Compléments de Mathématiques Discrètes: Cours 1 .

Michaël Quisquater (Maître de Conférences,UVSQ)

Modalités

- 6 cours, 6 TD.
- Examen: jeudi 11 octobre à 13h40 (Amphi B et E).
- Deux parties:
  1. Introduction à la théorie des nombres et à l'algèbre abstraite: Cours 1-2-3.
  2. Théorie des probabilités discrètes: Cours 4-5-6.

Rédaction mathématique

- Axiome: vérité indémontrable qui doit être admise
- Définition: Attribution d'un nom à un objet ou un concept
- Théorème: proposition qui peut être mathématiquement démontrée
- Corollaire: Résultat déduit d'un théorème
- Preuve/Démonstration: raisonnement logique construit à partir d'axiomes

Introduction à la théorie des nombres et à l'algèbre abstraite

Notion de structure algébrique

Exemples:

- L'ensemble des naturels $\mathbb{N}$ $(= \{0, 1, 2, \cdots\})$ muni de l'addition et/ou de la multiplication.
- L'ensemble des entiers $\mathbb{Z}$ $(= \{\cdots, -3, -2, -1, 0, 1, 2, 3, \cdots\}$ muni de l'addition et/ou de la multiplication.
- L'ensemble des rationnels $\mathbb{Q}$ (=les entiers et les fractions positives et négatives) muni de l'addition et/ou de la multiplication.
- L'ensemble des réels $\mathbb{R}$ (=l'ensemble des rationnels et des irrationnels $(\sqrt{2}, \pi, \ldots)$) muni de l'addition et/ou de la multiplication.

Notion de structure algébrique (suite)

Point commun entre tous ces exemples: il s'agit d'un ensemble muni d'une ou plusieurs opérations

$\rightarrow$ cas particulier de structures algébriques

Opération binaire

Définition

Une opération binaire sur un ensemble G est une fonction $\cdot : G \times G \to G : (a, b) \mapsto a \cdot b$.

Pour tout $a, b \in G$, nous écrirons $a \cdot b$ ou ab pour $\cdot(a, b)$.

Exemples:

- addition réelle, entière, sur les rationnels, ...
- multiplication d'entiers, de matrices, ...
- ...

Opération binaire (suite)

Remarques:

- La notation d'une opération binaire est un choix (ce qui importe: lien entre les éléments). Nous dirons que $a \cdot b$ représente le produit de a par b. De même, Nous dirons que $a + b$ représente la somme de a et de b. Si $ab = c$ (resp. $a + b = c$), on dira que le résutlat de l'opération $\cdot$ (resp. $+$) appliquée aux éléments a et b est l'élément c.
- Une opération binaire s'applique à 2 éléments. Lorsque l'on écrit $3 + 4 + 5$, on sous-entend $(3 + 4) + 5$ ou $3 + (4 + 5)$. Est-ce le même résultat en général?
- Un ensemble G muni d'une opération binaire $\cdot$ est noté $(G, \cdot)$. Nous noterons $(G, +, \cdot)$ si G est muni des opérations binaires $+$ et $\cdot$.

Associativité et commutativité

Un ensemble muni d'une opération binaire générale ne permet pas de développer beaucoup de mathématiques

$\rightarrow$ définition de propriétés particulières d'une opération binaire.

Définition

Soit un ensemble G muni d'une opération binaire $\cdot : G \times G \rightarrow G$.

- *L'opération binaire $\cdot$ est dite associative si pour tout $a, b, c \in G$, $a \cdot (b \cdot c) = (a \cdot b) \cdot c$.*
- *L'opération $\cdot$ est dite commutative si pour tout élément $a, b \in G$, $a \cdot b = b \cdot a$. Un ensemble muni d'une opération binaire commutative est dit commutatif.*

Associativité et commutativité (suite)

Exemple d'opération associative et commutative:

l'addition des entiers

- Associativité: $(3 + 4) + 5 = 3 + (4 + 5)$
- Commutativité: $3 + 4 = 4 + 3$

Exemple d'opération non-associative et non-commutative:

la soustraction des entiers

- Non-associativité: $(3 - 4) - 5 \neq 3 - (4 - 5)$
- Non-commutativité: $3 - 4 \neq 4 - 3$

Associativité et commutativité (suite)

Remarques:

Lorsque l'opération binaire $\cdot$ est associative, le résultat de $(a \cdot b) \cdot c$ et de $a \cdot (b \cdot c)$ coincident et l'on peut donc écrire sans ambiguité $a \cdot b \cdot c = a \cdot (b \cdot c) = (a \cdot b) \cdot c$ ce qui est très commode.

On peut utiliser les notations:

- $\sum_{i \in I} a_i$ (=somme des éléments a_i dont les indices appartiennent à l'ensemble I)
- $\prod_{i \in I} a_i$ (=produit des éléments a_i dont les indices appartiennent à l'ensemble I)

Neutre et inverse

Définisson à présent des éléments particuliers d'un ensemble muni d'une opération binaire.

