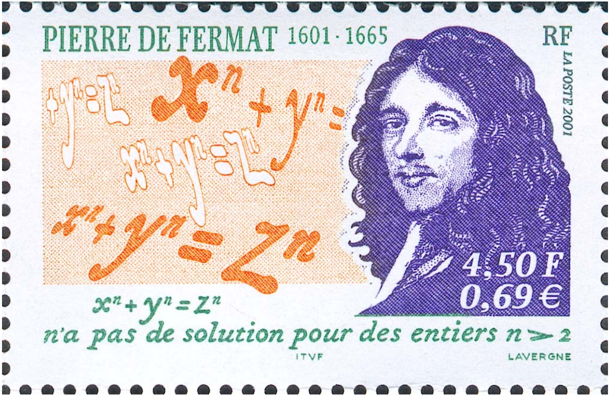

Leçon 40 - Groupes

5 décembre 2024

Problèmes

Problème Structure

Problèmes

Problème Structure

Problème Résolution des équations polynomiales

Problèmes

Problème Structure

Problème Résolution des équations polynomiales

Problème Groupe de Poincaré

Problèmes

Problème Structure

Problème Résolution des équations polynomiales

Problème Groupe de Poincaré

Problème Mariage chez les Murgin

Loi interne (opération)

Définition - Loi de composition interne

Une loi de composition interne sur un ensemble E est une application de $E\times E$ dans E : $\Phi\ : E\times E \to E, (x,y)\mapsto x\star y$.
On note, pour $(x,y,z)\in E^3$,

$$(x\star y)\star z = \Phi(\Phi(x,y),z) \text{ et } x\star(y\star z) = \Phi(x,\Phi(y,z)).$$

Un tel couple $(E,\star)$ est appelé un magma.
Quand la loi interne est clairement identifiée, par abus, on peut dire que E est un magma sans précision supplémentaire.

Loi interne (opération)

Définition - Loi de composition interne

Une loi de composition interne sur un ensemble E est une application de $E \times E$ dans E : $\Phi\ : E \times E \to E, (x,y) \mapsto x \star y$.
On note, pour $(x,y,z) \in E^3$,

$$(x \star y) \star z = \Phi(\Phi(x,y),z) \text{ et } x \star (y \star z) = \Phi(x, \Phi(y,z)).$$

Un tel couple $(E, \star)$ est appelé un magma.
Quand la loi interne est clairement identifiée, par abus, on peut dire que E est un magma sans précision supplémentaire.

Exemple - $\mathbb{N}$.

Vocabulaire

Définition - Caractéristiques

On dit que le magma $(E,\star)$: $\star$:

- est *commutatif* si $\forall (x,y) \in E \times E, x \star y = y \star x$
- est *associatif* si $\forall (x,y,z) \in E \times E \times E, x \star (y \star z) = (x \star y) \star z$
- est unifère ou possède un élément *neutre* s'il existe $e \in E$ tel que $\forall x \in E, e \star x = x \star e = x$ (e est alors l'élément neutre.)

Pour x élément de E, on dit qu'un élément y de E est un *symétrique* ou un *inverse* de x pour $\star$ si $x \star y = y \star x = e$, où e est élément neutre.

Vocabulaire

Définition - Caractéristiques

On dit que le magma $(E,\star)$: $\star$:

- est *commutatif* si $\forall (x,y)\in E\times E, x\star y = y\star x$
- est *associatif* si $\forall (x,y,z)\in E\times E\times E, x\star(y\star z) = (x\star y)\star z$
- est unifère ou possède un élément *neutre* s'il existe $e\in E$ tel que $\forall x\in E, e\star x = x\star e = x$ (e est alors l'élément neutre.)

Pour x élément de E, on dit qu'un élément y de E est un *symétrique* ou un *inverse* de x pour $\star$ si $x\star y = y\star x = e$, où e est élément neutre.

Definition - Monoïde

Un magma $(M,\star)$ associatif et unifère est appelé un monoïde.

