

Algebre Lineaire I

David Wiedemann

Table des matières

| | | |
|----------|--|-----------|
| 1 | Le language des Ensembles | 5 |
| 1.1 | Notations | 5 |
| 1.2 | Ensembles | 6 |
| 1.2.1 | Exemples | 6 |
| 1.3 | Sous-Ensembles | 6 |
| 1.4 | $\mathcal{P}(E)$ l'ensemble des sous-ensembles | 6 |
| 1.4.1 | Exercice | 7 |
| 1.5 | Operations sur les ensembles | 7 |
| 1.6 | \times : Produit cartesien | 7 |
| 1.7 | Applications entre ensembles | 7 |
| 1.7.1 | Graphe | 8 |
| 1.8 | Composition/Associativite | 8 |
| 1.8.1 | Associativite | 9 |
| 1.9 | Image,Preimage | 9 |
| 1.10 | Relation de composition par les applications reciproques | 12 |
| 2 | Groupes | 14 |
| 2.1 | Le groupe Symmetrique | 14 |
| 3 | Sous-Groupe | 18 |
| 3.1 | Groupe engendre par un ensemble | 19 |
| 3.2 | Morphismes de Groupes | 21 |
| 4 | Noyau et Image | 25 |
| 5 | Anneaux | 29 |
| 5.1 | Elément inversible | 31 |
| 5.2 | Sous-Anneau | 32 |
| 5.3 | Morphismes d'anneaux | 32 |
| 5.4 | Noyau/Image | 33 |
| 5.5 | Modules sur un Anneau | 34 |
| 5.6 | Sous-Module | 36 |

| | | |
|----------|---|-----------|
| 5.7 | Module engendré par un ensemble | 37 |
| 5.8 | Morphismes de Modules | 38 |
| 5.9 | Structures Algebriques des espaces de morphismes | 40 |
| 6 | Corps | 42 |
| 6.1 | Corps des fractions | 42 |
| 6.2 | Caractéristique des Corps | 45 |
| 6.3 | Arithmétique des corps de caractéristique $p > 0$ | 47 |

List of Theorems

| | | |
|----|--|----|
| 1 | Theorème (Composition de fonctions) | 9 |
| 1 | Definition (Injectivite) | 10 |
| 2 | Definition (Surjectivite) | 10 |
| 3 | Definition (Bijectivite) | 11 |
| 2 | Proposition (Injectivite et cardinalite) | 11 |
| 3 | Proposition (Surjectivite et cardinalite) | 11 |
| 4 | Proposition (injectivite et condition) | 11 |
| 5 | Proposition (Surjectivite et condition) | 11 |
| 7 | Lemme (Composition d'applications surjectives et injectives) . . | 12 |
| 8 | Proposition (Inverse d'une composition) | 13 |
| 4 | Definition (Notations Injection) | 14 |
| 5 | Definition (Notations Surjection) | 14 |
| 6 | Definition (Notations Bijection) | 14 |
| 7 | Definition (Groupe abstrait) | 15 |
| 8 | Definition (Groupes commutatifs) | 16 |
| 9 | Definition (Notation additive) | 16 |
| 9 | Proposition (Lois de Groupe) | 16 |
| 10 | Definition (Notation exponentielle) | 17 |
| 11 | Definition (exponentielle) | 17 |
| 12 | Definition (Notation multiple) | 17 |
| 13 | Definition (Sous-groupe) | 18 |
| 11 | Proposition (Critere de Sous-groupe) | 18 |
| 14 | Theorème (Sous groupe de \mathbb{Z}) | 19 |
| 15 | Proposition (Intersection de sous-groupes) | 20 |
| 14 | Definition (Sous-groupe engendre) | 20 |
| 17 | Theorème | 20 |
| 15 | Definition (Morphisme de Groupe) | 21 |
| 18 | Theorème | 21 |
| 16 | Definition (Notations) | 22 |
| 21 | Proposition | 23 |

