HAX501X – Groupes et anneaux 1

CM7 29/09/2023

Clément Dupont

Morphismes de groupes

Définition

Soient deux groupes $(G, *)$ et $(H, \#)$. Un **morphisme de groupes** *de G dans H est une application $f : G \to H$ qui vérifie :*

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

Remarque

En notation multiplicative, on écrit plutôt $f(xy) = f(x)f(y)$.

Définition

Un **endomorphisme** *d'un groupe G est un morphisme de groupes de G dans G.*

Propriétés de base des morphismes de groupes

Proposition

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

1) *Si l'on note e_G et e_H les élément neutres respectifs de G et H, on a $f(e_G) = e_H$.*
2) *Pour tout $x \in G$, $f(x^{-1}) = f(x)^{-1}$.*

Proposition

Soient $f : G \to H$ et $g : H \to K$ deux morphismes de groupes. Alors la composée $g \circ f : G \to K$ est un morphisme de groupes.

Deux exercices

Exercice 42
Lister tous les morphismes de groupes de $\mathbb{Z}/3\mathbb{Z}$ dans $\mathbb{Z}/4\mathbb{Z}$. Lister tous les endomorphismes de $\mathbb{Z}/3\mathbb{Z}$.

Exercice 43
Montrer que les endomorphismes de $\mathbb{Z}$ sont les applications $k \mapsto ak$ avec $a \in \mathbb{Z}$. Pour $n \in \mathbb{N}^*$, montrer que les endomorphismes de $\mathbb{Z}/n\mathbb{Z}$ sont les applications $\overline{k} \mapsto \overline{ak} = \overline{a} \times \overline{k}$, avec $\overline{a} \in \mathbb{Z}/n\mathbb{Z}$.

Morphismes de groupes et sous-groupes

Proposition

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

1) *Soit* H' *un sous-groupe de* H. *Alors l'image réciproque* $f^{-1}(H')$ *est un sous-groupe de* G.
2) *Soit* G' *un sous-groupe de* G. *Alors l'image directe* $f(G')$ *est un sous-groupe de* H.

Noyau et image

Définition

Soit $f : G \to H$ *un morphisme de groupes. On appelle* **noyau** *de* f *et on note* $\ker(f)$ *le sous-ensemble*

$$\ker(f) = \{x \in G \,|\, f(x) = e_H\},$$

où e_H *désigne l'élément neutre de* H*.*

On rappelle aussi la notation

$$\mathrm{Im}(f) = f(G) = \{f(x),\, x \in G\}.$$

Proposition

Soit $f : G \to H$ *un morphisme de groupes. Alors* $\ker(f)$ *est un sous-groupe de* G *et* $\mathrm{Im}(f)$ *est un sous-groupe de* H*.*

Proposition

Soit $f : G \to H$ *un morphisme de groupes. Alors* f *est injectif si et seulement si* $\ker(f) = \{e_G\}$*, où* e_G *désigne l'élément neutre de* G*.*

Isomorphismes de groupes

Définition

Soient deux groupes G et H. Un **isomorphisme de groupes** *de G dans H est un morphisme de groupes bijectif de G dans H. S'il existe un isomorphisme de groupes de G dans H on dit que G est* **isomorphe** *à H, ou que G et H sont isomorphes, et on note $G \simeq H$.*

- La proposition suivante montre que si $G \simeq H$ alors $H \simeq G$.

Proposition

Soit $f : G \to H$ un isomorphisme de groupes. Alors sa réciproque $f^{-1} : H \to G$ est aussi un isomorphisme de groupes.

Définition

Soit G un groupe. Un **automorphisme** *de G est un isomorphisme de G dans G. (Ou dit autrement, c'est un endomorphisme de G qui est bijectif.)*

Un exemple

- Soit V un $\mathbb{R}$-espace vectoriel de dimension finie n, et choisissons une base $\mathcal{B}$ de V.
- On a l'application

$$\mathrm{Mat}_{\mathcal{B}} : \mathrm{Aut}(V) \to \mathrm{GL}_n(\mathbb{R}) \ , \ f \mapsto \mathrm{Mat}_{\mathcal{B}}(f)$$

  qui est bijective d'après le cours d'algèbre linéaire. (On rappelle que $\mathrm{Mat}_{\mathcal{B}}(f)$ désigne la matrice de f dans la base $\mathcal{B}$.)
- C'est un isomorphisme de groupes car on a, pour deux automorphismes linéaires $f, g : V \to V$:

$$\mathrm{Mat}_{\mathcal{B}}(f \circ g) = \mathrm{Mat}_{\mathcal{B}}(f) \times \mathrm{Mat}_{\mathcal{B}}(g).$$

- On a donc un isomorphisme de groupes :

$$\mathrm{Aut}(V) \simeq \mathrm{GL}_n(\mathbb{R}).$$

Que veut dire la notion d'isomorphisme de groupes ?

Remarque

Si G et H sont deux groupes finis, dire que $G \simeq H$ revient à dire que G et H ont la même table de multiplication quitte à renommer certains éléments (c'est-à-dire à permuter certaines lignes et colonnes).

Remarque

Deux groupes G et H qui sont isomorphes ont **les mêmes propriétés** (les propriétés qui s'énoncent dans le langage de la théorie des groupes). Ainsi, pour montrer que deux groupes G et H ne sont pas isomorphes, il suffit de trouver une propriété (qui s'énonce dans le langage de la théorie des groupes) qui est vraie dans G et pas dans H, ou vice versa.