Définition

Soit un ensemble G muni d'une opération binaire $\cdot : G \times G \to G$.

- *Un élément $e \in G$ est appelé élément neutre de G si pour tout $a \in G$, nous avons $a \cdot e = a = e \cdot a$.*
- *Un élément $a \in G$ est dit inversible si il existe un élément de G noté a^{-1} tel que $a \cdot a^{-1} = e = a^{-1} \cdot a$ où e est l'élément neutre de G.*

Neutre et inverse (suite)

Remarques:

- Si l'opération binaire de G est notée de façon additive, le neutre est alors noté 0 et l'inverse d'un élément $a \in G$ est appelé *opposé* et noté $-a$.
- Si l'opération binaire de G est notée de façon multiplicative le neutre est noté 1 et l'inverse d'un élément $a \in G$ est noté $a^{-1} \in G$.

Neutre et inverse (exemples)

Exemples:

- 0 est le neutre de $(\mathbb{Z}, +)$, 1 est neutre de $(\mathbb{Q}, \cdot)$, etc
- 1 est l'inverse de 1 dans $(\mathbb{Z}, \cdot)$, $1/3$ est l'inverse de 3 dans $(\mathbb{Q}, \cdot)$, 3 ne posséde pas d'inverse dans $(\mathbb{Z}, \cdot)$
- -3 est l'opposé de 3 dans $(\mathbb{Z}, +)$

Notion de groupe

Définition

Un groupe est un ensemble G muni d'une opération binaire $\cdot : G \times G \to G$ satisfaisant les propriétés suivantes:

1. *$\cdot$ est associative,*
2. *il existe un élément neutre $e \in G$,*
3. *tout élément $a \in G$ est inversible.*

Notion de groupe (exemples)

Exemples:

1. $(\mathbb{Z}, +)$, $(\mathbb{Q}, +)$, $(\mathbb{R}, +)$, $(\mathbb{C}, +)$ sont des groupes commutatifs dont le neutre est 0. $(\mathbb{N}, +)$ n'est pas un groupe car seul 0 possède un opposé c'est-à-dire lui-même.
2. $(\mathbb{Q} \setminus \{0\}, \cdot)$, $(\mathbb{R} \setminus \{0\}, \cdot)$, $(\mathbb{C} \setminus \{0\}, \cdot)$ sont des groupes commutatifs dont le neutre est 1.

Notion de sous-groupe

Soit $(G, \cdot)$ une structure algébrique particulière. Il est assez naturel de se demander si un sous-ensemble de G muni de l'opération binaire $\cdot$ forme une structure algébrique ayant les mêmes propriétés que $(G, \cdot)$. Ce principe appliqué à la notion de groupe aboutit à la définition d'un sous-groupe.

Définition

Soit $(G, \cdot)$ un groupe. Le sous-ensemble H de G est un sous-groupe de G si H est non vide et H est interne pour le produit et l'inversion (i.e. $x \cdot y \in H$ et x^{-1} pour tout $x, y \in H$).

Notion de sous-groupe (exemples)

Exemples:

- $(\mathbb{Q}, +)$ est un sous-groupe de $(\mathbb{R}, +)$
- L'ensemble des nombres pairs un sous-groupe de $(\mathbb{Z}, +)$
- $(\{-1, 1\}, \cdot)$ est un sous-groupe de $(\mathbb{R} \setminus \{0\}, \cdot)$

Notion d'anneau, de corps et de corps commutatif

Jusqu'à présent nous n'avons considéré que des structures algébriques n'ayant qu'une seule opération binaire. Il est fréquent de travailler dans des structures algébriques ayant deux opérations binaires qui interagissent. Ces opérations sont couramment notées $+$ et $\times$ (ou $\cdot$). Un exemple important d'une telle structure sont les anneaux.

Notion d'anneau

Définition

Un anneau $(R, +, \times)$ est un ensemble R muni de deux opérations binaires. L'une est appelée addition et est notée +. L'autre est appelée multiplication et est notée $\times$. Ces opérations satisfont les propriétés suivantes:

1. *$(R, +)$ est un groupe commutatif dont l'élément neutre est noté 0,*
2. *la multiplication est associative,*
3. *la multiplication est distributive par rapport à l'addition. i.e.*
   - *$a \times (b + c) = a \times b + a \times c$ pour tout $a, b, c \in R$,*
   - *$(b + c) \times a = b \times a + c \times a$ pour tout $a, b, c \in R$.*

Un anneau est dit avec élément neutre 1 si il existe un élément $1 \in R$ qui est neutre pour la multiplication

Notion d'anneau (suite)

Exemple:

- L'ensemble des nombres entiers muni de l'addition et de la multiplication usuelle, i.e. $(\mathbb{Z}, +, \times)$, forme un anneau.

Remarques:

- on supposera dans la suite du cours que $1 \neq 0$. En particulier, cela signifie que nous ne considérons pas la structure $(0, +, \times)$ (avec $0 + 0 = 0$ et $0 \times 0 = 0$) comme un anneau.
- la propriété de distributivité indique comment les opérations sont supposées interagir.

