Chapitre 1 : Structures algébriques - Groupes

L3-S5. Algèbre générale 1

Licence Mathématiques
Université d'Avignon

Année 2018–2019

On extrait des règles opératoires valables indépendamment des objets considérés. Plusieurs buts

- comprendre les principes qui sous-tendent les calculs classiques
- étendre ces principes à différents types d'objets
- généraliser dans diverses directions (objets abstraits, opérateurs variés).

I. Loi de composition

1. Loi de composition interne

Définition : Loi de composition interne sur un ensemble

Une *loi de composition interne* sur un ensemble E est une application de $E \times E$ sur E. On notera cette application

$$\begin{array}{ccccc} E & \times & E & \to & E \\ (x & , & y) & \mapsto & x * y \end{array}$$

On parle alors de la loi $*$. On note souvent $(E, *)$ pour désigner un ensemble E muni d'une loi de composition $*$.

Le symbole désignant la loi peut être noté $\top$, $\diamondsuit$, $\clubsuit$ ...

I. Loi de composition

1. Loi de composition interne

Définition : Loi de composition interne sur un ensemble

Une *loi de composition interne* sur un ensemble E est une application de $E \times E$ sur E. On notera cette application

$$\begin{array}{ccccc} E & \times & E & \to & E \\ (x & , & y) & \mapsto & x * y \end{array}$$

On parle alors de la loi $*$. On note souvent $(E, *)$ pour désigner un ensemble E muni d'une loi de composition $*$.

Le symbole désignant la loi peut être noté $\top$, $\diamondsuit$, $\clubsuit$ ...
Exemples incontournables de lois :

- addition $+$, multiplication $\times$ dans $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ ou $\mathbb{C}$
- composition $\circ$ dans l'ensemble des permutations dans E

Définition

Soit $*$ une loi de composition sur un ensemble E.

1. **Associativité d'une loi de composition** :
   On dit que la loi $*$ est *associative* si, pour tous x, y, z de E, on a : $(x * y) * z = x * (y * z)$. On écrit alors $x * y * z$.

Définition

Soit $*$ une loi de composition sur un ensemble E.

1. **Associativité d'une loi de composition** :
   On dit que la loi $*$ est *associative* si, pour tous x, y, z de E, on a : $(x * y) * z = x * (y * z)$. On écrit alors $x * y * z$.
2. **Eléments qui commutent pour une loi** :
   Soit x et y deux éléments de E. On dit que x et y *commutent* (pour la loi $*$) si $x * y = y * x$.

Définition

Soit $*$ une loi de composition sur un ensemble E.

1. **Associativité d'une loi de composition** :
   On dit que la loi $*$ est *associative* si, pour tous x, y, z de E, on a : $(x * y) * z = x * (y * z)$. On écrit alors $x * y * z$.
2. **Eléments qui commutent pour une loi** :
   Soit x et y deux éléments de E. On dit que x et y *commutent* (pour la loi $*$) si $x * y = y * x$.
3. **Commutativité d'une loi de composition** :
   On dit que la loi $*$ est *commutative* si, pour tous x et y de E, on a $x * y = y * x$.

Avec l'associativité et la commutativité, on peut changer l'ordre des éléments et les regrouper comme on veut, ce qui permet de simplifier les calculs.

2. Exemples de lois usuelles et notations usuelles

Somme et produit sur les ensembles de nombres

Les lois $+$ et $\times$ usuelles sur $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ et $\mathbb{C}$ sont associatives et commutatives.

2. Exemples de lois usuelles et notations usuelles

Somme et produit sur les ensembles de nombres

Les lois $+$ et $\times$ usuelles sur $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ et $\mathbb{C}$ sont associatives et commutatives.

La loi produit $\times$ est le plus souvent notée xy plutôt que $x \times y$.

2. Exemples de lois usuelles et notations usuelles

Somme et produit sur les ensembles de nombres

Les lois $+$ et $\times$ usuelles sur $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ et $\mathbb{C}$ sont associatives et commutatives.

La loi produit $\times$ est le plus souvent notée xy plutôt que $x \times y$. La loi $(x, y) \mapsto x - y$ sur $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ et $\mathbb{C}$, n'est ni associative ni commutative.

2. Exemples de lois usuelles et notations usuelles

Somme et produit sur les ensembles de nombres

Les lois $+$ et $\times$ usuelles sur $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ et $\mathbb{C}$ sont associatives et commutatives.

La loi produit $\times$ est le plus souvent notée xy plutôt que $x \times y$. La loi $(x, y) \mapsto x - y$ sur $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ et $\mathbb{C}$, n'est ni associative ni commutative.

La loi de composition des applications

Soit E un ensemble et $\mathcal{F}(E)$ l'ensemble des applications de E dans E. On définit la loi $\circ$ (loi de composition) sur $\mathcal{F}(E)$ par $(f, g) \mapsto f \circ g$. Cette loi est associative, mais elle n'est pas commutative (sauf si E est réduit à un singleton).

Les lois union et intersection sur les ensembles

Soit E un ensemble et $\mathcal{P}(E)$ l'ensemble des parties de E. On définit les lois union et intersection sur $\mathcal{P}(E)$ par $(A, B) \mapsto A \cup B$ et $(A, B) \mapsto A \cap B$. Ces lois sont associatives et commutatives.

Les lois union et intersection sur les ensembles

Soit E un ensemble et $\mathcal{P}(E)$ l'ensemble des parties de E. On définit les lois union et intersection sur $\mathcal{P}(E)$ par $(A, B) \mapsto A \cup B$ et $(A, B) \mapsto A \cap B$. Ces lois sont associatives et commutatives.

Maximum et minimum sur un ensemble totalement ordonné

Soit E un ensemble muni d'une relation d'ordre total noté $\preceq$. Les lois minimum et maximum sont notées par : $\min(x, y)$ et $\max(x, y)$. Ces deux lois sont associatives et commutatives.

Définition

Une *relation d'ordre* $\preceq$ sur E est une relation binaire sur E

- *réflexive* : $\forall x \in E,\ x \preceq x$;
- *antisymétrique* : $\forall x, y \in E,\ (x \preceq y \text{ et } y \preceq x) \Rightarrow x = y$;
- *transitive* : $\forall x, y, z \in E,\ (x \preceq y \text{ et } y \preceq z) \Rightarrow x \preceq z$.

Un ensemble muni d'une relation d'ordre est dit *ordonné*. L'ordre est dit *total* si deux éléments x et y de E sont comparables ($x \preceq y$ ou $y \preceq x$). Sinon l'ordre est dit *partiel*.

Définition

Une *relation d'ordre* $\preceq$ sur E est une relation binaire sur E

- *réflexive* : $\forall x \in E,\ x \preceq x$;
- *antisymétrique* : $\forall x, y \in E,\ (x \preceq y \text{ et } y \preceq x) \Rightarrow x = y$;
- *transitive* : $\forall x, y, z \in E,\ (x \preceq y \text{ et } y \preceq z) \Rightarrow x \preceq z$.

Un ensemble muni d'une relation d'ordre est dit *ordonné*. L'ordre est dit *total* si deux éléments x et y de E sont comparables ($x \preceq y$ ou $y \preceq x$). Sinon l'ordre est dit *partiel*.

Exemples.

1. Ordre usuel sur $\mathbb{R}$: $\leqslant$
2. Divisibilité dans $\mathbb{N}^\star$: $x \preceq y \iff x | y$
3. Inclusion sur $\mathcal{P}(X)$ ensemble des parties d'un ensemble X : $A \preceq B \iff A \subset B$

Pgcd et ppcm sur les entiers

Les lois pgcd et ppcm sur $\mathbb{N}$ et $\mathbb{Z}$ sont commutatives et associatives.

$a \wedge b = \text{pgcd}(a, b)$ le plus grand entier naturel qui divise a et b

$a \vee b = \text{ppcm}(a, b)$ le plus petit entier naturel non nul multiple de a et b

Pgcd et ppcm sur les entiers

Les lois pgcd et ppcm sur $\mathbb{N}$ et $\mathbb{Z}$ sont commutatives et associatives.

$a \wedge b = \text{pgcd}(a, b)$ le plus grand entier naturel qui divise a et b
$a \vee b = \text{ppcm}(a, b)$ le plus petit entier naturel non nul multiple de a et b

Lois $+$ et $\times$ sur l'ensemble des applications de E vers $\mathbb{R}$

On pose pour toutes applications $f, g : E \to \mathbb{R}$

$$\forall x \in E,\ (f + g)(x) = f(x) + g(x)$$

$$\forall x \in E,\ (f \times g)(x) = f(x) \times g(x).$$

Ces lois sont associatives et commutatives.

3. Elément neutre et inversibilité

Définition : Elément neutre

Soit E un ensemble muni d'une loi de composition $*$ et e un élément de E. On dit que e est un *élément neutre* pour la loi $*$ si, pour tout élément x de E, on a $x * e = e * x = x$.

Si la loi $*$ est commutative, l'égalité $x * e = e * x$ est automatiquement réalisée.

3. Elément neutre et inversibilité

Définition : Elément neutre

Soit E un ensemble muni d'une loi de composition $*$ et e un élément de E. On dit que e est un *élément neutre* pour la loi $*$ si, pour tout élément x de E, on a $x * e = e * x = x$.

Si la loi $*$ est commutative, l'égalité $x * e = e * x$ est automatiquement réalisée.

Proposition : unicité de l'élément neutre

L'élément neutre de l'ensemble E pour la loi $*$, s'il existe, est unique.

Exemples

- Dans $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ et $\mathbb{C}$, 0 est neutre pour la loi $+$
  1 est neutre pour la loi $\times$.

Exemples

- Dans $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ et $\mathbb{C}$, 0 est neutre pour la loi $+$
  1 est neutre pour la loi $\times$.

- Dans $\mathcal{F}(E)$, l'application identité Id_E est neutre pour la loi $\circ$.

Exemples

- Dans $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ et $\mathbb{C}$, 0 est neutre pour la loi $+$
  1 est neutre pour la loi $\times$.

- Dans $\mathcal{F}(E)$, l'application identité Id_E est neutre pour la loi $\circ$.

- Dans $\mathcal{P}(E)$, l'ensemble vide $\emptyset$ est neutre pour la loi $\cup$
  E est l'élément neutre pour la loi $\cap$.

Exemples

- Dans $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ et $\mathbb{C}$, 0 est neutre pour la loi $+$
  1 est neutre pour la loi $\times$.

- Dans $\mathcal{F}(E)$, l'application identité Id_E est neutre pour la loi $\circ$.

- Dans $\mathcal{P}(E)$, l'ensemble vide $\emptyset$ est neutre pour la loi $\cup$
  E est l'élément neutre pour la loi $\cap$.

- Dans $\mathbb{R}$, il n'y a pas d'élément neutre pour les lois min et max.

Exemples

- Dans $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ et $\mathbb{C}$, 0 est neutre pour la loi $+$
  1 est neutre pour la loi $\times$.

- Dans $\mathcal{F}(E)$, l'application identité Id_E est neutre pour la loi $\circ$.

- Dans $\mathcal{P}(E)$, l'ensemble vide $\emptyset$ est neutre pour la loi $\cup$
  E est l'élément neutre pour la loi $\cap$.

- Dans $\mathbb{R}$, il n'y a pas d'élément neutre pour les lois min et max.

- Dans $\mathcal{F}(E, \mathbb{R})$,
  l'application nulle est élément neutre pour la loi $+$
  l'application constante 1 est neutre pour la loi $\times$.

Soit E un ensemble muni d'une loi **associative** $*$. On suppose qu'il existe un élément neutre e.

Définition : Inversibilité d'un élément

Un élément x de E est dit *inversible* (pour la loi $*$) s'il existe x' dans E tel que $x * x' = x' * x = e$. Si un tel élément x' existe, il est unique. On le note en général x^{-1}, et on l'appelle l'*inverse* (ou le *symétrique*) de x pour la loi $*$.

Soit E un ensemble muni d'une loi **associative** $*$. On suppose qu'il existe un élément neutre e.

Définition : Inversibilité d'un élément

Un élément x de E est dit *inversible* (pour la loi $*$) s'il existe x' dans E tel que $x * x' = x' * x = e$. Si un tel élément x' existe, il est unique. On le note en général x^{-1}, et on l'appelle l'*inverse* (ou le *symétrique*) de x pour la loi $*$.