Remarques

Remarque Notations

Plusieurs remarques

Remarques

Remarque Notations

Plusieurs remarques

1. Les lois de composition interne sont usuellement notées $\star$, $\perp$, $\top$, $+$, $\times$, en notation multiplicative $x \star y = xy$.

Remarques

Remarque Notations
Plusieurs remarques

1. Les lois de composition interne sont usuellement notées $\star$, $\perp$, $\top$, $+$, $\times$, en notation multiplicative $x \star y = xy$.
2. La notation additive est usuellement réservée à une loi commutative et associative, dans ce cas le symétrique de x (s'il existe) est noté $-x$.

Remarques

Remarque Notations

Plusieurs remarques

1. Les lois de composition interne sont usuellement notées $\star$, $\perp$, $\top$, $+$, $\times$, en notation multiplicative $x \star y = xy$.
2. La notation additive est usuellement réservée à une loi commutative et associative, dans ce cas le symétrique de x (s'il existe) est noté $-x$.
3. Lorsque la loi est commutative et associative, on peut écrire :

   $\sum_{i=1}^{n} x_i = x_1 + \cdots + x_n$ (notation additive)

   ou $\prod_{i=1}^{n} x_i = x_1 \ldots x_n$ (notation multiplicative).

Remarques

Remarque Notations

Plusieurs remarques

1. Les lois de composition interne sont usuellement notées $\star$, $\perp$, $\top$, $+$, $\times$, en notation multiplicative $x \star y = xy$.
2. La notation additive est usuellement réservée à une loi commutative et associative, dans ce cas le symétrique de x (s'il existe) est noté $-x$.
3. Lorsque la loi est commutative et associative, on peut écrire :
   $\sum_{i=1}^{n} x_i = x_1 + \cdots + x_n$ (notation additive)
   ou $\prod_{i=1}^{n} x_i = x_1 \dots x_n$ (notation multiplicative).
4. Si la loi $\star$ est associative, on peut écrire $x^{\star n} = x \star \cdots \star x$ (n termes x), en notation multiplicative on obtient ainsi x^n et en notation additive nx.

Distributivité

Définition - Distributivité

Supposons que l'ensemble E est muni de deux lois internes $\star$ et $\top$.

On dit que $\star$ est *distributive* par rapport à la loi interne $\top$ si : $\forall (x,y,z) \in K^3$

- $x \star (y \top z) = (x \star y) \top (x \star z)$ (distributive à gauche)
- $(x \top y) \star z = (x \star z) \top (y \star z)$ (distributive à droite)

Premières propriétés

Proposition - Unicités (éléments neutres, symétrique)...si existence

Soit $(F, \top)$ un magma.

Si F est unifère, l'élément neutre pour $\top$ est unique.

Soit $(E, \star)$ un monoïde.

Si $x \in E$ admet un symétrique alors celui-ci est unique ;

Si $x, y \in E$ admettent des symétriques x^{-1} et y^{-1}
alors $x \star y$ admet un symétrique : $y^{-1} \star x^{-1}$.

Si x est symétrique alors x est régulier (à gauche et à droite) :
$\forall\ y, z \in E, x \star y = x \star z \Rightarrow y = z$ et $y \star x = z \star x \Rightarrow y = z$.

Premières propriétés

Proposition - Unicités (éléments neutres, symétrique)...si existence

Soit $(F,\top)$ un magma.

Si F est unifère, l'élément neutre pour $\top$ est unique.

Soit $(E,\star)$ un monoïde.

Si $x\in E$ admet un symétrique alors celui-ci est unique ;

Si $x,y\in E$ admettent des symétriques x^{-1} et y^{-1} alors $x\star y$ admet un symétrique : $y^{-1}\star x^{-1}$.

Si x est symétrique alors x est régulier (à gauche et à droite) :
$\forall\ y,z\in E,\ x\star y = x\star z \Rightarrow y=z$ et $y\star x = z\star x \Rightarrow y=z$.

