HAX501X – Groupes et anneaux 1

CM5 21/09/2023

Clément Dupont

Questions de cours en contrôle / examen

- Tout le cours des chapitres 2, 3, 4 est à connaître.
- Cela inclut les démonstrations.

Retour sur les exercices du cours

Exercice 25

Pour $n = 12$, quels sont les générateurs de $\mathbb{Z}/12\mathbb{Z}$? Pour chacun de ces générateurs, vérifiez que vous avez compris ce que cela veut dire en faisant tourner les aiguilles d'une horloge.

- Par le cours, les générateurs de $\mathbb{Z}/12\mathbb{Z}$ sont les $\overline{a}$ avec $a \wedge 12 = 1$. Ce sont donc :

$$\overline{1}\ ,\ \overline{5}\ ,\ \overline{7} = \overline{-5}\ ,\ \overline{11} = \overline{-1}.$$

- Par exemple, si l'on calcule les $\overline{5k}$ pour $k = 0, 1, 2, \ldots$ on trouve successivement :

$$\overline{0}, \overline{5}, \overline{10}, \overline{3}, \overline{8}, \overline{1}, \overline{6}, \overline{11}, \overline{4}, \overline{9}, \overline{2}, \overline{7}, \overline{0}, \overline{5}, \text{etc.}$$

Exercice 26

Supposons que toutes les années ont 365 jours. Ma comète préférée passe à proximité de la Terre tous les 146 jours. Y aura-t-il une année où elle passera un 14 juillet ? Le résultat change-t-il si la comète passe à proximité de la Terre tous les 147 jours ?

- On se place dans $\mathbb{Z}/365\mathbb{Z}$, où l'on choisit que $\overline{0}$ correspond à un jour où la comète passe à proximité de la Terre. L'ensemble des jours où passe la comète est donc le sous-groupe $\langle\,\overline{146}\,\rangle$. Or $365 \wedge 146 = 73$ et donc

  $$\langle\,\overline{146}\,\rangle = \langle\,\overline{73}\,\rangle = \{\overline{0}, \overline{73}, \overline{146}, \overline{219}, \overline{292}\}.$$

  Conclusion : la comète passera un 14 juillet ssi le 14 juillet est un des 5 jours de l'année $\overline{0}, \overline{73}, \overline{146}, \overline{219}, \overline{292}$.

- Si la comète repasse tous les 147 jours la situation est différente puisque $365 \wedge 147 = 1$. On a donc

  $$\langle\,\overline{147}\,\rangle = \mathbb{Z}/365\mathbb{Z}.$$

  Conclusion : il y aura une année où la comète passera le 14 juillet.

3 – Introduction à la théorie des groupes

1. Le langage des groupes

1.1 Définition
1.2 Exemples
1.3 Inversibles dans un monoïde
1.4 Règles de calcul dans un groupe
1.5 Produits de groupes
1.6 Fonctions à valeurs dans un groupe

Définition

Une **loi de composition interne** $*$ sur un ensemble E est une application

$$E \times E \to E\,,\ (x,y) \mapsto x*y.$$

Définition

Un **groupe** *est une paire $(G,*)$ où G est un ensemble et $*$ est une loi de composition interne sur G qui vérifie les axiomes suivants.*

(1) *Associativité : $\forall x,y,z \in G\,,\ (x*y)*z = x*(y*z)$.*

(2) *Élément neutre : il existe un élément $e \in G$ tel que $\forall x \in G\,,\ x*e = x = e*x$. On l'appelle l'* **élément neutre** *du groupe.*

(3) *Inverse : pour tout $x \in G$ il existe un $y \in G$ tel que $x*y = e = y*x$. On l'appelle l'* **inverse** *de x dans le groupe et on le note x^{-1}.*

- On a donc :
$$x*x^{-1} = e = x^{-1}*x.$$
- Grâce à l'associativité de $*$ on n'est pas obligé de parenthéser quand on utilise plusieurs fois la loi $*$, et on peut écrire par exemple $x*y*z$ pour signifier $x*(y*z)$ ou $(x*y)*z$, qui sont égaux.