Remarques immédiates.

1. Si x est inversible, x^{-1} l'est aussi et $(x^{-1})^{-1} = x$.
2. L'élément neutre e de $(E, *)$ est inversible et il est son propre inverse.
3. Tout élément inversible a est *régulier*, c.–à–d.
   - $\forall x, y \in E,\ x * a = y * a \Rightarrow x = y$ (a régulier à droite)
   - $\forall x, y \in E,\ a * x = a * y \Rightarrow x = y$ (a régulier à gauche).

Remarques.

1. Dans le cas d'une loi $+$ (nécessairement commutative, d'élément neutre 0), on ne parle pas d'inverse ou de symétrique, mais d'*opposé*, et celui-ci n'est pas noté x^{-1} mais $-x$.

Remarques.

1. Dans le cas d'une loi $+$ (nécessairement commutative, d'élément neutre 0), on ne parle pas d'inverse ou de symétrique, mais d'*opposé*, et celui-ci n'est pas noté x^{-1} mais $-x$.
2. S'il n'y a pas de neutre dans $(E, *)$, la notion d'élément inversible n'a aucun sens.

Remarques.

1. Dans le cas d'une loi $+$ (nécessairement commutative, d'élément neutre 0), on ne parle pas d'inverse ou de symétrique, mais d'*opposé*, et celui-ci n'est pas noté x^{-1} mais $-x$.
2. S'il n'y a pas de neutre dans $(E, *)$, la notion d'élément inversible n'a aucun sens.
3. On suppose la loi $*$ associative pour garantir l'unicité du symétrique s'il existe.

Remarques.

1. Dans le cas d'une loi $+$ (nécessairement commutative, d'élément neutre 0), on ne parle pas d'inverse ou de symétrique, mais d'*opposé*, et celui-ci n'est pas noté x^{-1} mais $-x$.
2. S'il n'y a pas de neutre dans $(E, *)$, la notion d'élément inversible n'a aucun sens.
3. On suppose la loi $*$ associative pour garantir l'unicité du symétrique s'il existe.

Proposition : inversibilité du produit

Soit x et y deux éléments de E, inversibles pour la loi $*$, d'inverses respectifs x^{-1} et y^{-1}. Alors $x * y$ est inversible, et son inverse est $(x * y)^{-1} = y^{-1} * x^{-1}$.

Exemples

- Dans $(\mathbb{N}, +)$, seul 0 admet un opposé.

Dans $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ et $\mathbb{C}$ munis de la loi $+$, tous les éléments admettent un opposé.

Exemples

- Dans $(\mathbb{N}, +)$, seul 0 admet un opposé.

Dans $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ et $\mathbb{C}$ munis de la loi $+$, tous les éléments admettent un opposé.

- Dans $(\mathbb{N}, \times)$, le seul élément inversible est 1.

Dans $(\mathbb{Z}, \times)$, les seuls éléments inversibles sont -1 et 1.
Dans $\mathbb{Q}$, $\mathbb{R}$ et $\mathbb{C}$ munis de la loi $\times$, tous les éléments non nuls sont inversibles.

Exemples

- Dans $(\mathbb{N}, +)$, seul 0 admet un opposé.

Dans $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ et $\mathbb{C}$ munis de la loi $+$, tous les éléments admettent un opposé.

- Dans $(\mathbb{N}, \times)$, le seul élément inversible est 1.

Dans $(\mathbb{Z}, \times)$, les seuls éléments inversibles sont -1 et 1.
Dans $\mathbb{Q}$, $\mathbb{R}$ et $\mathbb{C}$ munis de la loi $\times$, tous les éléments non nuls sont inversibles.

- Dans $(\mathcal{F}(E), \circ)$, une application est inversible ssi elle est bijective de E sur E. Son inverse est son application réciproque.

Exemples

- Dans $(\mathbb{N}, +)$, seul 0 admet un opposé.

Dans $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ et $\mathbb{C}$ munis de la loi $+$, tous les éléments admettent un opposé.

- Dans $(\mathbb{N}, \times)$, le seul élément inversible est 1.

Dans $(\mathbb{Z}, \times)$, les seuls éléments inversibles sont -1 et 1.
Dans $\mathbb{Q}$, $\mathbb{R}$ et $\mathbb{C}$ munis de la loi $\times$, tous les éléments non nuls sont inversibles.

- Dans $(\mathcal{F}(E), \circ)$, une application est inversible ssi elle est bijective de E sur E. Son inverse est son application réciproque.

Dans $(\mathcal{F}(\mathbb{R}), \circ)$, f est inversible ssi $f : \mathbb{R} \to \mathbb{R}$ est bijective, son inverse est f^{-1}.
Dans $(\mathcal{F}(\mathbb{R}), \times)$, f est inversible ssi f ne s'annule pas, son inverse est $1/f$.

4. Stabilité pour une loi

Soit E un ensemble muni d'une loi de composition $*$ et F une partie de E.

Définition : Partie stable pour une loi

On dit que F est *stable* pour la loi $*$ si $x * y \in F$ pour tout $x, y \in F$. La restriction à $F \times F$ de la loi $*$ définit alors une loi de composition sur F appelée *loi induite* sur F par celle de E, et en général encore notée $*$.

4. Stabilité pour une loi

Soit E un ensemble muni d'une loi de composition $*$ et F une partie de E.

Définition : Partie stable pour une loi

On dit que F est *stable* pour la loi $*$ si $x * y \in F$ pour tout $x, y \in F$. La restriction à $F \times F$ de la loi $*$ définit alors une loi de composition sur F appelée *loi induite* sur F par celle de E, et en général encore notée $*$.

Remarques.

1. Si la loi $*$ sur E est commutative (resp. associative), il en est de même de la loi induite $*$ sur F.

4. Stabilité pour une loi

Soit E un ensemble muni d'une loi de composition $*$ et F une partie de E.

Définition : Partie stable pour une loi

On dit que F est *stable* pour la loi $*$ si $x * y \in F$ pour tout $x, y \in F$. La restriction à $F \times F$ de la loi $*$ définit alors une loi de composition sur F appelée *loi induite* sur F par celle de E, et en général encore notée $*$.

Remarques.

1. Si la loi $*$ sur E est commutative (resp. associative), il en est de même de la loi induite $*$ sur F.
2. Si e est neutre dans $(E, *)$, et si $e \in F$, alors bien sûr e est encore neutre dans $(F, *)$.

5. Distributivité

Soit $*$ et $\top$ deux lois de composition interne sur un même ensemble E.

Définition : Distributivité

On dit que $\top$ est *distributive* par rapport à $*$ si, pour tout $x, y, z \in E$, on a

$$x\top(y * z) = (x\top y) * (x\top z) \quad \text{(distributivité à gauche)},$$

$$(y * z)\top x = (y\top x) * (z\top x) \quad \text{(distributivité à droite)}.$$

5. Distributivité

Soit $*$ et $\top$ deux lois de composition interne sur un même ensemble E.

Définition : Distributivité

On dit que $\top$ est *distributive* par rapport à $*$ si, pour tout $x, y, z \in E$, on a

$$x\top(y * z) = (x\top y) * (x\top z) \quad \text{(distributivité à gauche)},$$

$$(y * z)\top x = (y\top x) * (z\top x) \quad \text{(distributivité à droite)}.$$

Exemples.

1. Dans $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, la loi $\times$ est distributive par rapport à la loi $+$.
2. Dans $\mathcal{P}(E)$, les lois $\cap$ et $\cup$ sont distributives l'une par rapport à l'autre.

II. Groupes et sous-groupes

1. Structure de groupe

Définition : Groupe

Soit G un ensemble muni d'une loi de composition interne $*$. On dit que $(G, *)$ est un *groupe* si :

- la loi $*$ est associative
- $(G, *)$ admet un élément neutre
- tout élément de G est inversible.

Si de plus la loi $*$ est commutative, on dit que $(G, *)$ est un *groupe commutatif* (ou encore *abélien*).

II. Groupes et sous-groupes

1. Structure de groupe

Définition : Groupe

Soit G un ensemble muni d'une loi de composition interne $*$. On dit que $(G, *)$ est un *groupe* si :

- la loi $*$ est associative
- $(G, *)$ admet un élément neutre
- tout élément de G est inversible.

Si de plus la loi $*$ est commutative, on dit que $(G, *)$ est un *groupe commutatif* (ou encore *abélien*).

Remarques. ① Un groupe est toujours non vide.

II. Groupes et sous-groupes

1. Structure de groupe

Définition : Groupe

Soit G un ensemble muni d'une loi de composition interne $*$. On dit que $(G, *)$ est un *groupe* si :

- la loi $*$ est associative
- $(G, *)$ admet un élément neutre
- tout élément de G est inversible.

Si de plus la loi $*$ est commutative, on dit que $(G, *)$ est un *groupe commutatif* (ou encore *abélien*).

Remarques. ① Un groupe est toujours non vide.
② Si la loi est notée $+$, $(G, +)$ est dit *groupe additif*. Le neutre est noté 0.

II. Groupes et sous-groupes

1. Structure de groupe

Définition : Groupe

Soit G un ensemble muni d'une loi de composition interne $*$. On dit que $(G, *)$ est un *groupe* si :

- la loi $*$ est associative
- $(G, *)$ admet un élément neutre
- tout élément de G est inversible.

Si de plus la loi $*$ est commutative, on dit que $(G, *)$ est un *groupe commutatif* (ou encore *abélien*).

Remarques. ① Un groupe est toujours non vide.

② Si la loi est notée $+$, $(G, +)$ est dit *groupe additif*. Le neutre est noté 0.

③ En cas de loi produit $\times$, $(G, \times)$ est dit *groupe multiplicatif*. Le neutre est noté 1.

Exemples usuels à connaître

1. Les ensembles $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ et $\mathbb{C}$ munis de la loi $+$ sont des groupes additifs de neutre 0.
2. Les ensembles $\mathbb{Q}^\star$, $\mathbb{R}^\star$ et $\mathbb{C}^\star$ munis de la loi $\times$ sont des groupes multiplicatifs de neutre 1.

Exemples usuels à connaître

1. Les ensembles $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ et $\mathbb{C}$ munis de la loi $+$ sont des groupes additifs de neutre 0.
2. Les ensembles $\mathbb{Q}^\star$, $\mathbb{R}^\star$ et $\mathbb{C}^\star$ munis de la loi $\times$ sont des groupes multiplicatifs de neutre 1.
3.  $(\mathbb{N},+)$, $(\mathbb{Z}^\star,\times)$, $(\mathbb{R},\times)$ **ne** sont **pas** des groupes.

Exemples usuels à connaître

1. Les ensembles $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ et $\mathbb{C}$ munis de la loi $+$ sont des groupes additifs de neutre 0.
2. Les ensembles $\mathbb{Q}^\star$, $\mathbb{R}^\star$ et $\mathbb{C}^\star$ munis de la loi $\times$ sont des groupes multiplicatifs de neutre 1.
3.  $(\mathbb{N},+)$, $(\mathbb{Z}^\star,\times)$, $(\mathbb{R},\times)$ **ne** sont **pas** des groupes.
4. **Groupes des permutations**. Soit E un ensemble et $\mathcal{S}(E)$ l'ensemble des permutations de E, c.–à–d. des bijections de E dans E. $(\mathcal{S}(E),\circ)$ est un groupe appelé le *groupe symétrique* de E. Son élément neutre est l'application identité Id_E. Il est non commutatif dès que E a au moins 3 éléments.

Exemples usuels à connaître

1. Les ensembles $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ et $\mathbb{C}$ munis de la loi $+$ sont des groupes additifs de neutre 0.
2. Les ensembles $\mathbb{Q}^\star$, $\mathbb{R}^\star$ et $\mathbb{C}^\star$ munis de la loi $\times$ sont des groupes multiplicatifs de neutre 1.
3.  $(\mathbb{N},+)$, $(\mathbb{Z}^\star,\times)$, $(\mathbb{R},\times)$ **ne** sont **pas** des groupes.
4. **Groupes des permutations**. Soit E un ensemble et $\mathcal{S}(E)$ l'ensemble des permutations de E, c.–à–d. des bijections de E dans E. $(\mathcal{S}(E),\circ)$ est un groupe appelé le *groupe symétrique* de E. Son élément neutre est l'application identité Id_E. Il est non commutatif dès que E a au moins 3 éléments.