| | | |
|----|---|----|
| 22 | Proposition | 24 |
| 17 | Definition (Groupes Isomorphes) | 24 |
| 24 | Theorème | 25 |
| 25 | Proposition | 25 |
| 18 | Definition | 26 |
| 26 | Theorème (Critere d'injectivite) | 26 |
| 19 | Definition (Anneaux) | 29 |
| 30 | Lemme | 29 |
| 20 | Definition (Element Inversible) | 31 |
| 33 | Proposition | 31 |
| 21 | Definition (Sous-Anneau) | 32 |
| 35 | Lemme (Critère de sous-anneau) | 32 |
| 22 | Definition (Morphisme d'anneaux) | 32 |
| 39 | Proposition (Noyau d'un morphisme d'anneau) | 33 |
| 40 | Theorème | 34 |
| 23 | Definition (Modules sur un Anneau) | 34 |
| 24 | Definition (A -Algebre) | 35 |
| 25 | Definition (Sous-Module) | 36 |
| 26 | Definition (Ideal) | 36 |
| 45 | Lemme (Critère de Sous-Module) | 36 |
| 47 | Proposition | 37 |
| 27 | Definition | 37 |
| 48 | Theorème | 37 |
| 28 | Definition (Morphismes de Module) | 38 |
| 50 | Lemme (Critere de l'application lineaire) | 39 |
| 51 | Proposition | 39 |
| 29 | Definition | 40 |
| 53 | Proposition | 40 |
| 54 | Proposition | 41 |
| 55 | Theorème | 41 |
| 30 | Definition (Corps) | 42 |
| 57 | Proposition | 42 |
| 58 | Lemme | 43 |
| 31 | Definition | 43 |
| 59 | Proposition | 43 |
| 32 | Definition | 43 |
| 33 | Definition (Caractéristique) | 45 |
| 61 | Lemme | 46 |
| 34 | Definition | 46 |
| 62 | Lemme | 46 |
| 63 | Lemme | 47 |

| | | |
|----|-----------------------|----|
| 35 | Definition | 47 |
| 65 | Proposition | 47 |
| 36 | Definition | 47 |
| 66 | Lemme | 48 |

Lecture 1: Le langage des Ensembles

Mon 14 Sep

1 Le langage des Ensembles

Le terme “Algebre” est derive du mot arabe al-jabr tire du titre d’un ouvrage.
Al-jabr signifie restoration.

Par exemple : $2x - 4 = 0$ Ce qu’on veut c’est trouver x . Il faut donc transformer cette egalite en effectuant des operations de part et d’autres de l’egalite.

$$\begin{array}{ll} 2x = 4 & | + 4 \\ x = \frac{4}{2} = 2 & | : 2 \end{array}$$

Le but de l’ouvrage etait de resoudre des soucis administratifs, comment partager des champs etc.

Le but c’est d’introduire les espaces vectoriels a partir de 0.

Il y aura besoin d’introduire des groupes, anneaux, corps (anneaux particuliers), modules et des ensembles.

Il faut donc commencer avec les objets les plus simples, i.e. les groupes.
Ici, on introduit de maniere moins rigoureuse qu’avec les systemes algebriques.

1.1 Notations

- "Il existe" \exists , "Il existe un unique" $\exists!$
- "Quel que soit", "Pour tout", \forall
- "Implique", \Rightarrow
- "est equivalent" \iff , ou “ssi”
- "sans perte de generalite" “spdg”, “wlog”
- “on peut supposer” “ops, wma”
- “tel que” t.q. ou |

On ne va pas parler de logique mathematique dans ce cours, ni de definition rigoureuse des ensembles

1.2 Ensembles

Un ensemble est une collection d'éléments "appartenant" à E

$$e \underbrace{\in}_\text{"appartient à"} E$$

1.2.1 Exemples

- \emptyset ne contient aucun élément
- $\mathbb{N} = \{0, 1, 2\}$
- $\mathbb{Z} = \{-2, -1, 0, 1, 2\}$
- $\mathbb{Q} = \{\frac{p}{q} | p, q \in \mathbb{Z}, q \neq 0\}$
- \mathbb{R} , nombres réels, nombres complexes.