Démonstration

⇒ Reconnaitre les groupes
1. Problèmes
2. Lois de composition internes
2.1. Définitions
2.2. Propriétés
2.3. Induction
3. Structure de groupe
3.1. Def & Prop
3.2. Groupes produits
3.3. Exemples

Loi induite

Définition - Loi induite

Soit $A \subset E$, avec $(E, \top)$ magma.

<u>A est stable par $\top$</u> (loi de composition interne sur E) si

$\forall x, y \in A, x \top y \in A$.

$\top_A = \top_{|A \times A}$ s'appelle la loi induite (par $\top$ sur A).

Loi induite

Définition - Loi induite

Soit $A \subset E$, avec $(E, \top)$ magma.
A est stable par $\top$ (loi de composition interne sur E) si $\forall x, y \in A, x \top y \in A$.
$\top_A = \top_{|A\times A}$ s'appelle la loi induite (par $\top$ sur A).

Remarque Transmission des propriétés

Définition et régularité

Définition - Groupe

On appelle groupe un ensemble G muni d'une loi de composition interne $\top$ vérifiant :

- la loi $\top$ est associative ;
- G possède un élément neutre pour $\top$;
- tout élément x de G possède un symétrique pour $\top$ (ou tout élément de G est inversible, est symétrisable).

Si de plus la loi $\top$ est commutative, on dit que le groupe est abélien (ou commutatif).

Définition et régularité

Définition - Groupe

On appelle groupe un ensemble G muni d'une loi de composition interne $\top$ vérifiant :

- la loi $\top$ est associative ;
- G possède un élément neutre pour $\top$;
- tout élément x de G possède un symétrique pour $\top$ (ou tout élément de G est inversible, est symétrisable).

Si de plus la loi $\top$ est commutative, on dit que le groupe est abélien (ou commutatif).

Exemple Groupes des racines de l'unité

Définition et régularité

Définition - Groupe

On appelle groupe un ensemble G muni d'une loi de composition interne $\top$ vérifiant :

- la loi $\top$ est associative ;
- G possède un élément neutre pour $\top$;
- tout élément x de G possède un symétrique pour $\top$ (ou tout élément de G est inversible, est symétrisable).

Si de plus la loi $\top$ est commutative, on dit que le groupe est abélien (ou commutatif).

Exemple Groupes des racines de l'unité

Remarque Sous-groupe

Régularité

Proposition - Régularité

Dans un groupe tous les éléments sont réguliers à gauche et à droite

Régularité

Proposition - Régularité

Dans un groupe tous les éléments sont réguliers à gauche et à droite

Démonstration

Propriétés immédiates

Comme les groupes sont des magmas infères, où tous les éléments sont inversibles. Nécessairement :

Propriétés immédiates

Comme les groupes sont des magmas infères, où tous les éléments sont inversibles. Nécessairement :

Théorème - Existence et unicité

Soit $(G, \top)$ un groupe. Alors :

- L'élément neutre est unique.
- Tout élément possède un unique symétrique.
- En notant x^{-1} le symétrique (l'inverse) de x, on a $(x^{-1})^{-1} = x$.
- $(x \top y)^{-1} = y^{-1} \top x^{-1}$.

Définition

Définition - Produit de groupes

Soient $(G, \perp)$ et $(H, \top)$ deux groupes.
On appelle groupe produit (de ces deux groupes), le groupe $(G \times H, \star)$ tel que :

$$\forall\ (x_1, y_1)(x_2, y_2) \in G \times H \qquad (x_1, y_1) \star (x_2, y_2) = (x_1 \perp x_2, y_1 \top y_2)$$

Définition

Définition - Produit de groupes

Soient $(G, \perp)$ et $(H, \top)$ deux groupes.
On appelle groupe produit (de ces deux groupes), le groupe $(G \times H, \star)$ tel que :

$$\forall\ (x_1, y_1)(x_2, y_2) \in G \times H \qquad (x_1, y_1) \star (x_2, y_2) = (x_1 \perp x_2, y_1 \top y_2)$$