   Lorsque E est un ensemble fini $\{1,2,\ldots,n\}$ on note alors $\mathcal{S}_n$ le n-ième groupe symétrique de E.

❺ **Matrices inversibles**. Pour $\mathbb{K} = \mathbb{R}$ ou $\mathbb{C}$, l'ensemble des matrices carrées $n \times n$ inversibles à coefficients dans $\mathbb{K}$

$$GL(n, \mathbb{K}) = \{M \in \mathcal{M}_n(\mathbb{K}) : \det M \neq 0\}$$

muni de $\times$ est un groupe appelé *groupe général linéaire* d'ordre n.

5. **Matrices inversibles**. Pour $\mathbb{K} = \mathbb{R}$ ou $\mathbb{C}$, l'ensemble des matrices carrées $n \times n$ inversibles à coefficients dans $\mathbb{K}$

$$GL(n, \mathbb{K}) = \{M \in \mathcal{M}_n(\mathbb{K}) : \det M \neq 0\}$$

muni de $\times$ est un groupe appelé *groupe général linéaire* d'ordre n.

6. L'ensemble des isométries (applications qui préservent les distances) du plan muni de $\circ$ est un groupe non commutatif. Ce sont les translations, rotations, réflexions et leurs composées.

Définition : Ordre d'un groupe

L'*ordre* d'un groupe $(G, *)$ est le cardinal de G, c.–à–d. le nombre d'éléments de G, noté card$G$.
Un groupe est dit *fini* si son ordre est fini. Sinon il est dit *infini*.

Définition : Ordre d'un groupe

L'*ordre* d'un groupe $(G, *)$ est le cardinal de G, c.–à–d. le nombre d'éléments de G, noté card$G$.
Un groupe est dit *fini* si son ordre est fini. Sinon il est dit *infini*.

Exemples de groupes finis

1. le groupe symétrique $(\mathcal{S}_n, \circ)$ est fini d'ordre $n!$.
2. $(G, \times)$ où $G = \{1, -1, i, -i\}$ est un groupe fini d'ordre 4.

Définition : Ordre d'un groupe

L'*ordre* d'un groupe $(G, *)$ est le cardinal de G, c.–à–d. le nombre d'éléments de G, noté card$G$.
Un groupe est dit *fini* si son ordre est fini. Sinon il est dit *infini*.

Exemples de groupes finis

1. le groupe symétrique $(\mathcal{S}_n, \circ)$ est fini d'ordre $n!$.
2. $(G, \times)$ où $G = \{1, -1, i, -i\}$ est un groupe fini d'ordre 4.

Pour faciliter l'étude des groupes finis, la *table de Cayley* (mathématicien britannique, 19^e) donne tous les résultats de la loi de composition interne dans un groupe fini. Les propriétés d'un groupe se déduisent à la lecture d'une telle table. Les éléments de la table sont uniques sur chaque ligne et sur chaque colonne. La table de Cayley comporte toutes les permutations des éléments du groupe.

Définition : Ordre d'un groupe

L'*ordre* d'un groupe $(G, *)$ est le cardinal de G, c.–à–d. le nombre d'éléments de G, noté card$G$.
Un groupe est dit *fini* si son ordre est fini. Sinon il est dit *infini*.

Exemples de groupes finis

1. le groupe symétrique $(\mathcal{S}_n, \circ)$ est fini d'ordre $n!$.
2. $(G, \times)$ où $G = \{1, -1, i, -i\}$ est un groupe fini d'ordre 4.

Pour faciliter l'étude des groupes finis, la *table de Cayley* (mathématicien britannique, 19^e) donne tous les résultats de la loi de composition interne dans un groupe fini. Les propriétés d'un groupe se déduisent à la lecture d'une telle table. Les éléments de la table sont uniques sur chaque ligne et sur chaque colonne. La table de Cayley comporte toutes les permutations des éléments du groupe.

2. Produit fini de groupes

Définition : Loi produit

Soit $\top_1, \ldots, \top_n$ des lois de composition interne sur des ensembles $E_1, \ldots, E_n$. On appelle *loi produit* sur $E := E_1 \times \cdots \times E_n$ la loi $\top$ définie par

$$(x_1, \cdots, x_n) \top (y_1, \cdots, y_n) = (x_1 \top_1 y_1, \cdots, x_n \top_n y_n).$$

2. Produit fini de groupes

Définition : Loi produit

Soit $\top_1, \ldots, \top_n$ des lois de composition interne sur des ensembles $E_1, \ldots, E_n$. On appelle *loi produit* sur $E := E_1 \times \cdots \times E_n$ la loi $\top$ définie par

$$(x_1, \cdots, x_n) \top (y_1, \cdots, y_n) = (x_1 \top_1 y_1, \cdots, x_n \top_n y_n).$$

Proposition

Si $(G_1, \top_1), \ldots, (G_n, \top_n)$ sont des groupes de neutres $e_1, \ldots, e_n$, alors $G = G_1 \times \cdots \times G_n$ muni de la loi produit $\top$ est un groupe de neutre $e := (e_1, \cdots, e_n)$. De plus,

1. l'inverse de $(x_1, \cdots, x_n) \in G$ est $(x_1^{-1}, \cdots, x_n^{-1})$,
2. si tous les groupes $(G_1, \top_1), \ldots, (G_n, \top_n)$ sont commutatifs, le groupe $(G, \top)$ l'est aussi.

3. Sous-groupe : définition et caractérisation

Définition : Sous-groupe d'un groupe

Soit $(G, *)$ un groupe et H une partie **non vide** de G. On dit que H est un *sous-groupe* de $(G, *)$ si :

- H est stable par loi de composition : $\forall x, y \in H,\ x * y \in H$.
- H est stable par passage à l'inverse : $\forall x \in H,\ x^{-1} \in H$.

3. Sous-groupe : définition et caractérisation

Définition : Sous-groupe d'un groupe

Soit $(G, *)$ un groupe et H une partie **non vide** de G. On dit que H est un *sous-groupe* de $(G, *)$ si :

- H est stable par loi de composition : $\forall x, y \in H,\ x * y \in H$.
- H est stable par passage à l'inverse : $\forall x \in H,\ x^{-1} \in H$.

Proposition

Soit H un sous-groupe de $(G, *)$. On munit H de la loi induite. Alors,

1. $(H, *)$ est lui-même un groupe ;
2. les deux groupes $(H, *)$ et $(G, *)$ ont même élément neutre ;
3. si x est un élément de H, l'inverse x^{-1} de x dans H est le même que celui dans G.

Proposition : Caractérisation des sous-groupes

Soit $(G, *)$ un groupe et H une partie **non vide** de G. Alors, H est un sous-groupe de $(G, *)$ si et seulement si :

$$\forall x, y \in H,\ x * y^{-1} \in H.$$

Proposition : Caractérisation des sous-groupes

Soit $(G, *)$ un groupe et H une partie **non vide** de G. Alors, H est un sous-groupe de $(G, *)$ si et seulement si :

$$\forall x, y \in H,\ x * y^{-1} \in H.$$

En notation additive, H est un sous-groupe de $(G, +)$ ssi $x - y \in H$ pour tous $x, y \in H$.

Proposition : Caractérisation des sous-groupes

Soit $(G, *)$ un groupe et H une partie **non vide** de G. Alors, H est un sous-groupe de $(G, *)$ si et seulement si :

$$\forall x, y \in H,\ x * y^{-1} \in H.$$

En notation additive, H est un sous-groupe de $(G, +)$ ssi $x - y \in H$ pour tous $x, y \in H$.

Proposition

Soit $(G, *)$ un groupe, H et H' deux sous-groupes de G. Alors, si elle est non vide, l'intersection $H \cap H'$ est un sous-groupe de G.

Proposition : Caractérisation des sous-groupes

Soit $(G, *)$ un groupe et H une partie **non vide** de G. Alors, H est un sous-groupe de $(G, *)$ si et seulement si :

$$\forall x, y \in H,\ x * y^{-1} \in H.$$

En notation additive, H est un sous-groupe de $(G, +)$ ssi $x - y \in H$ pour tous $x, y \in H$.

Proposition

Soit $(G, *)$ un groupe, H et H' deux sous-groupes de G. Alors, si elle est non vide, l'intersection $H \cap H'$ est un sous-groupe de G.

C'est faux pour la réunion !

Beaucoup d'exemples de groupes s'obtiennent en tant que sous-groupe d'un groupe plus gros, ce qui simplifie la vérification de l'associativité...

Exemples

1. Si $(G, *)$ est un groupe d'élément neutre e, alors G et $\{e\}$ sont des sous-groupes de G dits *sous-groupes triviaux* de G.

Exemples

1. Si $(G, *)$ est un groupe d'élément neutre e, alors G et $\{e\}$ sont des sous-groupes de G dits *sous-groupes triviaux* de G.
2. $(\mathbb{Z}, +)$ est un sous-groupe de $(\mathbb{Q}, +)$, lui-même sous-groupe de $(\mathbb{R}, +)$.

Exemples

1. Si $(G, *)$ est un groupe d'élément neutre e, alors G et $\{e\}$ sont des sous-groupes de G dits *sous-groupes triviaux* de G.
2. $(\mathbb{Z}, +)$ est un sous-groupe de $(\mathbb{Q}, +)$, lui-même sous-groupe de $(\mathbb{R}, +)$.
3. Les ensembles des translations, homothéties, rotations du plan sont des sous-groupes du groupe des permutations du plan muni de $\circ$. L'ensemble des isométries du plan aussi.

Exemples

1. Si $(G, *)$ est un groupe d'élément neutre e, alors G et $\{e\}$ sont des sous-groupes de G dits *sous-groupes triviaux* de G.
2. $(\mathbb{Z}, +)$ est un sous-groupe de $(\mathbb{Q}, +)$, lui-même sous-groupe de $(\mathbb{R}, +)$.
3. Les ensembles des translations, homothéties, rotations du plan sont des sous-groupes du groupe des permutations du plan muni de $\circ$. L'ensemble des isométries du plan aussi.
4. **Nombres complexes de module** 1. Notons $\mathbb{U} = \{z \in \mathbb{C} \mid |z| = 1\}$. Alors $(\mathbb{U}, \times)$ est un sous-groupe du groupe $(\mathbb{C}^\star, \times)$.

❺ **Racines de l'unité.** Soit $n \in \mathbb{N}^\star$. Notons $\mathbb{U}_n \overset{\text{déf.}}{=} \{z \in \mathbb{C} \mid z^n = 1\}$. Alors,

$$\mathbb{U}_n = \{1, \omega, \omega^2, \cdots, \omega^{n-1}\},\ \omega = e^{2i\pi/n}$$

et $(\mathbb{U}_n, \times)$ est un sous-groupe du groupe $(\mathbb{C}^\star, \times)$. C'est un groupe fini d'ordre n.

❺ **Racines de l'unité**. Soit $n \in \mathbb{N}^\star$. Notons $\mathbb{U}_n \overset{\text{déf.}}{=} \{z \in \mathbb{C} \mid z^n = 1\}$. Alors,

$$\mathbb{U}_n = \{1, \omega, \omega^2, \cdots, \omega^{n-1}\},\ \omega = e^{2i\pi/n}$$

et $(\mathbb{U}_n, \times)$ est un sous-groupe du groupe $(\mathbb{C}^\star, \times)$. C'est un groupe fini d'ordre n.

❻ **Groupe spécial linéaire**. Pour $\mathbb{K} = \mathbb{R}$ ou $\mathbb{C}$, l'ensemble

$$SL(n, \mathbb{K}) = \{M \in \mathcal{M}_n(\mathbb{K}) : \det M = 1\}$$

muni de $\times$ est un sous-groupe de $(GL(n, \mathbb{K}), \times)$. Il est appelé *groupe spécial linéaire* d'ordre n sur $\mathbb{K}$.

❼ **Les sous-groupes de $\mathbb{Z}$.** Pour tout $n \in \mathbb{N}$, on note $\boldsymbol{n\mathbb{Z}} \overset{\text{déf.}}{=} \boldsymbol{\{kn, k \in \mathbb{Z}\}}$ l'ensemble des entiers divisibles par n ou encore l'ensemble des multiples de n.