1.3 Sous-Ensembles

Un sous-ensemble A d'un ensemble E est un ensemble t.q. tout élément de A appartient à E . Formellement :

$$a \in A \Rightarrow a \in E$$

$$A \underbrace{\subset}_{\text{inclut dans } E} E$$

L'ensemble vide est un sous-ensemble de E pour tout ensemble E .

$$\emptyset \subset E \forall E$$

Deux ensembles E et F sont égaux si ils ont les mêmes éléments, ssi E est inclus dans F et F est inclus dans E (regarder notations)

$$E \subset F \wedge F \subset E \Rightarrow E = F.$$

1.4 $\mathcal{P}(E)$ l'ensemble des sous-ensembles

C'est l'ensemble des $A \in E$, aussi appelé l'ensemble des parties de E .

Remarque : L'ensemble de TOUS les ensembles n'est pas un ensemble et c'est du au paradoxe de Russell (Logicien anglais) Si c'était le cas, on considérerait

$$N_{\text{cont}} = \{ \text{L'ensemble des } E \text{ tq } E \text{ n'est pas contenu dans lui même.} \}$$

Cet ensemble N_{cont} est-il contenu dans lui même ou pas ?

1.4.1 Exercice

Ncont est il contenu dans lui meme ou pas ? \nexists

1.5 Operations sur les ensembles

— $A, B \subset E$

$$A \cup B = \{e \in E \text{ tq } e \in A \text{ ou bien } e \in B\}$$

Réunion de A et B .

— $A \cap B = \{e \in E | e \in A \text{ et } e \in B\}$

Difference : $A - B$ ou $A \setminus B$

$$= \{e \in A \wedge e \notin B\}$$

Difference symmetrique :

$$A \Delta B = (A - B) \cup (B - A)$$

Si $A \cap B = \emptyset$ on dit que A et B sont disjoints. $A_1, \dots, A_n \subset E \quad n \geq 1$

On peut noter une grande reunion ainsi :

$$\begin{aligned} A_1 \cup A_2 \cup \dots \cup A_n &= A_1 \cup (A_2 \cup \dots \cup A_n) \\ &= \{e \in E | \exists i \in \{1, \dots, n\} \text{ avec } e \in A_i\} \\ &= \bigcup_{i=1}^n A_i \end{aligned}$$

1.6 \times : Produit cartésien

Si A et B sont des ensembles

$$A \times B = \{(a, b) | a \in A \wedge b \in B\}$$

On peut bien sur iterer

$$A_1 \times \dots \times A_n = \prod_{i=1}^n A_i = \{a_1, a_2, \dots, a_n \text{ avec } a_i \in A_i\}$$

1.7 Applications entre ensembles

Soient X et Y deux ensembles.

Une application (fonction) f est la donnée pour chaque element $x \in X$ (L'espace de depart) d'un element $f(x) \in Y$ (l'espace d'arrivee)

$$f : X \rightarrow Y$$

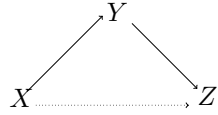


FIGURE 1 – Schema de la composition de 2 applications

1.7.1 Graphe

Se donner une application

$$f : X \rightarrow Y$$

equivaut a se donner un graphe G (graphe de f)

$$G \subset X \times Y = \{(x, y) | x \in X, y \in Y\}$$

tq pour $x_0 \in X$ l'ensemble des elements du graphe G de la forme (x_0, y) possede exactement un element (x_0, y_0) . $y_0 = f(x_0)$ = l'image de x_0 par l'application f .

On associe simplement au premier element un autre element.

1.8 Composition/Associativite

Soient

$$f : X \rightarrow Y$$

$$g : Y \rightarrow Z$$

$$\begin{aligned} g \circ f : X &\longrightarrow Z | x \in X \longrightarrow f(x) \in Y \\ &\longrightarrow g(f(x)) \in Z \end{aligned}$$

Cette application s'appelle la composee de f et g .