Premières propriétés

Proposition

Soit $(G, *)$ un groupe. On a les propriétés suivantes :

(a) *L'élément neutre est unique. (Cela justifie le fait de l'appeler* **l'***élément neutre.)*

(b) *L'inverse d'un élément $x \in G$ est unique. (Cela justifie le fait de l'appeler* **l'***inverse et de le noter x^{-1}.)*

(c) *Pour tout $x \in G$ on a $(x^{-1})^{-1} = x$.*

(d) *Pour tous $x, y \in G$ on a $(x * y)^{-1} = y^{-1} * x^{-1}$.*

Plus de vocabulaire

Définition

Un dit qu'un groupe $(G, *)$ *est* **abélien** *si la loi* $*$ *est commutative :*

$$\forall x, y \in G,\ x * y = y * x.$$

Définition

Un groupe $(G, *)$ *est dit* **fini** *si l'ensemble* G *est fini. Son cardinal* $|G|$ *est alors appelé l'***ordre** *de* G*.*

- Pour un groupe fini d'ordre $|G| = n$ pas trop grand, on peut écrire $G = \{x_1, \ldots, x_n\}$ et représenter la loi de composition interne $*$ sous la forme d'une **table de multiplication** (aussi appelée **table de Cayley**), qui est un tableau à deux entrées qui contient le résultat de $x_i * x_j$ à l'intersection de la ligne i et de la colonne j.

Et un exercice

Exercice 27
Soit $(G, *)$ un groupe et soit $x \in G$. On suppose qu'il existe $y \in G$ tel que $x * y = e$. Montrer que $y = x^{-1}$.

Exemples de groupes abéliens

- Un ensemble $G = \{e\}$ à un élément, muni de la loi $*$ définie par $e * e = e$, est un groupe abélien, qu'on appelle **groupe trivial**.
- $(\mathbb{Z}, +)$ est un groupe abélien. L'élément neutre est 0 et l'inverse de $n \in \mathbb{Z}$ est $-n$.
- $(\mathbb{R}, +)$, est un groupe abélien. Il en est de même pour $(\mathbb{K}, +)$ pour n'importe quel corps $\mathbb{K}$: par exemple, $(\mathbb{Q}, +)$ et $(\mathbb{C}, +)$ sont des groupes abéliens.
- Si V un $\mathbb{R}$-espace vectoriel, $(V, +)$ est un groupe abélien. Il en en de même pour les $\mathbb{K}$-espaces vectoriels, pour n'importe quel corps $\mathbb{K}$, par exemple $\mathbb{K} = \mathbb{Q}$ ou $\mathbb{K} = \mathbb{C}$.
- $(\mathbb{Z}/n\mathbb{Z}, +)$ est un groupe abélien fini, d'ordre n. L'élément neutre est $\overline{0}$ et l'inverse de $\overline{a} \in \mathbb{Z}/n\mathbb{Z}$ est $\overline{-a}$.
- $(\mathbb{R}^*, \times)$ est un groupe abélien. L'élément neutre est 1 et l'inverse d'un élément $x \in \mathbb{R}^*$ est $\frac{1}{x}$. Il en est de même pour $(\mathbb{K}^*, \times)$ pour n'importe quel corps $\mathbb{K}$: par exemple, $(\mathbb{Q}^*, \times)$ et $(\mathbb{C}^*, \times)$ sont des groupes abéliens.

Un exercice

Exercice 28
Écrire la table de multiplication du groupe $\mathbb{Z}/4\mathbb{Z}$.