Théorème

Les sous-groupes de $(\mathbb{Z}, +)$ sont exactement les $n\mathbb{Z}$ où $n \in \mathbb{N}$.

❼ **Les sous-groupes de $\mathbb{Z}$.** Pour tout $n \in \mathbb{N}$, on note $\boldsymbol{n\mathbb{Z}} \overset{\text{déf.}}{=} \boldsymbol{\{kn, k \in \mathbb{Z}\}}$ l'ensemble des entiers divisibles par n ou encore l'ensemble des multiples de n.

Théorème

Les sous-groupes de $(\mathbb{Z}, +)$ sont exactement les $n\mathbb{Z}$ où $n \in \mathbb{N}$.

dém. Tout d'abord, on vérifie aisément que $n\mathbb{Z}$ est un sous-groupe de $(\mathbb{Z}, +)$ pour tout $n \in \mathbb{N}$: il est non vide, la somme et l'oppposé de multiples de n sont encores des multiples de n.

❼ **Les sous-groupes de $\mathbb{Z}$.** Pour tout $n \in \mathbb{N}$, on note $\boldsymbol{n\mathbb{Z}} \overset{\text{déf.}}{=} \boldsymbol{\{kn, k \in \mathbb{Z}\}}$ l'ensemble des entiers divisibles par n ou encore l'ensemble des multiples de n.

Théorème

Les sous-groupes de $(\mathbb{Z}, +)$ sont exactement les $n\mathbb{Z}$ où $n \in \mathbb{N}$.

dém. Tout d'abord, on vérifie aisément que $n\mathbb{Z}$ est un sous-groupe de $(\mathbb{Z}, +)$ pour tout $n \in \mathbb{N}$: il est non vide, la somme et l'oppposé de multiples de n sont encores des multiples de n.
Ensuite, on considère un sous-groupe H de $(\mathbb{Z}, +)$ et on montre qu'il est de la forme $n\mathbb{Z}$.

❼ Les sous-groupes de $\mathbb{Z}$. Pour tout $n \in \mathbb{N}$, on note $\boldsymbol{n\mathbb{Z}} \overset{\text{déf.}}{=} \boldsymbol{\{kn, k \in \mathbb{Z}\}}$ l'ensemble des entiers divisibles par n ou encore l'ensemble des multiples de n.

Théorème

Les sous-groupes de $(\mathbb{Z}, +)$ sont exactement les $n\mathbb{Z}$ où $n \in \mathbb{N}$.

dém. Tout d'abord, on vérifie aisément que $n\mathbb{Z}$ est un sous-groupe de $(\mathbb{Z}, +)$ pour tout $n \in \mathbb{N}$: il est non vide, la somme et l'oppposé de multiples de n sont encores des multiples de n.
Ensuite, on considère un sous-groupe H de $(\mathbb{Z}, +)$ et on montre qu'il est de la forme $n\mathbb{Z}$. Déjà, H contient le neutre 0. Si $H = \{0\}$, alors $H = 0\mathbb{Z}$, sinon H contient un élément x_0 entier non nul.

❼ Les sous-groupes de $\mathbb{Z}$. Pour tout $n \in \mathbb{N}$, on note $\boldsymbol{n\mathbb{Z}} \overset{\text{déf.}}{=} \boldsymbol{\{kn, k \in \mathbb{Z}\}}$ l'ensemble des entiers divisibles par n ou encore l'ensemble des multiples de n.

Théorème

Les sous-groupes de $(\mathbb{Z}, +)$ sont exactement les $n\mathbb{Z}$ où $n \in \mathbb{N}$.

dém. Tout d'abord, on vérifie aisément que $n\mathbb{Z}$ est un sous-groupe de $(\mathbb{Z}, +)$ pour tout $n \in \mathbb{N}$: il est non vide, la somme et l'oppposé de multiples de n sont encores des multiples de n.
Ensuite, on considère un sous-groupe H de $(\mathbb{Z}, +)$ et on montre qu'il est de la forme $n\mathbb{Z}$. Déjà, H contient le neutre 0. Si $H = \{0\}$, alors $H = 0\mathbb{Z}$, sinon H contient un élément x_0 entier non nul. Posons

$$H^+ = \{x \in H \mid x > 0\}.$$

Alors, x_0 ou $-x_0$ appartient à H^+. Dans tous les cas, H^+ est une partie non vide de $\mathbb{N}$.

Rappelons : *Toute partie non vide de* $\mathbb{N}$ *admet un plus petit élément.*
Donc, $H^+ = \{x \in H \mid x > 0\}$ admet un plus petit élément, noté n :

$$n = \min H^+.$$

Rappelons : *Toute partie non vide de* $\mathbb{N}$ *admet un plus petit élément.*
Donc, $H^+ = \{x \in H \mid x > 0\}$ admet un plus petit élément, noté n :

$$n = \min H^+.$$

Comme $n \in H$, par propriété de sous-groupe, on a : $n\mathbb{Z} \subset H$.

Rappelons : *Toute partie non vide de* $\mathbb{N}$ *admet un plus petit élément.*
Donc, $H^+ = \{x \in H \mid x > 0\}$ admet un plus petit élément, noté n :

$$n = \min H^+.$$

Comme $n \in H$, par propriété de sous-groupe, on a : $n\mathbb{Z} \subset H$.
Pour l'iclusion inverse, on fixe $x \in H$ et on effectue la division euclidienne de x par n. Il existe un unique couple d'entiers (q, r) tel que $x = nq + r$ et $0 \leqslant r < n$.

Rappelons : *Toute partie non vide de* $\mathbb{N}$ *admet un plus petit élément.*
Donc, $H^+ = \{x \in H \mid x > 0\}$ admet un plus petit élément, noté n :

$$n = \min H^+.$$

Comme $n \in H$, par propriété de sous-groupe, on a : $n\mathbb{Z} \subset H$.
Pour l'iclusion inverse, on fixe $x \in H$ et on effectue la division euclidienne de x par n. Il existe un unique couple d'entiers (q, r) tel que $x = nq + r$ et $0 \leqslant r < n$. Alors, $r = x - nq \in H$ car $x, nq \in H$, et donc

$$r \in H^+ \text{ et } r < n.$$

Rappelons : *Toute partie non vide de* $\mathbb{N}$ *admet un plus petit élément.*
Donc, $H^+ = \{x \in H \mid x > 0\}$ admet un plus petit élément, noté n :

$$n = \min H^+.$$

Comme $n \in H$, par propriété de sous-groupe, on a : $n\mathbb{Z} \subset H$.
Pour l'iclusion inverse, on fixe $x \in H$ et on effectue la division euclidienne de x par n. Il existe un unique couple d'entiers (q, r) tel que $x = nq + r$ et $0 \leqslant r < n$. Alors, $r = x - nq \in H$ car $x, nq \in H$, et donc

$$r \in H^+ \quad \text{et } r < n.$$

Par défintion de n, il s'ensuit $r = 0$, ce qui entraîne $x = nq \in n\mathbb{Z}$. Ainsi, $H \subset n\mathbb{Z}$ et par double inclusion on a l'égalité. ■

4. Sous-groupe engendré par une partie

Soit $(G, *)$ un groupe et A une partie de G. Désignons par $\mathcal{H}$ la famille des sous-groupes de G contenant A. On pose $\langle \boldsymbol{A} \rangle = \bigcap_{\boldsymbol{H} \in \boldsymbol{\mathcal{H}}} \boldsymbol{H}$ l'intersection de tous les sous-groupes de G qui contiennent A.

4. Sous-groupe engendré par une partie

Soit $(G, *)$ un groupe et A une partie de G. Désignons par $\mathcal{H}$ la famille des sous-groupes de G contenant A. On pose $\langle \boldsymbol{A} \rangle = \bigcap_{\boldsymbol{H} \in \boldsymbol{\mathcal{H}}} \boldsymbol{H}$ l'intersection de tous les sous-groupes de G qui contiennent A. Lorsque A est réduit à un singleton $\{a\}$, on note simplement $\langle A \rangle = \langle a \rangle$.

4. Sous-groupe engendré par une partie

Soit $(G, *)$ un groupe et A une partie de G. Désignons par $\mathcal{H}$ la famille des sous-groupes de G contenant A. On pose $\langle \boldsymbol{A} \rangle = \bigcap_{\boldsymbol{H} \in \boldsymbol{\mathcal{H}}} \boldsymbol{H}$ l'intersection de tous les sous-groupes de G qui contiennent A. Lorsque A est réduit à un singleton $\{a\}$, on note simplement $\langle A \rangle = \langle a \rangle$.

Proposition

$\langle A \rangle$ est le plus petit (pour l'inclusion) sous-groupe de G contenant A.

4. Sous-groupe engendré par une partie

Soit $(G, *)$ un groupe et A une partie de G. Désignons par $\mathcal{H}$ la famille des sous-groupes de G contenant A. On pose $\langle \boldsymbol{A} \rangle = \bigcap_{\boldsymbol{H} \in \boldsymbol{\mathcal{H}}} \boldsymbol{H}$ l'intersection de tous les sous-groupes de G qui contiennent A. Lorsque A est réduit à un singleton $\{a\}$, on note simplement $\langle A \rangle = \langle a \rangle$.

Proposition

$\langle A \rangle$ est le plus petit (pour l'inclusion) sous-groupe de G contenant A.

Définitions

A est appelé un *système générateur* de $\langle A \rangle$. On dit que $\langle A \rangle$ est le *sous-groupe engendré* par A.

4. Sous-groupe engendré par une partie

Soit $(G, *)$ un groupe et A une partie de G. Désignons par $\mathcal{H}$ la famille des sous-groupes de G contenant A. On pose $\langle \boldsymbol{A} \rangle = \bigcap_{\boldsymbol{H} \in \boldsymbol{\mathcal{H}}} \boldsymbol{H}$ l'intersection de tous les sous-groupes de G qui contiennent A. Lorsque A est réduit à un singleton $\{a\}$, on note simplement $\langle A \rangle = \langle a \rangle$.

Proposition

$\langle A \rangle$ est le plus petit (pour l'inclusion) sous-groupe de G contenant A.

Définitions

A est appelé un *système générateur* de $\langle A \rangle$. On dit que $\langle A \rangle$ est le *sous-groupe engendré* par A.

On dit qu'un groupe est *monogène* s'il est engendré par un des ses éléments ; on dit qu'il est *cyclique* s'il est monogène et fini.

Exemples et remarques

1. $\langle \emptyset \rangle = \{e\}$ (e étant l'élément neutre) et $\langle G \rangle = G$.

Exemples et remarques

1. $\langle \emptyset \rangle = \{e\}$ (e étant l'élément neutre) et $\langle G \rangle = G$.
2. Si $G = \mathbb{Z}$, $\langle \{2, 3\} \rangle = \mathbb{Z}$ et $\langle \{6, 8\} \rangle = 2\mathbb{Z}$.

Exemples et remarques

1. $\langle \emptyset \rangle = \{e\}$ (e étant l'élément neutre) et $\langle G \rangle = G$.
2. Si $G = \mathbb{Z}$, $\langle \{2, 3\} \rangle = \mathbb{Z}$ et $\langle \{6, 8\} \rangle = 2\mathbb{Z}$.
3. **Sous-groupe monogène** : le sous-groupe de G engendré par $a \in G$ est $\langle a \rangle = \{a^n \mid n \in \mathbb{Z}\}$. En notation additive, $\langle a \rangle = a\mathbb{Z}$.

Exemples et remarques

1. $\langle \emptyset \rangle = \{e\}$ (e étant l'élément neutre) et $\langle G \rangle = G$.
2. Si $G = \mathbb{Z}$, $\langle \{2, 3\} \rangle = \mathbb{Z}$ et $\langle \{6, 8\} \rangle = 2\mathbb{Z}$.
3. **Sous-groupe monogène** : le sous-groupe de G engendré par $a \in G$ est $\langle a \rangle = \{a^n \mid n \in \mathbb{Z}\}$. En notation additive, $\langle a \rangle = a\mathbb{Z}$.

Complément : puissance entière d'un élément

On définit les puissances entières x^n ($n \in \mathbb{Z}$) de $x \in G$ par :

- $x^0 = e$
- $x^{n+1} = x * x^n$ pour tout $n \in \mathbb{N}$
- $x^{-n} = (x^n)^{-1} = (x^{-1})^n$ pour tout $n \in \mathbb{N}^\star$.