1.8.1 Associativite

$$f : X \longrightarrow Y$$

$$g : Y \longrightarrow Z$$

$$h : Z \longrightarrow W$$

Alors

$$\begin{aligned}(g \circ f) : X &\longrightarrow Z \circ h : Z \longrightarrow W \\ &\Rightarrow h \circ (g \circ f)\end{aligned}$$

$$f : X \longrightarrow Y \circ h \circ g : Y \longrightarrow W$$

On a que

| |
|--|
| Theorème 1 (Composition de fonctions) |
|--|

| |
|---|
| $h \circ (g \circ f) = (h \circ g) \circ f = h \circ g \circ f$ |
|---|

Preuve

$$\begin{aligned}h \circ (g \circ f) : x &\longrightarrow h((g \circ f)(x)) \\ &= h(g(f(x))) \in W \\ (h \circ g) \circ f : x &\longrightarrow (h \circ g)(f(x)) \\ h(g(f(x))) &\in W\end{aligned}$$

□

1.9 Image, Preimage

$$f : X \longrightarrow Y$$

A l'application f sont associes deux applications impliquant $\mathcal{P}(X), \mathcal{P}(Y)$.

$$— \text{ } Im(f) : \mathcal{P}(X) \longrightarrow \mathcal{P}(Y)$$

$$A \subset X \longrightarrow Im(f)(A) = f(A)$$

C'est ce qu'on appelle l'image de A par f

$$= \{f(a) \in Y | a \in A\} \subset Y \in \mathcal{P}(Y)$$

$$\text{L'image de } f \text{ } Im(f) := f(X) = \{f(x) \in Y | x \in X\}$$

— Preimage de $f : \text{Preim}(f) :$

$$\text{Preim}(f) : \mathcal{P}(Y) \longrightarrow \mathcal{P}(X)$$

$$B \longrightarrow \text{Preim}(f)(B) = f^{-1}(B) \quad = \text{preimage de l'ensemble } B \text{ par } f.$$

$$f^{-1}(B) = \{x \in X | f(x) \in B\}$$

Exemples

$$f_1(\{1, 2\}) = \{2, 4\}$$

$$f_1^{-1}(\{1, 2, 3, 4\}) = \{1, 2, 3, 4\}$$

Lecture 2: Injectivite, Surjectivite et Bijectivite

Tue 15 Sep

Definition 1 (Injectivite)

Une application $f : X \mapsto Y$ est injective (injection) si $\forall y \in Y f^{-1}(\{y\})$ ne possede pas plus d'un element. On note

$$f : X \hookrightarrow Y$$

Remarque : Une condition equivalente d' injectivite :

$$\forall x \neq x' \in X \Rightarrow f(x) \neq f(x')$$

Definition 2 (Surjectivite)

Une application $f : X \mapsto Y$ est surjective (surjection) si $\forall y \in Y f^{-1}(\{y\})$ possede au moins un element.

On note

$$f : X \twoheadrightarrow Y$$

Soit $f^{-1}(\{y\}) \neq \emptyset$, il existe au moins $x \in X$ tq $f(x) = y$

De maniere equivalente

$$\text{surjectif} \iff \text{Im}(f) = f(X) = Y$$

Alors on a une application

$$\begin{aligned} "f'' : X &\mapsto Y \\ x &\mapsto f(x) \end{aligned}$$

Cette application est toujours surjective.

Definition 3 (Bijectivite)

Une application $f : X \mapsto Y$ est bijective (bijection) si elle est injective et surjective, cad si $\forall y \in Y, f^{-1}(\{y\})$ (l'ensemble des antecedents de y par f) possede exactement un element. On note la bijectivite par

$$f : X \simeq Y$$

Si $f : X \simeq Y$, alors on peut identifier les els de X avec ceux de Y :

$$x \in X \leftrightarrow f(x) \in Y$$

Remarque : Si $f : X \hookrightarrow Y$

$Y' = f(X)$ l'application

$$f : X \twoheadrightarrow Y' = f(X)$$

et toujours surjective. et comme f est injective, on obtient une bijection $f : X \simeq Y' = f(X)$ entre X et $f(X)$.

X peut etre identifie a $f(X)$.

- $Id_X : \underbrace{X \mapsto X}_{x \mapsto x}$ est bijective
- $x \in \mathbb{R}_{\geq 0} \mapsto x^2 \in \mathbb{R}_{\geq 0}$ est inj et bijective.
- $\mathcal{P} \simeq \{0, 1\}^X = \mathcal{F}(X, \{0, 1\})$

Exercice

$$C : \mathbb{N} \times \mathbb{N} \mapsto \mathbb{N}$$

$$(m, n) \mapsto \frac{1}{2}((m+n)^2 + m + 3n)$$

Montrer la bijectivite.