Il s'agit bien d'un groupe

Définition

Définition - Produit de groupes

Soient $(G, \perp)$ et $(H, \top)$ deux groupes.
On appelle groupe produit (de ces deux groupes), le groupe $(G \times H, \star)$ tel que :

$$\forall\ (x_1, y_1)(x_2, y_2) \in G \times H \qquad (x_1, y_1) \star (x_2, y_2) = (x_1 \perp x_2, y_1 \top y_2)$$

Il s'agit bien d'un groupe

Démonstration

Définition

Définition - Produit de groupes

Soient $(G, \perp)$ et $(H, \top)$ deux groupes.
On appelle groupe produit (de ces deux groupes), le groupe $(G \times H, \star)$ tel que :

$$\forall\ (x_1, y_1)(x_2, y_2) \in G \times H \qquad (x_1, y_1) \star (x_2, y_2) = (x_1 \perp x_2, y_1 \top y_2)$$

Il s'agit bien d'un groupe

Démonstration

Remarque - Souvent $G = H$.

Groupes triviaux

Exemple Avec l'addition

Groupes triviaux

Exemple Avec l'addition

Exemple Avec la multiplication

Ensemble $\dfrac{\mathbb{Z}}{n\mathbb{Z}}$

Définition - Ensemble des classes d'équivalence modulo n

Soit $n \in \mathbb{N}$, fixé.

La relation $\equiv_n$ ou encore $\cdot \equiv \cdot [n]$ est une relation d'équivalence sur $\mathbb{Z}$.

L'ensemble des classes d'équivalence associées est noté $\dfrac{\mathbb{Z}}{n\mathbb{Z}}$.

Un système de représentant est $[\![0, n-1]\!]$ puisque $\dfrac{\mathbb{Z}}{n\mathbb{Z}} = \{\overline{0}, \overline{1}, \cdots, \overline{n-1}\}$ où pour tout $k \in [\![0, n-1]\!]$,
$\overline{k} = \{k, k+n, k+2n, \ldots, k-n, k-2n, \ldots\} = \{k + rn, r \in \mathbb{Z}\}$.

On peut alors définir sur $\dfrac{\mathbb{Z}}{n\mathbb{Z}}$ les lois $\overline{+}$ et $\overline{\times}$ par :

$$\overline{h}\,\overline{+}\,\overline{k} = \overline{h+k} \qquad \overline{h}\,\overline{\times}\,\overline{k} = \overline{h \times k}$$

Ensemble $\dfrac{\mathbb{Z}}{n\mathbb{Z}}$

Définition - Ensemble des classes d'équivalence modulo n

Soit $n \in \mathbb{N}$, fixé.

La relation $\equiv_n$ ou encore $\cdot \equiv \cdot [n]$ est une relation d'équivalence sur $\mathbb{Z}$.

L'ensemble des classes d'équivalence associées est noté $\dfrac{\mathbb{Z}}{n\mathbb{Z}}$.

Un système de représentant est $[\![0, n-1]\!]$ puisque $\dfrac{\mathbb{Z}}{n\mathbb{Z}} = \{\overline{0}, \overline{1}, \cdots, \overline{n-1}\}$ où pour tout $k \in [\![0, n-1]\!]$,
$\overline{k} = \{k, k+n, k+2n, \ldots, k-n, k-2n, \ldots\} = \{k + rn, r \in \mathbb{Z}\}$.