Exemples et remarques

1. $\langle \emptyset \rangle = \{e\}$ (e étant l'élément neutre) et $\langle G \rangle = G$.
2. Si $G = \mathbb{Z}$, $\langle \{2, 3\} \rangle = \mathbb{Z}$ et $\langle \{6, 8\} \rangle = 2\mathbb{Z}$.
3. **Sous-groupe monogène** : le sous-groupe de G engendré par $a \in G$ est $\langle a \rangle = \{a^n \mid n \in \mathbb{Z}\}$. En notation additive, $\langle a \rangle = a\mathbb{Z}$.

Complément : puissance entière d'un élément

On définit les puissances entières x^n ($n \in \mathbb{Z}$) de $x \in G$ par :

- $x^0 = e$
- $x^{n+1} = x * x^n$ pour tout $n \in \mathbb{N}$
- $x^{-n} = (x^n)^{-1} = (x^{-1})^n$ pour tout $n \in \mathbb{N}^\star$.

- $(\mathbb{Z}, +)$ est monogène engendré par 1. Les sous-groupes de $(\mathbb{Z}, +)$ sont tous monogènes.

Exemples et remarques

1. $\langle \emptyset \rangle = \{e\}$ (e étant l'élément neutre) et $\langle G \rangle = G$.
2. Si $G = \mathbb{Z}$, $\langle \{2, 3\} \rangle = \mathbb{Z}$ et $\langle \{6, 8\} \rangle = 2\mathbb{Z}$.
3. **Sous-groupe monogène** : le sous-groupe de G engendré par $a \in G$ est $\langle a \rangle = \{a^n \mid n \in \mathbb{Z}\}$. En notation additive, $\langle a \rangle = a\mathbb{Z}$.

Complément : puissance entière d'un élément

On définit les puissances entières x^n ($n \in \mathbb{Z}$) de $x \in G$ par :

- $x^0 = e$
- $x^{n+1} = x * x^n$ pour tout $n \in \mathbb{N}$
- $x^{-n} = (x^n)^{-1} = (x^{-1})^n$ pour tout $n \in \mathbb{N}^\star$.

- $(\mathbb{Z}, +)$ est monogène engendré par 1. Les sous-groupes de $(\mathbb{Z}, +)$ sont tous monogènes.
- $(\mathbb{U}_n, \times)$ est cylique engendré par $e^{2i\pi/n}$.

Exemples et remarques

1. $\langle \emptyset \rangle = \{e\}$ (e étant l'élément neutre) et $\langle G \rangle = G$.
2. Si $G = \mathbb{Z}$, $\langle \{2, 3\} \rangle = \mathbb{Z}$ et $\langle \{6, 8\} \rangle = 2\mathbb{Z}$.
3. **Sous-groupe monogène** : le sous-groupe de G engendré par $a \in G$ est $\langle a \rangle = \{a^n \mid n \in \mathbb{Z}\}$. En notation additive, $\langle a \rangle = a\mathbb{Z}$.

Complément : puissance entière d'un élément

On définit les puissances entières x^n ($n \in \mathbb{Z}$) de $x \in G$ par :

- $x^0 = e$
- $x^{n+1} = x * x^n$ pour tout $n \in \mathbb{N}$
- $x^{-n} = (x^n)^{-1} = (x^{-1})^n$ pour tout $n \in \mathbb{N}^\star$.

- $(\mathbb{Z}, +)$ est monogène engendré par 1. Les sous-groupes de $(\mathbb{Z}, +)$ sont tous monogènes.
- $(\mathbb{U}_n, \times)$ est cylique engendré par $e^{2i\pi/n}$.
- Par contre, $(\mathbb{C}, +)$, $(\mathbb{C}^\star, \times)$ ou $(S_n, \circ)$, $n \geqslant 3$, ne sont pas des groupes monogènes.

Théorème

Soit A une partie du groupe $(G, *)$. Le sous-groupe $\langle A \rangle$ de G est formé des éléments $x_1 * x_2 * \ldots * x_n$ où $n \in \mathbb{N}$ et, x_i ou $(x_i)^{-1}$ dans A.

Théorème

Soit A une partie du groupe $(G, *)$. Le sous-groupe $\langle A \rangle$ de G est formé des éléments $x_1 * x_2 * \ldots * x_n$ où $n \in \mathbb{N}$ et, x_i ou $(x_i)^{-1}$ dans A.

idée de la dém. pour $A \neq \emptyset$. Posons

$$H = \{x_1 * x_2 * \ldots * x_n \mid n \in \mathbb{N}, x_i \text{ ou } (x_i)^{-1} \in A\}.$$

On vérifie aisément que H est un sous-groupe de G contenant A. Il reste à montrer que c'est le plus petit contenant A.

Théorème

Soit A une partie du groupe $(G, *)$. Le sous-groupe $\langle A \rangle$ de G est formé des éléments $x_1 * x_2 * \ldots * x_n$ où $n \in \mathbb{N}$ et, x_i ou $(x_i)^{-1}$ dans A.

idée de la dém. pour $A \neq \emptyset$. Posons

$$H = \{x_1 * x_2 * \ldots * x_n \mid n \in \mathbb{N}, x_i \text{ ou } (x_i)^{-1} \in A\}.$$

On vérifie aisément que H est un sous-groupe de G contenant A. Il reste à montrer que c'est le plus petit contenant A.
On suppose qu'il existe K sous-groupe de G contenant A. Alors si x_i ou x_i^{-1}, $i \in \{1, \cdots, n\}$, appartiennent à A, par propriété de sous-groupe, ils appartiennent à K et, $x_1 * x_2 * \ldots * x_n$ appartient à K.

Théorème

Soit A une partie du groupe $(G, *)$. Le sous-groupe $\langle A \rangle$ de G est formé des éléments $x_1 * x_2 * \ldots * x_n$ où $n \in \mathbb{N}$ et, x_i ou $(x_i)^{-1}$ dans A.

idée de la dém. pour $A \neq \emptyset$. Posons

$$H = \{x_1 * x_2 * \ldots * x_n \mid n \in \mathbb{N}, x_i \text{ ou } (x_i)^{-1} \in A\}.$$

On vérifie aisément que H est un sous-groupe de G contenant A. Il reste à montrer que c'est le plus petit contenant A.
On suppose qu'il existe K sous-groupe de G contenant A. Alors si x_i ou x_i^{-1}, $i \in \{1, \cdots, n\}$, appartiennent à A, par propriété de sous-groupe, ils appartiennent à K et, $x_1 * x_2 * \ldots * x_n$ appartient à K.Donc $H \subset K$, et H est bien le plus petit sous-groupe de G contenant A. ■

5. Ordre d'un élément dans un groupe

Définition : ordre d'un élément

Un élément a d'un groupe $(G, *)$ est dit *d'ordre fini* s'il existe $n \in \mathbb{N}^\star$ vérifiant $a^n = e$. On appelle alors *ordre de* a le plus petit entier $n \in \mathbb{N}^\star$ vérifiant $a^n = e$.
Sinon, son ordre est dit *infini*.

5. Ordre d'un élément dans un groupe

Définition : ordre d'un élément

Un élément a d'un groupe $(G, *)$ est dit *d'ordre fini* s'il existe $n \in \mathbb{N}^\star$ vérifiant $a^n = e$. On appelle alors *ordre de* a le plus petit entier $n \in \mathbb{N}^\star$ vérifiant $a^n = e$.
Sinon, son ordre est dit *infini*.

Exemples

- L'ordre du neutre e est 1 ; c'est l'unique élément d'ordre 1.

5. Ordre d'un élément dans un groupe

Définition : ordre d'un élément

Un élément a d'un groupe $(G, *)$ est dit *d'ordre fini* s'il existe $n \in \mathbb{N}^\star$ vérifiant $a^n = e$. On appelle alors *ordre de* a le plus petit entier $n \in \mathbb{N}^\star$ vérifiant $a^n = e$.
Sinon, son ordre est dit *infini*.

Exemples

- L'ordre du neutre e est 1 ; c'est l'unique élément d'ordre 1.
- Dans $(\mathbb{Z}, +)$, tous les entiers non nuls sont d'ordre infini.

5. Ordre d'un élément dans un groupe

Définition : ordre d'un élément

Un élément a d'un groupe $(G, *)$ est dit *d'ordre fini* s'il existe $n \in \mathbb{N}^\star$ vérifiant $a^n = e$. On appelle alors *ordre de* a le plus petit entier $n \in \mathbb{N}^\star$ vérifiant $a^n = e$.
Sinon, son ordre est dit *infini*.

Exemples

- L'ordre du neutre e est 1 ; c'est l'unique élément d'ordre 1.
- Dans $(\mathbb{Z}, +)$, tous les entiers non nuls sont d'ordre infini.
- Dans $(\mathbb{C}^\star, \times)$, l'élément 2 est d'ordre infini ; $\frac{-1+\sqrt{3}}{2}$ est d'ordre fini.

5. Ordre d'un élément dans un groupe

Définition : ordre d'un élément

Un élément a d'un groupe $(G, *)$ est dit *d'ordre fini* s'il existe $n \in \mathbb{N}^\star$ vérifiant $a^n = e$. On appelle alors *ordre de* a le plus petit entier $n \in \mathbb{N}^\star$ vérifiant $a^n = e$.
Sinon, son ordre est dit *infini*.

Exemples

- L'ordre du neutre e est 1 ; c'est l'unique élément d'ordre 1.
- Dans $(\mathbb{Z}, +)$, tous les entiers non nuls sont d'ordre infini.
- Dans $(\mathbb{C}^\star, \times)$, l'élément 2 est d'ordre infini ; $\frac{-1+\sqrt{3}}{2}$ est d'ordre fini.
- Dans $(\mathbb{U}_n, \times)$, $\omega = e^{2i\pi/n}$ est d'ordre fini égal à n.

5. Ordre d'un élément dans un groupe

Définition : ordre d'un élément

Un élément a d'un groupe $(G, *)$ est dit *d'ordre fini* s'il existe $n \in \mathbb{N}^\star$ vérifiant $a^n = e$. On appelle alors *ordre de* a le plus petit entier $n \in \mathbb{N}^\star$ vérifiant $a^n = e$.
Sinon, son ordre est dit *infini*.

Exemples

- L'ordre du neutre e est 1 ; c'est l'unique élément d'ordre 1.
- Dans $(\mathbb{Z}, +)$, tous les entiers non nuls sont d'ordre infini.
- Dans $(\mathbb{C}^\star, \times)$, l'élément 2 est d'ordre infini ; $\frac{-1+\sqrt{3}}{2}$ est d'ordre fini.
- Dans $(\mathbb{U}_n, \times)$, $\omega = e^{2i\pi/n}$ est d'ordre fini égal à n.
- Dans le groupe symétrique $\mathcal{S}_3$, les trois transpositions sont d'ordre 2 et les deux permutations circulaires sont d'ordre 3.

Théorème

Si a est d'ordre fini égal à p, alors pour tout entier $n \in \mathbb{Z}$

$$a^n = e \iff p|n.$$

Théorème

Si a est d'ordre fini égal à p, alors pour tout entier $n \in \mathbb{Z}$

$$a^n = e \iff p|n.$$

dém. "$\Leftarrow$" Si p divise n, il existe $q \in \mathbb{Z}$ tel que $n = qp$, ce qui entraîne $a^n = \left(a^p\right)^q = e^q = e$.

Théorème

Si a est d'ordre fini égal à p, alors pour tout entier $n \in \mathbb{Z}$

$$a^n = e \iff p|n.$$

dém. "$\Leftarrow$" Si p divise n, il existe $q \in \mathbb{Z}$ tel que $n = qp$, ce qui entraîne $a^n = \left(a^p\right)^q = e^q = e$.

"$\Rightarrow$" On suppose que $a^n = e$.
D'abord, si $n \geqslant 1$, on effectue la division euclidienne de n par p : il existe un unique couple d'entiers (q, r) tel que $n = qp + r$ et $0 \leqslant r < p$.
Alors, $a^r = a^{qp} * a^r = a^n = e$ avec $r < p$.