Dans ce qui suit, soient X et Y des ensembles finis possedant respectivement $|X|$ et $|Y|$ elements et $f : X \mapsto Y$ une application entre ces ensembles. On a les proprietes suivantes :

Proposition 2 (Injectivite et cardinalite)

Si $f : X \hookrightarrow Y$ est injective alors $|X| \leq |Y|$

Proposition 3 (Surjectivite et cardinalite)

Si $f : X \twoheadrightarrow Y$ est surjective alors $|X| \geq |Y|$.

Proposition 4 (injectivite et condition)

Si $f : X \hookrightarrow Y$ et $|X| \geq |Y|$ alors $|Y| = |X|$ et f bijective.

Proposition 5 (Surjectivite et condition)

Si $f : X \twoheadrightarrow Y$ et $|X| \leq |Y|$ alors $|Y| = |X|$ et f bijective.

Propriete 6 (Bijectivite)

Si f bijective, on peut lui associer une application reciproque :

$$f^{-1} : Y \mapsto X$$

$$y \mapsto x$$

tel que $f^{-1}(\{y\}) = \{x\}$, x unique.

1.10 Relation de composition par les applications reciproques

— $f : X \simeq Y$ et $f^{-1} : Y \simeq X$

$$f^{-1} \circ f : X \mapsto Y \mapsto X = Id_X.$$

En effet, $\forall x \in X$ si on pose $y = f(x)$

on a $f^{-1}(y) = x = f^{-1}(f(x)) = x$

— $f \circ f^{-1} : Y \mapsto X \mapsto Y$

$$f \circ f^{-1} = Id_Y$$

— $(f^{-1})^{-1} = f$

— $f : X \simeq Y$ et $g : Y \simeq Z$

Alors $g \circ f : X \mapsto Z$ est bijective et $(g \circ f)^{-1} = f^{-1} \circ g^{-1}$

Lemme 7 (Composition d'applications surjectives et injectives)

1. Si f et g sont injectives, $g \circ f$ est injective.

2. Si f et g sont surjectives, $g \circ f$ est surjective.

3. Si f et g sont bijectives, $g \circ f$ est bijective et

$$(g \circ f)^{-1} = f^{-1} \circ g^{-1}.$$

Preuve

1. $g \circ f : X \mapsto Y \mapsto Z$

$$x \mapsto g(f(x))$$

$\forall z \in Z$ on veut montrer que $(g \circ f)^{-1}(\{z\})$ a au plus un element

$$(g \circ f)^{-1}(\{z\}) = \{x \in X | g(f(x)) = z\}$$

$$\text{si } g(f(x)) = z \Rightarrow f(x) \in g^{-1}(\{z\})$$

l'ensemble $\{x \in X | g(f(x)) = z\}$ est contenu dans $g^{-1}(\{z\})$ et donc possede au plus 1 element. Si cet ensemble est vide on a fini $(g \circ f)^{-1}(\{z\}) =$

\emptyset . Si $g^{-1}(\{z\}) \neq \emptyset$ alors $g^{-1}(\{z\}) = \{y\}$
et $x \in (g \circ f)^{-1}(\{z\})$ verifie

$$f(x) = y \Rightarrow x \in f^{-1}(\{y\})$$

Comme f^{-1} est injective $f^{-1}(\{y\})$ possede au plus un element.
Et donc $g^{-1}(f^{-1}(\{z\}))$ a au plus 1 element car g est surjective

2. Surjectivite : Exercice

3. Bijectivite : si f et g sont bijectives $g \circ f$ est bijective.

f et g sont inj $\Rightarrow g \circ f$ inj.

f et g sont surj $\Rightarrow g \circ f$ surj

Si f et g sont bij $\Rightarrow g \circ f$ est injective et surjective

$\Rightarrow g \circ f$ bijective. □

Proposition 8 (Inverse d'une composition)

On veut montrer que $\forall z \in Z$

$$X := (g \circ f)^{-1}(z) = f^{-1} \circ g^{-1}(z) \underbrace{=}_{?} f^{-1}(g^{-1}(z)) = x'$$