Trois exercices

Exercice 44
Montrer que si $G \simeq H$ et $H \simeq K$ alors $G \simeq K$.

Exercice 45
Soit $n \in \mathbb{N}^*$. Montrer que les groupes $\mathbb{Z}/n\mathbb{Z}$ et $\mathbb{U}_n$ sont isomorphes.

Exercice 46
Soient G et H deux groupes qui sont isomorphes.

1) Montrer que si G est abélien alors H est abélien.
2) Montrer que si G est cyclique alors H est cyclique.
3) Montrer que si l'équation $x^5 = e_G$ a 10 solutions $x \in G$ alors l'équation $y^5 = e_H$ a 10 solutions $y \in H$.

Le théorème chinois des restes refait son apparition

Théorème (Théorème chinois des restes)
Soient $m, n \in \mathbb{N}$ *avec* $m \wedge n = 1$. *Alors on a un isomorphisme de groupes :*

$$\mathbb{Z}/mn\mathbb{Z} \simeq \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}.$$

Démonstration. Le théorème chinois des restes affirme qu'on a une bijection

$$g : \mathbb{Z}/mn\mathbb{Z} \longrightarrow \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}\ ,\ \overline{k} \mapsto (\,\widetilde{k}\,,\,\widehat{k}\,).$$

C'est un morphisme de groupes. En effet, on a pour tous $\overline{k}, \overline{l} \in \mathbb{Z}/mn\mathbb{Z}$:

$$g(\overline{k}+\overline{l}) = g(\overline{k+l}) = (\widetilde{k+l}, \widehat{k+l}) = (\widetilde{k}+\widetilde{l}, \widehat{k}+\widehat{l}) = (\widetilde{k}, \widehat{k}) + (\widetilde{l}, \widehat{l}) = g(\overline{k}) + g(\overline{l}).$$

C'est donc un isomorphisme de groupes. $\square$

Exercice 47
Montrer que les groupes $\mathbb{Z}/4\mathbb{Z}$ et $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ ne sont pas isomorphes (même s'il existe une bijection entre les ensembles sous-jacents à ces deux groupes).

Une remarque pour finir

Remarque

Soit $f : G \to H$ un morphisme de groupes qui est **injectif**. Alors f induit un isomorphisme de groupes $G \simeq f(G)$. (On rappelle que $f(G)$ est un sous-groupe de H.) Donc G est isomorphe à un sous-groupe de H.

4. Autour de la notion d'ordre

4.1 Ordre d'un élément dans un groupe

Ordre d'un élément dans un groupe

Définition

*Soit G un groupe et soit $x \in G$. L'***ordre** *de x dans G est le plus petit $n \in \mathbb{N}^*$ tel que $x^n = e$, avec la convention que x est d'***ordre infini** *si pour tout $n \in \mathbb{N}^*$, $x^n \neq e$.*

Remarque

En notation additive : l'ordre de x dans G est le plus petit $n \in \mathbb{N}^*$ tel que $nx = 0$, avec la convention que x est d'ordre infini si pour tout $n \in \mathbb{N}^*$, $nx \neq 0$.

Exemple

Le seul élément d'ordre 1 dans un groupe G est l'élément neutre e. Un élément x est d'ordre 2 si et seulement si $x \neq e$ et $x^2 = e$.

Le cas d'un élément d'ordre infini

- Soit $x \in G$ un élément d'ordre infini.
- Alors dans
$$\langle\, x\,\rangle = \{x^k,\, k \in \mathbb{Z}\},$$
tous les x^k, pour $k \in \mathbb{Z}$, sont deux à deux distincts.
- La loi de groupe dans $\langle\, x\,\rangle$ se calcule comme la somme dans $\mathbb{Z}$:
$$x^k x^{k'} = x^{k+k'}.$$
- Conclusion : le groupe $\langle\, x\,\rangle$ se comporte comme le groupe $\mathbb{Z}$.
- Plus formellement, le groupe $\langle\, x\,\rangle$ est isomorphe à $\mathbb{Z}$.

Le cas d'un élément d'ordre fini

- Soit $x \in G$ un élément d'ordre fini $n \in \mathbb{N}^*$.
- Alors on a
$$\langle\, x\,\rangle = \{x^k,\ k \in \mathbb{Z}\} = \{e, x, x^2, \ldots, x^{n-1}\}$$
et les x^k, pour $k \in \{0, \ldots, n-1\}$, sont deux à deux distincts.

- La loi de groupe dans $\langle\, x\,\rangle$ se calcule comme la somme dans $\mathbb{Z}/n\mathbb{Z}$:
$$x^k x^{k'} = x^{k+k'} \qquad \text{avec } \ x^n = e.$$

- Par exemple, si x est d'ordre 6 on a
$$\langle\, x\,\rangle = \{e, x, x^2, x^3, x^4, x^5\},$$
qui a 6 éléments et où la loi de groupe se calcule comme :
$$x^5 x^4 = x^9 = x^6 x^3 = e x^3 = x^3.$$
(Ça revient à calculer dans $\mathbb{Z}/6\mathbb{Z}$: $\overline{5} + \overline{4} = \overline{3}$.)

- Conclusion : le groupe $\langle\, x\,\rangle$ se comporte comme le groupe $\mathbb{Z}/n\mathbb{Z}$.
- Plus formellement, le groupe $\langle\, x\,\rangle$ est isomorphe à $\mathbb{Z}/n\mathbb{Z}$.