Théorème

Si a est d'ordre fini égal à p, alors pour tout entier $n \in \mathbb{Z}$

$$a^n = e \iff p|n.$$

dém. "$\Leftarrow$" Si p divise n, il existe $q \in \mathbb{Z}$ tel que $n = qp$, ce qui entraîne $a^n = \left(a^p\right)^q = e^q = e$.

"$\Rightarrow$" On suppose que $a^n = e$.
D'abord, si $n \geqslant 1$, on effectue la division euclidienne de n par p : il existe un unique couple d'entiers (q, r) tel que $n = qp + r$ et $0 \leqslant r < p$. Alors, $a^r = a^{qp} * a^r = a^n = e$ avec $r < p$. Par définition de p (le plus entier positif non nul tel que $a^p = e$...), on obtient $r = 0$, et donc p divise n.

Théorème

Si a est d'ordre fini égal à p, alors pour tout entier $n \in \mathbb{Z}$

$$a^n = e \iff p | n.$$

dém. "$\Leftarrow$" Si p divise n, il existe $q \in \mathbb{Z}$ tel que $n = qp$, ce qui entraîne $a^n = \left(a^p\right)^q = e^q = e$.

"$\Rightarrow$" On suppose que $a^n = e$.
D'abord, si $n \geqslant 1$, on effectue la division euclidienne de n par p : il existe un unique couple d'entiers (q, r) tel que $n = qp + r$ et $0 \leqslant r < p$. Alors, $a^r = a^{qp} * a^r = a^n = e$ avec $r < p$. Par définition de p (le plus entier positif non nul tel que $a^p = e$...), on obtient $r = 0$, et donc p divise n. Ensuite, si $n = 0$, on a toujours $p \mid n$.

Théorème

Si a est d'ordre fini égal à p, alors pour tout entier $n \in \mathbb{Z}$

$$a^n = e \iff p | n.$$

dém. "$\Leftarrow$" Si p divise n, il existe $q \in \mathbb{Z}$ tel que $n = qp$, ce qui entraîne $a^n = \left(a^p\right)^q = e^q = e$.

"$\Rightarrow$" On suppose que $a^n = e$.
D'abord, si $n \geqslant 1$, on effectue la division euclidienne de n par p : il existe un unique couple d'entiers (q, r) tel que $n = qp + r$ et $0 \leqslant r < p$. Alors, $a^r = a^{qp} * a^r = a^n = e$ avec $r < p$. Par définition de p (le plus entier positif non nul tel que $a^p = e$...), on obtient $r = 0$, et donc p divise n.
Ensuite, si $n = 0$, on a toujours $p \mid n$.
Enfin, si $n \leqslant -1$, alors $-n \geqslant 1$, et d'après ce qui précède, $p \mid -n$, ce qui équivaut à $p \mid n$. ■

III. Introduction aux groupes quotient

1. Classes suivant un sous-groupe

Soit $(G, *)$ un groupe et H un sous-groupe. On définit la relation binaire sur G suivante

$$x\mathcal{R}y \overset{\text{déf.}}{\iff} x^{-1} * y \in H.$$

Rappel : une *relation binaire* sur un ensemble G est la donnée d'une partie $\mathcal{R}$ de $G \times G$; on note $x\mathcal{R}y$ pour signifier $(x, y) \in \mathcal{R}$.

III. Introduction aux groupes quotient

1. Classes suivant un sous-groupe

Soit $(G, *)$ un groupe et H un sous-groupe. On définit la relation binaire sur G suivante

$$x\mathcal{R}y \overset{\text{déf.}}{\iff} x^{-1} * y \in H.$$

Rappel : une *relation binaire* sur un ensemble G est la donnée d'une partie $\mathcal{R}$ de $G \times G$; on note $x\mathcal{R}y$ pour signifier $(x, y) \in \mathcal{R}$.

Propriété

$\mathcal{R}$ est une **relation d'équivalence**, c.–à–d.

1. $\mathcal{R}$ est *réflexive* : $\forall x \in G,\ x\mathcal{R}x$;
2. $\mathcal{R}$ est *symétrique* : $\forall x, y \in G,\ x\mathcal{R}y \Rightarrow y\mathcal{R}x$;
3. $\mathcal{R}$ est *transitive* : $\forall x, y, z \in G,\ (x\mathcal{R}y \text{ et } y\mathcal{R}z) \Rightarrow x\mathcal{R}z$.

Propriété

$\mathcal{R}$ est une **congruence à gauche**, c.–à–d.

1. $\mathcal{R}$ est une relation d'équivalence
2. $x\mathcal{R}y \Longrightarrow (\forall a \in G,\ (a * x)\mathcal{R}(a * y))$.

Propriété

$\mathcal{R}$ est une **congruence à gauche**, c.–à–d.

1. $\mathcal{R}$ est une relation d'équivalence
2. $x\mathcal{R}y \Longrightarrow (\forall a \in G,\ (a * x)\mathcal{R}(a * y))$.

Posons $xH \overset{\text{déf.}}{=} \{x * h : h \in H\}$. Alors,

$$x\mathcal{R}y \iff y \in xH$$

Propriété

$\mathcal{R}$ est une **congruence à gauche**, c.–à–d.

1. $\mathcal{R}$ est une relation d'équivalence
2. $x\mathcal{R}y \Longrightarrow (\forall a \in G,\ (a * x)\mathcal{R}(a * y))$.

Posons $xH \overset{\text{déf.}}{=} \{x * h : h \in H\}$. Alors,

$$x\mathcal{R}y \iff y \in xH$$

Exemple

Si $G = \mathbb{Z}$ muni de $+$ et $H = n\mathbb{Z}$, alors $xH = \{x + ny : y \in \mathbb{Z}\}$ et

$$x\mathcal{R}y \iff x \equiv y[n],$$

autrement dit x est congru à y modulo n, c.–à–d. n divise $y - x$. $\mathcal{R}$ est une congruence (à gauche et à droite).

Définition : classe d'équivalence

On appelle *classe d'équivalence* d'un élément x de G pour la relation $\mathcal{R}$, le sous-ensemble formé des éléments qui sont en relation avec x, c.–à–d. l'ensemble $\{y \in G \mid x\mathcal{R}y\}$.

La classe d'équivalence de x est notée $\overline{x}$. Dans notre cas

$$\overline{x} = xH = \{y \in G : x^{-1} * y \in H\}$$

appelé *classe à gauche de x modulo H*.

Définition : classe d'équivalence

On appelle *classe d'équivalence* d'un élément x de G pour la relation $\mathcal{R}$, le sous-ensemble formé des éléments qui sont en relation avec x, c.–à–d. l'ensemble $\{y \in G \mid x\mathcal{R}y\}$.

La classe d'équivalence de x est notée $\overline{x}$. Dans notre cas

$$\overline{x} = xH = \{y \in G : x^{-1} * y \in H\}$$

appelé *classe à gauche de x modulo H*.

Quatre remarques immédiates. ① $\overline{e} = H$

② Une classe d'équivalence est toujours non vide : $\overline{x} \ni x$.

Définition : classe d'équivalence

On appelle *classe d'équivalence* d'un élément x de G pour la relation $\mathcal{R}$, le sous-ensemble formé des éléments qui sont en relation avec x, c.–à–d. l'ensemble $\{y \in G \mid x\mathcal{R}y\}$.

La classe d'équivalence de x est notée $\overline{x}$. Dans notre cas

$$\overline{x} = xH = \{y \in G : x^{-1} * y \in H\}$$

appelé *classe à gauche de x modulo H*.

Quatre remarques immédiates. ① $\overline{e} = H$

② Une classe d'équivalence est toujours non vide : $\overline{x} \ni x$.

③ Deux classes d'équivalence sont soient égales soient disjointes. Tout élément d'une classe d'équivalence détermine celle-ci : on dit que c'est un *représentant* de la classe.

Définition : classe d'équivalence

On appelle *classe d'équivalence* d'un élément x de G pour la relation $\mathcal{R}$, le sous-ensemble formé des éléments qui sont en relation avec x, c.–à–d. l'ensemble $\{y \in G \mid x\mathcal{R}y\}$.

La classe d'équivalence de x est notée $\overline{x}$. Dans notre cas

$$\overline{x} = xH = \{y \in G : x^{-1} * y \in H\}$$

appelé *classe à gauche de x modulo H*.

Quatre remarques immédiates. ① $\overline{e} = H$

② Une classe d'équivalence est toujours non vide : $\overline{x} \ni x$.

③ Deux classes d'équivalence sont soient égales soient disjointes. Tout élément d'une classe d'équivalence détermine celle-ci : on dit que c'est un *représentant* de la classe.

④ $f : H \to \overline{x}$ définie par $f(h) = x * h$ est bijective, et $\mathrm{card} H = \mathrm{card}(\overline{x})$.

Exemple

Si $G = \mathbb{Z}$ et $H = n\mathbb{Z}$, et $x, y \in G$, alors $\overline{x} = x + n\mathbb{Z}$ et

$$\overline{x} = \overline{y} \iff x \equiv y[n] \iff \exists k \in \mathbb{Z},\ x = y + kn.$$

Rappelons dans $\mathbb{Z}$: x et y sont congrus modulo n s'ils ont le même reste dans la division euclidienne par n, c.–à–d. $y - x$ est un multiple de n, ou encore n divise $y - x$.

2. Ensemble quotient

Définition

On appelle *ensemble quotient* de G par H l'ensemble des classes à gauche de $(G, *)$ modulo H. On le note G/H.

G/H se comprend comme l'ensemble obtenu lorsqu'on " identifie entre eux les éléments qui sont égaux modulo $\mathcal{R}$ " :

$$G/H = \{xH : x \in G\}.$$

Cet espace admet parfois une structure naturelle de groupe. On regardera l'exemple de $\mathbb{Z}/n\mathbb{Z}$ l'ensemble quotient de $\mathbb{Z}$ pour la relation de congruence modulo n :

$$\mathbb{Z}/n\mathbb{Z} = \{\overline{0}, \overline{1}, \ldots, \overline{(n-1)}\}.$$

3. Théorème de Lagrange

Un résultat important :

Théorème de Lagrange

Soit G un groupe fini d'ordre n et H un sous-groupe de G d'ordre p. Alors, p divise n et

$$n = \text{card}(G/H)p.$$

❄ On dit que $\text{card}(G/H)$ est l'*indice* de H : c'est le nombre de classes d'équivalence distinctes.

3. Théorème de Lagrange

Un résultat important :

Théorème de Lagrange

Soit G un groupe fini d'ordre n et H un sous-groupe de G d'ordre p. Alors, p divise n et

$$n = \text{card}(G/H)p.$$

❄ On dit que $\text{card}(G/H)$ est l'*indice* de H : c'est le nombre de classes d'équivalence distinctes.
❄ Les classes à gauche de H forment une partition de G, à savoir qu'elles forment un ensemble de parties non vides de G deux à deux disjointes qui recouvrent G.

3. Théorème de Lagrange

Un résultat important :

Théorème de Lagrange

Soit G un groupe fini d'ordre n et H un sous-groupe de G d'ordre p. Alors, p divise n et

$$n = \text{card}(G/H)p.$$

❄ On dit que $\text{card}(G/H)$ est l'*indice* de H : c'est le nombre de classes d'équivalence distinctes.

❄ Les classes à gauche de H forment une partition de G, à savoir qu'elles forment un ensemble de parties non vides de G deux à deux disjointes qui recouvrent G.

❄ Les classes à gauche de H ont toutes le même nombre d'éléments $p = \text{card}H$.

Corollaire

Soit G un groupe fini d'ordre n. Alors pour tout $a \in G$, on a $a^n = e$ et l'ordre de a divise n.

L'ordre de a est le cardinal du sous-groupe $\langle a \rangle$ (c.–à–d. l'ordre de ce sous-groupe).

Corollaire

Soit G un groupe fini d'ordre n. Alors pour tout $a \in G$, on a $a^n = e$ et l'ordre de a divise n.

L'ordre de a est le cardinal du sous-groupe $\langle a \rangle$ (c.–à–d. l'ordre de ce sous-groupe).