Preuve

$$\begin{aligned} g \circ f(x) &= g(f(x)) = z \\ g \circ f(f^{-1}(g^{-1}(z))) &= g(f(f^{-1}(g^{-1}(z)))) \\ &= g(f \circ f^{-1}(g^{-1}(z))) \end{aligned}$$

Or on sait que

$$f \circ f^{-1} = g \circ g^{-1} Id_Y$$

et donc

$$g(f \circ f^{-1}(g^{-1}(z))) = g(g^{-1}(z)) = z = (g \circ f)(x)$$

On a donc montre que

$$(g \circ f)(x) = z = (g \circ f)(x') \quad \square$$

$\Rightarrow x$ et x' on la meme image par $g \circ f$ et comme $g \circ f$ est injective $x = x'$. Donc
 $\forall z \in Z (g \circ f)^{-1}(z) = f^{-1} \circ g^{-1}(z)$.

L'ensemble des applications entre X et Y seran note

$$\mathcal{F}(X, Y) = HOM_{ENS}(X, Y) = Y^X$$

Definition 4 (Notations Injection)

L'ensemble des applications injectives sera noté

$$INJ_{ENS}(X, Y)$$

Definition 5 (Notations Surjection)

L'ensemble des applications surjectives sera noté

$$SURJ_{ENS}(X, Y)$$

Definition 6 (Notations Bijection)

L'ensemble des applications bijectives sera noté

$$BIJ_{ENS}(X, Y) = ISO_{ENS}(X, Y)$$

Si il s'agit d'une bijections de X vers $Y = X$ alors

$$Hom_{ENS}(X, X) = END_{ENS}(X) = AUT_{ENS} = ISO_{ENS}(X)$$

On appelle cet ensemble aussi parfois l'ensemble des permutations de X .

2 Groupes

2.1 Le groupe Symétrique

Voici un exemple d'un groupe, le groupe des bijections muni de la composition.

X ensemble

$$Bij(X, X) = Bij(X)$$

Clairement $\{Id_X\} \subset Bij(X) \Rightarrow Bij(X) \neq \emptyset$.

Supposons $f, g \in Bij(X)$, alors

$$f, g \mapsto g \circ f \in Bij(X)$$

On dispose donc de cette loi de composition :

$$\begin{aligned} \circ : Bij(X) \times Bij(X) &\longrightarrow Bij(X) \\ (g, f) &\longrightarrow g \circ f \end{aligned}$$

\circ est associative :

$f, g, h \in Bij(X)$, alors

$$(f \circ g) \circ h = f \circ (g \circ h) = f \circ g \circ h$$

Id_X est neutre : $\forall f \in Bij(X)$

$$f \circ Id_X = Id_X \circ f = f$$

Donc

$$x \in X(f \circ Id_X)(x) = f(Id_X(x)) = f(x)$$

Pour chaque element f on trouve une reciproque notee f^{-1} tel que

$$f^{-1} \circ f = Id_X = f \circ f^{-1}$$

Toutes ces proprietes font de

$$Bij(X) = Aut_{ENS}(X)$$

un groupe

Definition 7 (Groupe abstrait)

Un groupe $(G, \star, e_G, \cdot^{-1})$ est la donnee d'un quadruple forme

- d'un ensemble G non-vide
- d'une application (appelee loi de composition interne) \star tq

$$\begin{aligned} \star : G \times G &\mapsto G \\ (g, g') &\mapsto \star(g, g') =: g \star g' \end{aligned}$$

- d'un element $e_G \in G$ (element neutre)
- de l'application d'inversion \cdot^{-1}

$$\begin{aligned} \cdot^{-1} : G &\mapsto G \\ g &\mapsto g^{-1} \end{aligned}$$

ayant les proprietes suivantes

- Associativite : $\forall g, g', g'' \in G, (g \star g') \star g'' = g \star (g' \star g'')$.
- Neutralite e_G : $\forall g \in G, g \star e_G = e_G \star g = g$.
- Inversibilite : $\forall g \in G, g^{-1} \star g = g \star g^{-1} = e_G$.