On peut alors définir sur $\dfrac{\mathbb{Z}}{n\mathbb{Z}}$ les lois $\overline{+}$ et $\overline{\times}$ par :

$$\overline{h}\,\overline{+}\,\overline{k} = \overline{h+k} \qquad \overline{h}\,\overline{\times}\,\overline{k} = \overline{h \times k}$$

Remarque Le plus dur dans ce qui précède

Groupe $\left(\frac{\mathbb{Z}}{n\mathbb{Z}}, \overline{+}\right)$

Proposition - Groupe $\left(\frac{\mathbb{Z}}{n\mathbb{Z}}, \overline{+}\right)$

Pour tout entier $n \in \mathbb{N}^*$, $\left(\frac{\mathbb{Z}}{n\mathbb{Z}}, \overline{+}\right)$ est un groupe commutatif.
Son élément neutre est $\overline{0}$ et l'opposé de $\overline{k}$ est $\overline{n-k}$.

Groupe $\left(\frac{\mathbb{Z}}{n\mathbb{Z}}, \overline{+}\right)$

Proposition - Groupe $\left(\frac{\mathbb{Z}}{n\mathbb{Z}}, \overline{+}\right)$

Pour tout entier $n \in \mathbb{N}^*$, $\left(\frac{\mathbb{Z}}{n\mathbb{Z}}, \overline{+}\right)$ est un groupe commutatif.

Son élément neutre est $\overline{0}$ et l'opposé de $\overline{k}$ est $\overline{n-k}$.

Démonstration

Groupe $\left(\frac{\mathbb{Z}}{n\mathbb{Z}}, \overline{\times}\right)$?

Analyse Et pour la multiplication $\overline{\times}$?

Groupe $\left(\frac{\mathbb{Z}}{n\mathbb{Z}}, \overline{\times}\right)$?

Analyse Et pour la multiplication $\overline{\times}$?

Proposition - Groupe $\left(\frac{\mathbb{Z}}{p\mathbb{Z}}^*, \overline{\times}\right)$, avec p premier

Pour tout nombre premier p, $\left(\frac{\mathbb{Z}}{p\mathbb{Z}}^*, \overline{\times}\right)$ est un groupe commutatif.
Son élément neutre est $\overline{1}$ et l'opposé de $\overline{k}$ est obtenu en exploitant le théorème de Bézout (ou autre).

Groupe $\left(\frac{\mathbb{Z}}{n\mathbb{Z}}, \overline{\times}\right)$?

Analyse Et pour la multiplication $\overline{\times}$?

Proposition - Groupe $\left(\frac{\mathbb{Z}}{p\mathbb{Z}}^*, \overline{\times}\right)$, avec p premier

Pour tout nombre premier p, $\left(\frac{\mathbb{Z}}{p\mathbb{Z}}^*, \overline{\times}\right)$ est un groupe commutatif.
Son élément neutre est $\overline{1}$ et l'opposé de $\overline{k}$ est obtenu en exploitant le théorème de Bézout (ou autre).

<u>Exercice</u>

A démontrer

Groupe $\left(\frac{\mathbb{Z}}{n\mathbb{Z}}, \overline{\times}\right)$?

Analyse Et pour la multiplication $\overline{\times}$?

Proposition - Groupe $\left(\frac{\mathbb{Z}}{p\mathbb{Z}}^{*}, \overline{\times}\right)$, avec p premier

Pour tout nombre premier p, $\left(\frac{\mathbb{Z}}{p\mathbb{Z}}^{*}, \overline{\times}\right)$ est un groupe commutatif.

Son élément neutre est $\overline{1}$ et l'opposé de $\overline{k}$ est obtenu en exploitant le théorème de Bézout (ou autre).

Exercice

A démontrer

Remarque Autre point de vue.

« Petits »groupes

Analyse Groupe à deux éléments

« Petits »groupes

Analyse Groupe à deux éléments

Exercice

Construire un groupe de 3 éléments

Groupes matriciels

$(\mathscr{M}_{n,p}(\mathbb{K}), +)$ est un groupe ?

Groupes matriciels

$(\mathscr{M}_{n,p}(\mathbb{K}), +)$ est un groupe ?
$(\mathscr{M}_n(\mathbb{K}), \times)$ est un groupe ?

Groupes matriciels

$(\mathscr{M}_{n,p}(\mathbb{K}), +)$ est un groupe ?
$(\mathscr{M}_n(\mathbb{K}), \times)$ est un groupe ?
$(GL_n(\mathbb{K}), \times)$? oui !

