Leftrightarrow h.(g.x) = g.x \\ &\Leftrightarrow (hg).x = g.x \\ &\Leftrightarrow g^{-1}.[(hg).x] = g^{-1}.(g.x) \\ &\Leftrightarrow (g^{-1}hg).x = x \\ &\Leftrightarrow g^{-1}hg \in G_x \\ &\Leftrightarrow h \in gG_xg^{-1}. \end{aligned}$$

Remarque

Cela signifie que les sous-groupes d'isotropies de deux éléments d'une même orbite sont conjugués.

Définitions

Soit G un groupe et K un sous-groupe de G .

G opère sur lui-même par automorphisme intérieur : $\forall g \in G, \forall x \in G, g.x = gxg^{-1}$.

Le fixateur de K dans G est appelé centralisateur de K dans G et est noté $C_G(K)$.

Le stabilisateur de K dans G est appelé normalisateur de K dans G et est noté $N_G(K)$.

Remarque

Autrement dit $C_G(K) = \{g \in G / gkg^{-1} = k \ \forall k \in K\}$ et $N_G(K) = \{g \in G / gKg^{-1} = K\}$.
On a $K \triangleleft N_G(K)$.

Corollaire

Soit G un groupe et K un sous-groupe de G .

$C_G(K) \triangleleft N_G(K)$ et $N_G(K)/C_G(K)$ est isomorphe à un sous-groupe de $\text{Aut}(K)$.

Propriété

Soit G un groupe qui opère sur un ensemble E .

La relation \mathcal{R}^G définie sur E par $x \mathcal{R}^G y \Leftrightarrow \exists g \in G / y = g.x$ est une relation d'équivalence.

Démonstration

- # $\forall x \in E, 1.x = x$ donc $x \mathcal{R}^G x$.
- # $\forall x, y \in E, x \mathcal{R}^G y \Leftrightarrow \exists g \in G / y = g.x$
 $\Rightarrow x = g^{-1}.y$
 $\Rightarrow y \mathcal{R}^G x$.
- # $\forall x, y, z \in E, x \mathcal{R}^G y \Leftrightarrow \exists g \in G / y = g.x$
 $y \mathcal{R}^G z \Leftrightarrow \exists g' \in G / z = g'.y$
 $\Rightarrow z = g'.(g.x)$
 $\Rightarrow z = (g'g).x$
 $\Rightarrow x \mathcal{R}^G z$.

Définition

Soit G un groupe qui opère sur un ensemble E et soit x un élément de E .

On appelle orbite de x suivant G la classe d'équivalence de x suivant \mathcal{R}^G .

Deux éléments d'une même orbite sont dits conjugués.

On dit que G opère transitivement (ou que G est transitif) sur E si et seulement si il n'y a qu'une seule orbite c'est-à-dire, $\forall x, y \in E, \exists g \in G / y = g.x$.

On dit aussi que E est un G -espace homogène.

Remarque

Dans le cas où G opère sur lui-même par automorphismes intérieurs, l'orbite de $x (\in G)$ suivant G est aussi appelée classe de conjugaison de x dans G .

En effet, cet orbite est composé des conjugués de x dans G .

Propriété

Si G est un groupe et si H est un sous-groupe de G , alors G opère transitivement sur $(G/H)_g$ par :

$$\forall g \in G, \forall x \in G, g.xH = (gx)H.$$

Le noyau en est $\bigcap_{x \in G} xHx^{-1}$.

Démonstration

- # On a bien $\forall x \in G, 1.xH = (1x)H = xH$.
- # $\forall x \in G, \forall a, b \in G, a.(b.xH) = a.(bx)H$
 $= (a(bx))H$
 $= ((ab)x)H$
 $= (ab).xH$
- $\forall xH, yH \in (G/H)_d$, on pose $g = yx^{-1}$.
 On a $g.xH = (gx)H$
 $= (yx^{-1}x)H$
 $= yH$.
- Soit $g \in G$ tel que, $\forall x \in G, g.xH = xH$.
 On a donc : $(gx)H = xH \quad \forall x \in G$
 $\Leftrightarrow x^{-1}gx \in H \quad \forall x \in G$
 $\Leftrightarrow g \in xHx^{-1} \quad \forall x \in G$
 $\Leftrightarrow g \in \bigcap_{x \in G} xHx^{-1}$.

Propriété

Soit G un groupe qui opère sur un ensemble E et soit x un élément de E .
 L'orbite $G.x$ est finie si et seulement si le groupe G_x est d'indice fini dans G .
 Dans ce cas, $\text{card}(G.x) = (G : G_x)$.

Démonstration

On considère l'application $\varphi : G \rightarrow G.x$
 $g \mapsto g.x$

Soit \mathcal{R} la relation d'équivalence définie sur G par : $a \mathcal{R} b \Leftrightarrow a^{-1}b \in G_x$.

Nous avons vu que la classe de a selon \mathcal{R} est aG_x .

On note $(G/G_x)_g$ l'ensemble quotient selon \mathcal{R} .

Soient g_1, g_2 deux éléments de G .

$$\begin{aligned} \varphi(g_1) = \varphi(g_2) &\Leftrightarrow g_1.x = g_2.x \\ &\Leftrightarrow g_2^{-1}g_1.x = x \\ &\Leftrightarrow g_2^{-1}g_1 \in G_x \end{aligned}$$

Donc les ensembles $G.x$ et $(G/G_x)_g$ sont équipotents.