Exemples : groupes d'ordre 4

On pose $G = \{e, a, b, c\}$ avec e l'élément neutre. G contient des éléments d'ordre 1 (c'est e), 2 ou 4. On a alors deux cas :

1. ou bien il existe un élément d'ordre 4 (par exemple a), et dans ce cas G est un groupe cyclique (engendré par a), donc abélien,
2. ou bien a, b et c sont d'ordre 2, dans ce cas, G est encore abélien (*exo : si tous les éléments x d'un groupe vérifient $x^2 = e$, le groupe est abélien*).

Dans tous les cas, un groupe d'ordre 4 est abélien.

4. L'ensemble $\mathbb{Z}/n\mathbb{Z}$

Définition

On note $\mathbb{Z}/n\mathbb{Z}$ l'ensemble quotient de $\mathbb{Z}$ pour la relation de congruence modulo n :

$$\mathbb{Z}/n\mathbb{Z} = \{x + n\mathbb{Z} : x \in \mathbb{Z}\}.$$

4. L'ensemble $\mathbb{Z}/n\mathbb{Z}$

Définition

On note $\mathbb{Z}/n\mathbb{Z}$ l'ensemble quotient de $\mathbb{Z}$ pour la relation de congruence modulo n :

$$\mathbb{Z}/n\mathbb{Z} = \{x + n\mathbb{Z} : x \in \mathbb{Z}\}.$$

Théorème

$\mathbb{Z}/n\mathbb{Z}$ est un ensemble fini à n éléments qui sont $\overline{0}, \overline{1}, \ldots, \overline{(n-1)}$.

4. L'ensemble $\mathbb{Z}/n\mathbb{Z}$

Définition

On note $\mathbb{Z}/n\mathbb{Z}$ l'ensemble quotient de $\mathbb{Z}$ pour la relation de congruence modulo n :

$$\mathbb{Z}/n\mathbb{Z} = \{x + n\mathbb{Z} : x \in \mathbb{Z}\}.$$

Théorème

$\mathbb{Z}/n\mathbb{Z}$ est un ensemble fini à n éléments qui sont $\overline{0}, \overline{1}, \ldots, \overline{(n-1)}$.

On définit deux opérations $+$ et $\times$ sur $\mathbb{Z}/n\mathbb{Z}$ en posant

$$\bar{x} + \bar{y} \overset{\text{déf.}}{=} \overline{x+y} \quad \text{et} \quad \overline{x} \times \overline{y} \overset{\text{déf.}}{=} \overline{xy}$$

autrement dit :

$$\bar{x} + \bar{y} = \bar{z} \iff x + y \equiv z[n] \quad \text{et} \quad \bar{x} \times \bar{y} = \bar{z} \iff xy \equiv z[n].$$

Théorème

❶ $(\mathbb{Z}/n\mathbb{Z}, +)$ est un groupe abélien fini d'ordre n et de neutre $\overline{0}$. De plus, $-\overline{x} = \overline{(-x)}$ et $k\overline{x} = \overline{(kx)}$ pour tous $k \in \mathbb{Z}$ et $x \in \mathbb{Z}/n\mathbb{Z}$.

Théorème

❶ $(\mathbb{Z}/n\mathbb{Z}, +)$ est un groupe abélien fini d'ordre n et de neutre $\overline{0}$. De plus, $-\overline{x} = \overline{(-x)}$ et $k\overline{x} = \overline{(kx)}$ pour tous $k \in \mathbb{Z}$ et $x \in \mathbb{Z}/n\mathbb{Z}$.

❷ $(\mathbb{Z}/n\mathbb{Z}, +)$ est monogène : il est engendré par $\overline{1}$.

Théorème

❶ $(\mathbb{Z}/n\mathbb{Z}, +)$ est un groupe abélien fini d'ordre n et de neutre $\overline{0}$. De plus, $-\overline{x} = \overline{(-x)}$ et $k\overline{x} = \overline{(kx)}$ pour tous $k \in \mathbb{Z}$ et $x \in \mathbb{Z}/n\mathbb{Z}$.

❷ $(\mathbb{Z}/n\mathbb{Z}, +)$ est monogène : il est engendré par $\overline{1}$.

❸ Ses générateurs sont les $\overline{m}$ pour $m \in \mathbb{Z}$ premier avec n.

$(\mathbb{Z}/n\mathbb{Z}, +)$ est appelé *groupe cyclique d'ordre n* : il est monogène (engendré par un élément) et fini (d'ordre n).

Théorème

❶ $(\mathbb{Z}/n\mathbb{Z}, +)$ est un groupe abélien fini d'ordre n et de neutre $\overline{0}$. De plus, $-\overline{x} = \overline{(-x)}$ et $k\overline{x} = \overline{(kx)}$ pour tous $k \in \mathbb{Z}$ et $x \in \mathbb{Z}/n\mathbb{Z}$.

❷ $(\mathbb{Z}/n\mathbb{Z}, +)$ est monogène : il est engendré par $\overline{1}$.

❸ Ses générateurs sont les $\overline{m}$ pour $m \in \mathbb{Z}$ premier avec n.

$(\mathbb{Z}/n\mathbb{Z}, +)$ est appelé *groupe cyclique d'ordre n* : il est monogène (engendré par un élément) et fini (d'ordre n).

Exercice : $((\mathbb{Z}/n\mathbb{Z})^\star, \times)$ est un groupe si et seulement si n est premier.

IV. Morphisme de groupes

1. Définitions et propriétés

Soit $(G, *)$ et $(G', \top)$ des groupes.

Définition : Morphisme de groupes

On appelle *(homo)morphisme* du groupe $(G, *)$ vers le groupe $(G', \top)$ toute application $f : G \to G'$ vérifiant

$$\forall x, y \in G,\ f(x * y) = f(x) \top f(y).$$

IV. Morphisme de groupes

1. Définitions et propriétés

Soit $(G, *)$ et $(G', \top)$ des groupes.

Définition : Morphisme de groupes

On appelle *(homo)morphisme* du groupe $(G, *)$ vers le groupe $(G', \top)$ toute application $f : G \to G'$ vérifiant

$$\forall x, y \in G,\ f(x * y) = f(x) \top f(y).$$

- Un morphisme de G vers G est un *endomorphisme* de G.
- Un morphisme bijectif est un *isomorphisme*.
- Un endomorphisme bijectif est un *automorphisme*.

Exemples

1. L'application constante $f : G \to G$ définie par $f(x) = e$ est un endomorphisme de $(G, *)$.

Exemples

1. L'application constante $f : G \to G$ définie par $f(x) = e$ est un endomorphisme de $(G, *)$.
2. L'application identité $\mathrm{Id}_G : G \to G$ est un automorphisme de $(G, *)$.

Exemples

1. L'application constante $f : G \to G$ définie par $f(x) = e$ est un endomorphisme de $(G, *)$.
2. L'application identité $\mathrm{Id}_G : G \to G$ est un automorphisme de $(G, *)$.
3. L'application $\ln : \mathbb{R}_+^\star \to \mathbb{R}$ est un isomorphisme de $(\mathbb{R}_+^\star, \times)$ vers $(\mathbb{R}, +)$.

Exemples

1. L'application constante $f : G \to G$ définie par $f(x) = e$ est un endomorphisme de $(G, *)$.
2. L'application identité $\mathrm{Id}_G : G \to G$ est un automorphisme de $(G, *)$.
3. L'application $\ln : \mathbb{R}_+^\star \to \mathbb{R}$ est un isomorphisme de $(\mathbb{R}_+^\star, \times)$ vers $(\mathbb{R}, +)$.
4. L'application $\exp : \mathbb{C} \to \mathbb{C}^\star$ est un morphisme de $(\mathbb{C}, +)$ vers $(\mathbb{C}^\star, \times)$.

Exemples

1. L'application constante $f : G \to G$ définie par $f(x) = e$ est un endomorphisme de $(G, *)$.
2. L'application identité $\mathrm{Id}_G : G \to G$ est un automorphisme de $(G, *)$.
3. L'application $\ln : \mathbb{R}_+^\star \to \mathbb{R}$ est un isomorphisme de $(\mathbb{R}_+^\star, \times)$ vers $(\mathbb{R}, +)$.
4. L'application $\exp : \mathbb{C} \to \mathbb{C}^\star$ est un morphisme de $(\mathbb{C}, +)$ vers $(\mathbb{C}^\star, \times)$.
5. Soit $a \in G$. L'application $f : \mathbb{Z} \to G$ définie par $f(k) = a^k$ est un morphisme de $(\mathbb{Z}, +)$ vers $(G, *)$.

Exemples

1. L'application constante $f : G \to G$ définie par $f(x) = e$ est un endomorphisme de $(G, *)$.
2. L'application identité $\mathrm{Id}_G : G \to G$ est un automorphisme de $(G, *)$.
3. L'application $\ln : \mathbb{R}_+^\star \to \mathbb{R}$ est un isomorphisme de $(\mathbb{R}_+^\star, \times)$ vers $(\mathbb{R}, +)$.
4. L'application $\exp : \mathbb{C} \to \mathbb{C}^\star$ est un morphisme de $(\mathbb{C}, +)$ vers $(\mathbb{C}^\star, \times)$.
5. Soit $a \in G$. L'application $f : \mathbb{Z} \to G$ définie par $f(k) = a^k$ est un morphisme de $(\mathbb{Z}, +)$ vers $(G, *)$.
6. La surjection canonique $p : \mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ qui à x associe sa classe d'équivalence est un morphisme de groupes de $(\mathbb{Z}, +)$ vers $(\mathbb{Z}/n\mathbb{Z}, +)$.

Soit $(G, *)$ et $(G', \top)$ des groupes. Notons e le neutre de G et e' celui de G'.

Propriétés

Soit $f : G \to G'$ un morphisme de groupes.

1. Soit $(G'', \perp)$ un groupe. Si $g : G' \to G''$ est autre morphisme de groupes alors $g \circ f : G \to G''$ en est un aussi.

Soit $(G, *)$ et $(G', \top)$ des groupes. Notons e le neutre de G et e' celui de G'.

Propriétés

Soit $f : G \to G'$ un morphisme de groupes.

1. Soit $(G'', \perp)$ un groupe. Si $g : G' \to G''$ est autre morphisme de groupes alors $g \circ f : G \to G''$ en est un aussi.
2. On a $f(e) = e'$ et pour tous $x \in G$ et $n \in \mathbb{Z}$, $f(x^n) = f(x)^n$.

Soit $(G, *)$ et $(G', \top)$ des groupes. Notons e le neutre de G et e' celui de G'.

Propriétés

Soit $f : G \to G'$ un morphisme de groupes.

1. Soit $(G'', \perp)$ un groupe. Si $g : G' \to G''$ est autre morphisme de groupes alors $g \circ f : G \to G''$ en est un aussi.
2. On a $f(e) = e'$ et pour tous $x \in G$ et $n \in \mathbb{Z}$, $f(x^n) = f(x)^n$.
3. L'image directe (resp. réciproque) d'un sous-groupe par un morphisme de groupes est un sous-groupe.

Soit $(G, *)$ et $(G', \top)$ des groupes. Notons e le neutre de G et e' celui de G'.

Propriétés

Soit $f : G \to G'$ un morphisme de groupes.

1. Soit $(G'', \perp)$ un groupe. Si $g : G' \to G''$ est autre morphisme de groupes alors $g \circ f : G \to G''$ en est un aussi.
2. On a $f(e) = e'$ et pour tous $x \in G$ et $n \in \mathbb{Z}$, $f(x^n) = f(x)^n$.
3. L'image directe (resp. réciproque) d'un sous-groupe par un morphisme de groupes est un sous-groupe.
4. Si $f : G \to G'$ est un isomorphisme alors $f^{-1} : G' \to G$ aussi un isomorphisme de groupes.

2. Noyau et image

Soit $f : G \to G'$ un morphisme de groupes. On définit son *noyau* et son *image* respectivement par :

$$\operatorname{Ker} f \overset{\text{déf.}}{=} f^{-1}(\{e'\}) = \{x \in G : f(x) = e'\}$$

$$\operatorname{Im} f \overset{\text{déf.}}{=} f(G) = \{f(x) : x \in G\}.$$

Ainsi,

Corollaire

$\operatorname{Ker} f$ est un sous-groupe de G, et $\operatorname{Im} f$ est un sous-groupe de G'.

Exemple

1. Soit $f : \mathbb{C}^\star \to \mathbb{C}^\star$ le morphisme défini par $f(z) = |z|$. Alors $\operatorname{Ker} f = \mathbb{U}$ et $\operatorname{Im} f = \mathbb{R}_+^\star$.