Exemples de groupes non abéliens

- Pour tout $n \in \mathbb{N}$, on note $\mathrm{GL}_n(\mathbb{R})$ l'ensemble des matrices inversibles de taille n. Alors $(\mathrm{GL}_n(\mathbb{R}), \times)$ est un groupe qui n'est pas abélien si $n \geqslant 2$. On l'appelle le **groupe général linéaire** de degré n sur $\mathbb{R}$. L'élément neutre est la matrice identité I_n et l'inverse de $A \in \mathrm{GL}_n(\mathbb{R})$ est l'inverse usuel des matrices A^{-1}. Il en est de même pour $(\mathrm{GL}_n(\mathbb{K}), \times)$ pour n'importe quel corps $\mathbb{K}$, par exemple $\mathbb{K} = \mathbb{Q}$ ou $\mathbb{K} = \mathbb{C}$.
- Soit V un $\mathbb{R}$-espace vectoriel et $\mathrm{Aut}(V)$ l'ensemble des automorphismes linéaires de V, c'est-à-dire des applications linéaires bijectives $f : V \to V$. Alors $(\mathrm{Aut}(V), \circ)$ est un groupe, qui n'est pas abélien si V est de dimension $\geqslant 2$. L'élément neutre est l'identité id_V et l'inverse de $f \in \mathrm{Aut}(V)$ est sa réciproque f^{-1}. Il en est de même si l'on part d'un espace vectoriel sur un corps $\mathbb{K}$, par exemple $\mathbb{K} = \mathbb{Q}$ ou $\mathbb{K} = \mathbb{C}$.

Exercice 29
Démontrer que $\mathrm{GL}_n(\mathbb{R})$ est abélien si $n \leqslant 1$ et ne l'est pas si $n \geqslant 2$. Pour V un $\mathbb{R}$-espace vectoriel, démontrer que $\mathrm{Aut}(V)$ est abélien si $\dim(V) \leqslant 1$ et non abélien si $\dim(V) \geqslant 2$.

Exemples de groupes non abéliens, suite

- Pour tout $n \in \mathbb{N}$, notons $\mathfrak{S}_n$ l'ensemble des **permutations** de $\{1, \dots, n\}$, c'est-à-dire des bijections $\sigma : \{1, \dots, n\} \to \{1, \dots, n\}$. Alors $(\mathfrak{S}_n, \circ)$ est un groupe, où l'élément neutre est l'identité $\mathrm{id}_{\{1,\dots,n\}}$ et l'inverse de $\sigma \in \mathfrak{S}_n$ est sa réciproque σ^{-1}. On l'appelle le **groupe symétrique** sur n éléments. C'est un groupe fini d'ordre $n!$. Il n'est pas abélien si $n \geqslant 3$.

- Plus généralement, pour un ensemble E, fini ou infini, on définit l'ensemble $\mathrm{Bij}(E)$ des permutations de E, c'est-à-dire des bijections $\sigma : E \to E$. Alors $(\mathrm{Bij}(E), \circ)$ est un groupe qui n'est pas abélien si E a au moins 3 éléments.

Exercice 30
Lister les éléments de $\mathfrak{S}_2$,, de $\mathfrak{S}_3$, de $\mathfrak{S}_4$. Écrire la table de multiplication de $\mathfrak{S}_2$ et $\mathfrak{S}_3$. Démontrer que $\mathfrak{S}_n$ est abélien si $n \leqslant 2$ et ne l'est pas si $n \geqslant 3$.

Non-exemples de groupes

- L'ensemble $\mathbb{Z}$ muni de la soustraction $-$ n'est pas un groupe car la loi $-$ n'est pas associative : on a $(7-2)-3=2$ et $7-(2-3)=8$.
- $(\mathbb{N},+)$ n'est pas un groupe car 7 n'a pas d'inverse pour $+$ dans $\mathbb{N}$.
- $(\mathbb{R},\times)$ n'est pas un groupe car 0 n'a pas d'inverse pour $\times$ dans $\mathbb{R}$.
- Pour $n \in \mathbb{N}^*$, notons $\mathrm{M}_n(\mathbb{R})$ l'ensemble des matrices carrées de taille n à coefficients dans $\mathbb{R}$. Alors $(\mathrm{M}_n(\mathbb{R}),\times)$ n'est pas un groupe car certaines matrices carrées n'ont pas d'inverse pour $\times$ dans $\mathrm{M}_n(\mathbb{R})$, par exemple la matrice nulle.
- Pour $n \in \mathbb{N}^*$, l'ensemble $\mathrm{GL}_n(\mathbb{R})$ muni de l'addition des matrices n'est pas un groupe... car l'addition des matrices n'est même pas une loi de composition interne sur $\mathrm{GL}_n(\mathbb{R})$. En effet, en général, la somme de deux matrices inversibles n'est pas inversible : par exemple, I_n et $-I_n$ sont inversibles mais leur somme est 0, qui n'est pas inversible.