Sous-groupe multiplicatif d'un anneau

Notons que les éléments d'un anneau $(A, +, \times)$ ne sont pas tous supposés être inversibles par rapport à la multiplication. L'ensemble des éléments inversibles d'un anneau forme un groupe que l'on notera A^*.

Exemple:

- Considérons l'anneau $(\mathbb{Q}, +, \cdot)$. Le sous-groupe multiplicatif $\mathbb{Q}^*$ est $\mathbb{Q} \setminus \{0\}$

Notion de corps et corps commutatif

Comme déja mentionné précédemment tous les éléments de $\mathbb{Z}$ ne sont pas inversibles par rapport à la multiplication. Cela peut poser des problèmes dans certains applications et dans ce cas il faut utiliser des structures algébriques plus riches. C'est la notion de corps et de corps commutatif.

Définition

Un corps $(F, +, \times)$ est un anneau avec élément neutre 1 tel que tout élément non-nul de F possède un inverse. Un corps dont la multiplication est commutative est appelé corps commutatif.

Notion d'anneau, de corps et de corps commutatif (exemples)

Exemples:

- $(\mathbb{Z}, +, \cdot)$ est un anneau qui n'est pas un corps commutatif
- $(\mathbb{Q}, +, \cdot)$, $(\mathbb{R}, +, \cdot)$ sont des corps commutatifs.
- corps non-commutatif: quaternions (sort du cadre du cours)

Le groupe $(\mathbb{Z}, +)$

Théorème

$(\mathbb{Z}, +)$ est un groupe dont 0 est neutre.

Théorème

Les sous-groupes de $(\mathbb{Z}, +)$ sont de la forme $n\mathbb{Z}$, où $n\mathbb{Z}$ représente l'ensemble des multiples de $n \in \mathbb{Z}$, i.e. $\{n \cdot x \mid x \in \mathbb{Z}\}$.

Exemple: L'ensemble des nombres pairs ($2\mathbb{Z}$) est un sous-groupe de $(\mathbb{Z}, +)$.

L'anneau des entiers $(\mathbb{Z}, +, *)$ muni de la division Euclidienne

Théorème

$(\mathbb{Z}, +, *)$ est un anneau avec neutre 1. Cet anneau est muni de la division Euclidienne. i.e. pour tout entier $a \in \mathbb{Z}$ et tout entier non-nul $b \in \mathbb{Z}$, il existe deux entiers q et r uniques tels que

$$a = b \cdot q + r \text{ avec } 0 \leq r < \mid b \mid,$$

où $\mid \cdot \mid$ est l'opérateur valeur absolue ($\mid x \mid = x$ si $x > 0$ et $\mid x \mid = -x$ sinon). L'entier q est appelé le quotient et r le reste positif.

Exemple: $7 = 2 \cdot 3 + 1$ et $0 < 1 < \mid 3 \mid$.

Notion de divisibilité

On dit que b est un diviseur de a ou encore que a est un multiple de b lorsqu'il existe $q \in \mathbb{Z}$ tel que $a = b \cdot q$. Cela signifie en particulier que le reste de la division de a par b est nul.

La notation $b \mid a$ doit être lue “b divise a” ce qui signifie que b est un diviseur de a.

Notons que l'opération de division a été construite à partir de l'opération de multiplication. Le quotient de a par b est le nombre q tel que $a = b \cdot q$.

Nombres premiers

Définition

Un nombre premier est un entier positif (naturel) possédant exactement deux diviseurs distincts, i.e. un et lui-même. Nous dénoterons par p_i le ième nombre premier, i.e, $p_1 = 2, p_2 = 3, p_3 = 5, p_4 = 7, p_5 = 11$ etc.

Théorème fondamental de l'arithmétique: factorisation

Théorème

Tout nombre naturel non-nul n se décompose de façon unique (à l'ordre des facteurs près) comme produit de puissances de nombres premiers distincts. Formellement,

$$n = \prod_{i \in I} p_i^{\alpha_i}$$

où I est un sous-ensemble de $\mathbb{N} \setminus \{0\}$, les p_i ($i \in I$), sont des nombres premiers distincts et les α_i, $i \in I$, sont des naturels non-nuls.

Théorème fondamental de l'arithmétique (suite)

Remarques:

- Cette décomposition s'appelle la factorisation d'un nombre.
- Résultat d'existence! Trouver les p_i's (factoriser) peut-être difficile en pratique.

Exemple:

$$126 = 2 \cdot 3^2 \cdot 7 \text{ ou encore } 126 = \prod_{i \in I} p_i^{\alpha_i} \text{ avec}$$

$I = \{1, 2, 4\}$, $p_1 = 2, p_3 = 3, p_4 = 7$ et $\alpha_1 = 1, \alpha_2 = 2, \alpha_4 = 1$.

Conclusion

- Notion de structure algébrique
- Groupe (sous-groupe), Anneau, Corps, Corps commutatif
- Structures algébriques des nombres entiers.