Groupes matriciels

$(\mathscr{M}_{n,p}(\mathbb{K}), +)$ est un groupe ?
$(\mathscr{M}_n(\mathbb{K}), \times)$ est un groupe ?
  $(GL_n(\mathbb{K}), \times)$? oui !
Autre exemple $(\mathscr{O}_n(\mathbb{K}), \times)$? où $M \in \mathscr{O}_n(\mathbb{K})$ ssi $M^T \times M = I_n$

Groupes des permutations

Un groupe très important, on reviendra sur cette notion plus tard. . .

Proposition - Groupe des permutations d'un ensemble

Soit X un ensemble non vide. On note S_X l'ensemble des permutations de X (c'est-à-dire des bijections de X dans X). Alors $(S_X, \circ)$ est un groupe, généralement non commutatif, appelé groupe des permutations de X.

Groupes des permutations

Un groupe très important, on reviendra sur cette notion plus tard. . .

Proposition - Groupe des permutations d'un ensemble

Soit X un ensemble non vide. On note S_X l'ensemble des permutations de X (c'est-à-dire des bijections de X dans X). Alors $(S_X, \circ)$ est un groupe, généralement non commutatif, appelé groupe des permutations de X.

Remarque Permutation

Qu'est-ce qu'une permutation de X ?

Groupes des permutations

Un groupe très important, on reviendra sur cette notion plus tard...

Proposition - Groupe des permutations d'un ensemble

Soit X un ensemble non vide. On note S_X l'ensemble des permutations de X (c'est-à-dire des bijections de X dans X). Alors $(S_X, \circ)$ est un groupe, généralement non commutatif, appelé groupe des permutations de X.

Remarque Permutation

Qu'est-ce qu'une permutation de X ?

Démonstration

Groupes et géométrie

Proposition - Groupes des similitudes directes du plan $\mathbb{C}$

L'ensemble des similitudes directes est un groupe pour la loi $\circ$.
L'élément neutre est l'identité.
L'inverse de la similitude de centre Ω, d'angle θ et de rapport k est la similitude de centre Ω, d'angle $-\theta$ et de rapport $\frac{1}{k}$.
L'inverse de la translation de vecteur $\overrightarrow{u}$ est la translation de vecteur $-\overrightarrow{u}$.

Groupes et géométrie

Proposition - Groupes des similitudes directes du plan $\mathbb{C}$

L'ensemble des similitudes directes est un groupe pour la loi $\circ$.
L'élément neutre est l'identité.
L'inverse de la similitude de centre Ω, d'angle θ et de rapport k est la similitude de centre Ω, d'angle $-\theta$ et de rapport $\frac{1}{k}$.
L'inverse de la translation de vecteur $\overrightarrow{u}$ est la translation de vecteur $-\overrightarrow{u}$.

Démonstration

Conclusion

Objectifs

⇒ Reconnaître les groupes

Conclusion

Objectifs

$\Rightarrow$ Reconnaître les groupes

- Définition avec une certaine stabilité opératoire et passage à l'inverse

Conclusion

Objectifs

$\Rightarrow$ Reconnaître les groupes

- Définition avec une certaine stabilité opératoire et passage à l'inverse
- De très nombreux exemples.

Conclusion

Objectifs

⇒ Reconnaître les groupes

- Définition avec une certaine stabilité opératoire et passage à l'inverse
- De très nombreux exemples.

Conclusion

Objectifs

$\Rightarrow$ Reconnaître les groupes

- Définition avec une certaine stabilité opératoire et passage à l'inverse
- De très nombreux exemples.

Conclusion

Objectifs

⇒ Reconnaître les groupes

- Définition avec une certaine stabilité opératoire et passage à l'inverse
- De très nombreux exemples.

Pour la prochaine fois

- Lecture du cours : chapitre 13 - Groupes
- Exercices N°267 & 270