Remarque

Puisqu'un groupe G opère sur lui-même par automorphisme intérieur, le nombre des conjugués d'un élément x de G est égale à $(G : G_x)$.

De plus, si G est fini, ce nombre est un diviseur de $\text{card}(G)$.

Corollaire

Soit G un groupe qui opère sur un ensemble fini E .

On suppose que x_1, x_2, \dots, x_p sont des éléments de E tels que les G_{x_1}, \dots, G_{x_p} soient les G -orbites deux à deux distinctes de G dans E .

Alors $\text{card} E = \text{card}(G.x_1) + \text{card}(G.x_2) + \dots + \text{card}(G.x_p) = (G : G_{x_1}) + (G : G_{x_2}) + \dots + (G : G_{x_p})$.

Propriété

Soit n un entier non nul et p un nombre premier.
Si G un groupe fini de cardinal p^n , alors $Z(G) \neq \{e\}$.

Démonstration

On peut faire opérer G sur lui-même par conjugaison (automorphisme intérieur).

Pour tout x de G , on a $x \in Z(G) \Leftrightarrow G.x = \{x\} \Leftrightarrow G = G_x \Leftrightarrow (G : G_x) = 1$.

Soient x_1, x_2, \dots, x_m les éléments de G tels que les $G_{x_1}, G_{x_2}, \dots, G_{x_m}$ soient les G -orbites non réduite à un point et deux à deux distinctes.

Alors $\text{card } G = \text{card } Z(G) + (G : G_{x_1}) + (G : G_{x_2}) + \dots + (G : G_{x_m})$.

Tous les $(G : G_{x_i})$ sont des puissances de p différentes de 1.

Si $\text{card } Z(G) = 1$, p divise 1 : absurde.

Théorème

Tout groupe est isomorphe à un groupe de permutation.

Démonstration

Pour tout élément a de G , la translation à gauche $\sigma_a : x \mapsto ax$ est une bijection de G et l'application $a \mapsto \sigma_a$ de G dans $S(G)$ est un morphisme injectif.

Définition

Soit G un groupe qui opère sur un ensemble E et soit m un entier non nul.

On dit que G opère m -transitivement sur E (ou que G opère m -fois transitivement sur E ou que G est m -transitif sur E) si et seulement si, pour tout couple de m -uplets d'éléments différents de E (x_1, x_2, \dots, x_m) et (y_1, y_2, \dots, y_m) , il existe $g \in G$ tel que $y_i = g.x_i$ pour tout i compris entre 1 et m .

Propriété

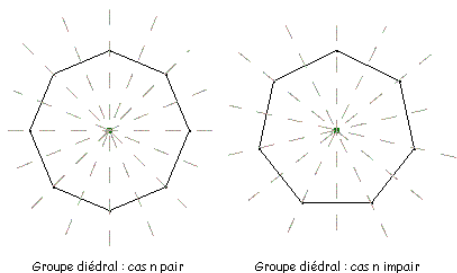
Pour tout entier $n \geq 3$, le groupe A_n opère $(n - 2)$ -transitivement sur \mathbb{N}_n^* mais pas $(n - 1)$ -transitivement.

Démonstration

- Posons $\mathbb{N}_n^* = \{a_1, a_2, \dots, a_n\} = \{b_1, b_2, \dots, b_n\}$.
Sans perte de généralité, on peut considérer les sous-ensembles $\{a_1, a_2, \dots, a_{n-2}\}$ et $\{b_1, b_2, \dots, b_{n-2}\}$.
Soit φ la permutation de S_n telle que $\varphi(a_i) = b_i$ pour tout entier i compris entre 1 et $n - 2$.
Soit τ la transposition $(b_{n-1} b_n)$.
Si φ est paire (i.e. $\varphi \in A_n$), on obtient le résultat. Sinon $\varphi \circ \tau$ est paire et vérifie bien $(\varphi \circ \tau)(a_i) = b_i$ pour tout entier i compris entre 1 et $n - 2$.
- Posons $a_i = b_i = i$ pour tout entier i compris entre 1 et $n - 2$.
De plus, on suppose que $a_{n-1} = b_{n-2} = n - 1$ et que $a_{n-2} = b_{n-1} = n - 2$.
La seule permutation σ de \mathbb{N}_n^* telle que $\sigma(a_i) = b_i$ pour tout entier i compris entre 1 et $n - 1$ est la transposition $(n - 1 n)$ qui est impaire.

Définition

On appelle groupe diédral d'ordre $n \geq 3$ le groupe des isométries du plan euclidien qui conservent un polygone régulier convexe à n côtés.



Propriété

Le groupe diédral d'ordre $n \geq 3$ contient $2n$ éléments :

- n rotations de centre le milieu du polygone, et d'angle $2 \times k \times \frac{\pi}{n}$ (pour k variant de 0 à $n - 1$).
- n réflexions.

Si n est pair, les axes de ces réflexions sont les droites joignant un sommet au sommet opposé, et les droites passant par les milieux de deux côtés opposés.

Si n est impair, il n'y a qu'une famille de réflexions. Leurs axes joignent un sommet au milieu du côté opposé.