Monoïdes

Définition

Un **monoïde** *est une paire* $(M, *)$ *où* M *est un ensemble et* $*$ *est une loi de composition interne sur* M *qui vérifie les axiomes suivants :*

(1) *Associativité :* $\forall x, y, z \in M$, $(x * y) * z = x * (y * z)$.

(2) *Élément neutre : il existe un élément* $e \in M$ *tel que* $\forall x \in M$, $x * e = x = e * x$. *On l'appelle l'***élément neutre** *du monoïde.*

Comme dans le cas d'un groupe, l'élément neutre est unique.

Définition

Soit $(M, *)$ *un monoïde. On dit qu'un élément* $x \in M$ *est* **inversible** *s'il existe* $y \in M$ *tel que* $x * y = e = y * x$. *On l'appelle l'***inverse** *de* x *dans* M *et on le note* x^{-1}. *On note*

$$M^{\times} \subset M$$

l'ensemble des éléments inversibles de M.

Comme dans le cas d'un groupe, l'inverse d'un élément est unique lorsqu'il existe.

Le groupe des inversibles dans un monoïde

Proposition

Soit $(M, *)$ *un monoïde. Alors* $(M^\times, *)$ *est un groupe.*

Démonstration.

- On montre facilement, comme dans une proposition vue plus haut, que si $x, y \in M$ sont inversibles alors $x * y$ est inversible (d'inverse $y^{-1} * x^{-1}$). Donc $*$ est bien une loi de composition interne sur $M^\times$.
- Elle est associative par définition d'un monoïde.
- Elle a un élément neutre car l'élément neutre e de M est bien inversible : $e * e = e$.
- Enfin, chaque élément $x \in M^\times$ a un inverse x^{-1} dans M, qui est inversible (d'inverse x) et donc $x^{-1} \in M^\times$. On en conclut que $(M^\times, *)$ est un groupe.

$\square$

Exemples de groupes d'inversibles dans un monoïde

- Si l'on part du monoïde $(\mathbb{R}, \times)$, on obtient le groupe $(\mathbb{R}^*, \times)$. De même en remplaçant $\mathbb{R}$ par un corps $\mathbb{K}$.
- Si l'on part du monoïde $(\mathrm{M}_n(\mathbb{R}), \times)$, on obtient le groupe $(\mathrm{GL}_n(\mathbb{R}), \times)$. De même en remplaçant $\mathbb{R}$ par un corps $\mathbb{K}$.
- Pour tout $n \geqslant 1$, on peut considérer le monoïde $(\mathbb{Z}/n\mathbb{Z}, \times)$, on obtient alors le groupe $((\mathbb{Z}/n\mathbb{Z})^\times, \times)$. C'est un groupe fini d'ordre $\varphi(n)$. Il est abélien puisque la multiplication dans $\mathbb{Z}/n\mathbb{Z}$ est commutative.

Exercice 31
Écrire la table de multiplication du groupe $((\mathbb{Z}/8\mathbb{Z})^\times, \times)$.

Exercice 32
Vérifier que $(\mathbb{Z}, \times)$ est un monoïde. Quel est le groupe $(\mathbb{Z}^\times, \times)$?

Notation

- On note souvent G à la place de $(G, *)$ quand la loi de composition interne est implicite. Par exemple : quand on écrit “le groupe $\mathbb{Z}$” on désigne implicitement le groupe $(\mathbb{Z}, +)$.
- Quand on parle d'un groupe abstrait G on note souvent la loi de composition interne sous la forme **multiplicative**, en écrivant xy à la place de $x * y$. Dans ce cas on peut utiliser le symbole 1 pour l'élément neutre.
- Dans le cadre d'un groupe abstrait qui est *abélien*, il est commun d'utiliser plutôt la notation $+$ et de noter 0 l'élément neutre et $-x$ l'inverse de x (notation **additive**).