Exemple

1. Soit $f : \mathbb{C}^\star \to \mathbb{C}^\star$ le morphisme défini par $f(z) = |z|$. Alors $\operatorname{Ker} f = \mathbb{U}$ et $\operatorname{Im} f = \mathbb{R}_+^\star$.
2. Pour $\exp : \mathbb{C} \to \mathbb{C}^\star$ morphisme de $(\mathbb{C}, +)$ vers $(\mathbb{C}^\star, \times)$, on a $\operatorname{Ker}(\exp) = 2i\pi\mathbb{Z}$ et $\operatorname{Im}(\exp) = \mathbb{C}^\star$.

Exemple

1. Soit $f : \mathbb{C}^\star \to \mathbb{C}^\star$ le morphisme défini par $f(z) = |z|$. Alors $\text{Ker}\, f = \mathbb{U}$ et $\text{Im}\, f = \mathbb{R}_+^\star$.
2. Pour $\exp : \mathbb{C} \to \mathbb{C}^\star$ morphisme de $(\mathbb{C}, +)$ vers $(\mathbb{C}^\star, \times)$, on a $\text{Ker}(\exp) = 2i\pi\mathbb{Z}$ et $\text{Im}(\exp) = \mathbb{C}^\star$.
3. Pour $\det : GL(n, \mathbb{K}) \to \mathbb{K}^\star$ morphisme de $(GL(n, \mathbb{K}), .)$ vers $(\mathbb{K}^\star, \times)$, on a $\text{Ker}(\det) = SL(n, \mathbb{K})$ et $\text{Im}(\det) = \mathbb{K}^\star$.

Exemple

1. Soit $f : \mathbb{C}^\star \to \mathbb{C}^\star$ le morphisme défini par $f(z) = |z|$. Alors $\text{Ker } f = \mathbb{U}$ et $\text{Im } f = \mathbb{R}_+^\star$.
2. Pour $\exp : \mathbb{C} \to \mathbb{C}^\star$ morphisme de $(\mathbb{C}, +)$ vers $(\mathbb{C}^\star, \times)$, on a $\text{Ker}(\exp) = 2i\pi\mathbb{Z}$ et $\text{Im}(\exp) = \mathbb{C}^\star$.
3. Pour $\det : GL(n, \mathbb{K}) \to \mathbb{K}^\star$ morphisme de $(GL(n, \mathbb{K}), .)$ vers $(\mathbb{K}^\star, \times)$, on a $\text{Ker}(\det) = SL(n, \mathbb{K})$ et $\text{Im}(\det) = \mathbb{K}^\star$.

Propiétés

Soit $f : G \to G'$ un morphisme de groupes.

1. $f : G \to G'$ est injective si et seulement si $\text{Ker } f = \{e\}$.

Exemple

1. Soit $f : \mathbb{C}^\star \to \mathbb{C}^\star$ le morphisme défini par $f(z) = |z|$. Alors $\text{Ker } f = \mathbb{U}$ et $\text{Im } f = \mathbb{R}_+^\star$.
2. Pour $\exp : \mathbb{C} \to \mathbb{C}^\star$ morphisme de $(\mathbb{C}, +)$ vers $(\mathbb{C}^\star, \times)$, on a $\text{Ker}(\exp) = 2i\pi\mathbb{Z}$ et $\text{Im}(\exp) = \mathbb{C}^\star$.
3. Pour $\det : GL(n, \mathbb{K}) \to \mathbb{K}^\star$ morphisme de $(GL(n, \mathbb{K}), .)$ vers $(\mathbb{K}^\star, \times)$, on a $\text{Ker}(\det) = SL(n, \mathbb{K})$ et $\text{Im}(\det) = \mathbb{K}^\star$.

Propiétés

Soit $f : G \to G'$ un morphisme de groupes.

1. $f : G \to G'$ est injective si et seulement si $\text{Ker } f = \{e\}$.
2. $f : G \to G'$ est surjective si et seulement si $\text{Im } f = G'$.

3. Groupes isomorphes

Définition : Groupes isomorphes

On dit que deux groupes sont *isomorphes* s'il existe un isomorphisme de l'un vers l'autre.

3. Groupes isomorphes

Définition : Groupes isomorphes

On dit que deux groupes sont *isomorphes* s'il existe un isomorphisme de l'un vers l'autre.

Exemples

1. $(\mathbb{R}_+^\star, \times)$ et $(\mathbb{R}, +)$ sont isomorphes.

   $(\mathbb{R}^\star, \times)$ et $(\mathbb{R}, +)$ ne sont pas isomorphes.
2. $(\mathbb{Z}/n\mathbb{Z}, +)$ et $(\mathbb{U}_n, \times)$ sont isomorphes.

3. Groupes isomorphes

Définition : Groupes isomorphes

On dit que deux groupes sont *isomorphes* s'il existe un isomorphisme de l'un vers l'autre.

Exemples

1. $(\mathbb{R}_+^\star, \times)$ et $(\mathbb{R}, +)$ sont isomorphes.
   $(\mathbb{R}^\star, \times)$ et $(\mathbb{R}, +)$ ne sont pas isomorphes.
2. $(\mathbb{Z}/n\mathbb{Z}, +)$ et $(\mathbb{U}_n, \times)$ sont isomorphes.

Théorème

Soit $(G, *)$ un groupe monogène.
Si G est fini d'ordre $n \in \mathbb{N}^\star$, $(G, *)$ est isomorphe à $(\mathbb{Z}/n\mathbb{Z}, +)$.
Si G est infini, $(G, *)$ est isomorphe à $(\mathbb{Z}, +)$

4. Notions sur les actions de groupes

Soit $(G, *)$ un groupe et X un ensemble non vide.

Définition

On dit que G *agit (à gauche) sur* X s'il existe une application $\varphi : G \times X \to X$, $(g, x) \mapsto g \cdot x$ qui vérifie :

1. $\forall x \in X,\ e \cdot x = x$
2. $\forall g_1, g_2 \in G,\ \forall x \in X,\ g_1 \cdot (g_2 \cdot x) = (g_1 * g_2) \cdot x.$

On dit que φ est une *action (à gauche) de* G *sur* X.

4. Notions sur les actions de groupes

Soit $(G, *)$ un groupe et X un ensemble non vide.

Définition

On dit que G *agit (à gauche) sur* X s'il existe une application $\varphi : G \times X \to X$, $(g, x) \mapsto g \cdot x$ qui vérifie :

1. $\forall x \in X,\ e \cdot x = x$
2. $\forall g_1, g_2 \in G, \forall x \in X,\ g_1 \cdot (g_2 \cdot x) = (g_1 * g_2) \cdot x.$

On dit que φ est une *action (à gauche) de* G *sur* X.

Remarques. (1) G agit sur X si, et seulement si, il existe un morphisme $\Phi : G \to \mathcal{S}(X)$. L'action de G sur X est alors donnée par $g \cdot x = \Phi(g)(x)$.

4. Notions sur les actions de groupes

Soit $(G, *)$ un groupe et X un ensemble non vide.

Définition

On dit que G *agit (à gauche) sur* X s'il existe une application $\varphi : G \times X \to X$, $(g, x) \mapsto g \cdot x$ qui vérifie :

1. $\forall x \in X,\ e \cdot x = x$
2. $\forall g_1, g_2 \in G,\ \forall x \in X,\ g_1 \cdot (g_2 \cdot x) = (g_1 * g_2) \cdot x.$

On dit que φ est une *action (à gauche) de* G *sur* X.

Remarques. (1) G agit sur X si, et seulement si, il existe un morphisme $\Phi : G \to \mathcal{S}(X)$. L'action de G sur X est alors donnée par $g \cdot x = \Phi(g)(x)$.
(2) Si G agit sur X, tout sous-groupe de G agit sur X.

Définition

On dit que l'action de G sur X est *fidèle* si le morphisme de groupes $\Phi : G \to \mathcal{S}(X)$, $\Phi(g)(x) = g \cdot x$, est injectif.

Conséquence. Une action fidèle permet d'identifier G à un sous-groupe du groupe des permutations $\mathcal{S}(X)$.

Exemples

1. **Action par translation à gauche.** G agit sur lui-même par translation à gauche : $(g, x) \in G \times G \mapsto g * x$.

Définition

On dit que l'action de G sur X est *fidèle* si le morphisme de groupes $\Phi : G \to \mathcal{S}(X)$, $\Phi(g)(x) = g \cdot x$, est injectif.

Conséquence. Une action fidèle permet d'identifier G à un sous-groupe du groupe des permutations $\mathcal{S}(X)$.

Exemples

1. **Action par translation à gauche.** G agit sur lui-même par translation à gauche : $(g, x) \in G \times G \mapsto g * x$.

Théorème de Cayley

L'action de G sur lui-même par translation à gauche est fidèle, et G est isomorphe à un sous-groupe de $(\mathcal{S}(G), \circ)$.

En particulier, si G est un groupe fini d'ordre n, il est isomorphe à un sous-groupe de $\mathcal{S}_n$.

❷ Action par conjugaison.

G agit sur lui-même par conjugaison :

$$(g, x) \in G \times G \mapsto g * x * g^{-1}.$$

❷ Action par conjugaison.

G agit sur lui-même par conjugaison :

$$(g, x) \in G \times G \mapsto g * x * g^{-1}.$$

G agit sur l'ensemble X des sous-groupes de G par conjugaison :

$$(g, H) \in G \times X \mapsto gHg^{-1}.$$

L'action n'est pas fidèle.

❷ Action par conjugaison.

G agit sur lui-même par conjugaison :

$$(g, x) \in G \times G \mapsto g * x * g^{-1}.$$

G agit sur l'ensemble X des sous-groupes de G par conjugaison :

$$(g, H) \in G \times X \mapsto gHg^{-1}.$$

L'action n'est pas fidèle.

❷ Action par conjugaison.

G agit sur lui-même par conjugaison :

$$(g, x) \in G \times G \mapsto g * x * g^{-1}.$$

G agit sur l'ensemble X des sous-groupes de G par conjugaison :

$$(g, H) \in G \times X \mapsto gHg^{-1}.$$

L'action n'est pas fidèle.

❸ Soit E un ensemble non vide. $\mathcal{S}(E)$ agit fidèlement sur E par l'action $(f, x) \mapsto f(x)$.

Soit un groupe G agissant sur un ensemble non vide X.

Définition

On appelle *stabilisateur de* x l'ensemble

$$G_x = \{g \in G \mid g \cdot x = x\}.$$

Proposition

Pour tout $x \in X$, G_x est un sous-groupe de G.

Soit un groupe G agissant sur un ensemble X. On définit la relation binaire sur G suivante pour $x, y \in X$

$$x \mathcal{R} y \overset{\text{déf.}}{\iff} \exists g \in G,\ y = g \cdot x.$$

Soit un groupe G agissant sur un ensemble X. On définit la relation binaire sur G suivante pour $x, y \in X$

$$x \mathcal{R} y \overset{\text{déf.}}{\iff} \exists g \in G,\ y = g \cdot x.$$

Propriété - Définition

$\mathcal{R}$ est une **relation d'équivalence** et les classes d'équivalence $G \cdot x = \{y \in X \mid \exists g \in G,\ y = g \cdot x\}$ sont appelés les *orbites de x selon G*. Elles forment une partition de X.
On dit qu'une action est *transitive* si il n'existe qu'une seule orbite selon G.

Soit un groupe G agissant sur un ensemble X. On définit la relation binaire sur G suivante pour $x, y \in X$

$$x \mathcal{R} y \overset{\text{déf.}}{\iff} \exists g \in G,\ y = g \cdot x.$$

Propriété - Définition

$\mathcal{R}$ est une **relation d'équivalence** et les classes d'équivalence $G \cdot x = \{y \in X \mid \exists g \in G,\ y = g \cdot x\}$ sont appelés les *orbites de x selon G*. Elles forment une partition de X.
On dit qu'une action est *transitive* si il n'existe qu'une seule orbite selon G.

Proposition

Soit G un groupe agissant sur un ensemble X et $x \in X$. Alors, il existe une bijection entre l'orbite $G \cdot x$ de x et l'ensemble des classes à gauche de G modulo G_x.