Puissances

- Pour un élément $x \in G$ et un entier naturel $n \in \mathbb{N}$ on note x^n le produit n fois de x avec lui-même, défini par récurrence sur n par
$$x^0 = e \quad \text{et} \quad x^n = x^{n-1}x \quad \text{pour } n \geqslant 1.$$
- On étend la notation x^n à tous les entiers relatifs $n \in \mathbb{Z}$ en posant, pour $n \in \mathbb{N}$,
$$x^{-n} = (x^{-1})^n.$$
- On a les relations usuelles, valables pour tous $m, n \in \mathbb{Z}$:
$$x^{m+n} = x^m x^n \quad \text{et} \quad (x^m)^n = x^{mn}.$$

Remarque

En notation additive, x^n s'écrit nx.

Simplification

On peut simplifier à gauche et à droite dans un groupe.

Proposition

Soit G un groupe. Pour des éléments $x, y, z \in G$ on a les règles de simplification :

$$xy = xz \iff y = z$$
$$xz = yz \iff x = y.$$

Démonstration. Dans les deux cas le sens $\Longleftarrow$ est évident. Pour le sens $\Longrightarrow$, il suffit de multiplier à gauche par x^{-1} dans le premier cas, à droite par z^{-1} dans le deuxième cas. □

- Notamment, on a, pour G un groupe et $a, x, y \in G$:

$$ax = y \iff x = a^{-1}y.$$

Un exercice

Exercice 33
Montrer qu'en général la table de multiplication d'un groupe fini contient chaque élément du groupe dans chaque ligne et dans chaque colonne.

Produit de groupes

Soient $(G_1, *_1)$ et $(G_2, *_2)$ deux groupes. On définit une loi de composition interne $*$ sur le produit cartésien $G_1 \times G_2$ par la formule :

$$(x_1, x_2) * (y_1, y_2) = (x_1 *_1 y_1, x_2 *_2 y_2).$$

Proposition

Muni de cette loi de composition interne, $G_1 \times G_2$ est un groupe.

Démonstration. Laissé au lecteur. On vérifie notamment que l'élément neutre de $G_1 \times G_2$ est (e_1, e_2), où e_1 est l'élément neutre de G_1 et e_2 l'élément neutre de G_2 ; et que l'inverse d'un élément $(x_1, x_2) \in G_1 \times G_2$ est (x_1^{-1}, x_2^{-1}). □

Définition

On appelle $G_1 \times G_2$ le **groupe produit** *(ou* **produit direct***) de G_1 et G_2.*

Exercice 34

Écrire la table de multiplication du groupe $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

Produit de groupes, suite

- Plus généralement, pour une famille $(G_i)_{i\in I}$ de groupes indexée par un ensemble I, on peut former le produit

$$\prod_{i\in I} G_i,$$

qui est un groupe où la loi de groupe se calcule "coordonnée par coordonnée".

- Si tous les groupes G_i sont égaux au même groupe G, on le note G^I.

1. Le langage des groupes

Fonctions à valeurs dans un groupe

Soit G un groupe et I un ensemble. Rappelons que G^I peut être vu comme l'ensemble des applications $f : I \to G$. Avec ce point de vue, la loi de groupe se calcule, pour $f_1, f_2 : I \to G$, par la formule

$$(f_1 f_2)(i) = f_1(i) f_2(i).$$

L'élément neutre est la fonction constante égale à e : $f(i) = e$ pour tout $i \in I$.

Exemple

Pour tout ensemble E, l'ensemble $\mathbb{Z}^E$ des applications $f : E \to \mathbb{Z}$ est un groupe pour l'addition des fonctions :

$$(f_1 + f_2)(x) = f_1(x) + f_2(x).$$

L'élément neutre est la fonction nulle.