Quelques exemples :

- $(Bij(X), \circ, Id_X, \cdot^{-1})$ est un groupe.
- $(\mathbb{Z}, +, 0, -\cdot)$ est un groupe.
- $(\mathbb{Q} \setminus \{0\}, \times, 1, \cdot^{-1})$ est un groupe.
- $(\{1, -1\}, \times, 1, \cdot^{-1})$ est un groupe.

Definition 8 (Groupes commutatifs)

Un groupe $(G, \star, e_G, \cdot^{-1})$ est dit commutatif si \star possède la propriété supplémentaire de commutativité :

$$\forall g, g' \in G \quad g \star g' = g' \star g$$

Exemple Les groupes $(\mathbb{Z}, +)$ ou $(\mathbb{Q} \setminus \{0\}, \cdot)$ sont des groupes commutatifs. Par contre si X possède au moins 3 éléments $\text{Bij}(X)$ n'est pas commutatif.

Lecture 3: Groupes, Anneaux, Corps

Tue 22 Sep

$$\exists \sigma, \tau \in \text{Bij}(X) \text{ tq. } \sigma \circ \tau \neq \tau \circ \sigma$$

Definition 9 (Notation additive)

Si un groupe est commutatif on pourra utiliser une notation "additive" :

- La loi sera notée $+$.
- L'élément neutre sera noté 0_G .
- L'inversion sera appelée opposé et notée $-g$ et $g + (-g) = 0_G$.

Proposition 9 (Lois de Groupe)

- Involutivité de l'inversion : $\forall g, (g^{-1})^{-1} = g, g^{-1} \star g = e_G$.
- L'élément neutre est unique, si $\exists e'_G$ tq $g \in G$ vérifiant $g \star e'_G = g$, alors e'_G est l'élément neutre.
- Unicité de l'inverse : si $g' \in G$ vérifie $g \star g' = e_G$, alors $g' = g^{-1}$.
- On a $(g \star g')^{-1} = g'^{-1} \star g^{-1}$

Preuve

La preuve de toutes les propriétés est donnée dans le support de cours.

On montre l'unicité de l'élément neutre.

Si e'_G est telle que pour un certain $g \in G$, tq

$$g \star e'_G = g$$

Alors on a à gauche par $g^{-1}g^{-1} \star g \star e'_G = g^{-1} \star g$

$$= e_G \star e'_G = e_G = e'_G$$

Admettons que l'inverse est unique et montrons que si $g, g' \in G$ $(g \star g')^{-1} = g'^{-1} \star g^{-1}$

On calcule

$$\begin{aligned}(g \star g') \star (g'^{-1} \star g^{-1}) &= g \star g' \star g'^{-1} \star g^{-1} \\ &= g \star e_G \star g^{-1} = g \star g^{-1}\end{aligned}$$

de meme :

$$(g'^{-1} \star g^{-1}) \star (g \star g') = e_G$$

Donc $g'^{-1} \star g^{-1}$ a les meme proprietes d'inversion que $(g \star g')$ et par unicite c'est $(g \star g')^{-1}$. \square

Definition 10 (Notation exponentielle)

(G, \cdot) un groupe et $g \in G$. On peut :

$$g \rightarrow g^{-1} g \cdot g, g \cdot g \cdot g, g \cdot g \cdot g \cdot g \dots$$

On peut faire ca n fois $n \geq 1$ un entier, on notera :

$$g \cdot g \cdot g \cdot g = g^n$$

si $n < 0$:

$$g^n := (g^{-1})^n = \underbrace{g^{-1} \cdot g^{-1} \cdot \dots \cdot g^{-1}}_{|n| \text{ fois}}$$

et $g^0 := e_G$

Exercice 10

Verifier que : $g^{m+n} = g^m \cdot g^n$

Definition 11 (exponentielle)

$$\begin{aligned}\exp_g : \mathbb{Z} &\rightarrow G \\ n &\rightarrow g^n\end{aligned}$$

On l'appelle l'exponentielle de n en base g .

$$\exp_g(m+n) = \exp_g(m) \cdot \exp_g(n)$$

Definition 12 (Notation multiple)

Si G est commutatif et que le groupe est note additivement

$$n \geq 1 \quad \underbrace{g + \dots + g}_{n \text{ fois}} = n \cdot g$$

Si $n < 0$

$$n \cdot g := \underbrace{(-g) + \dots + (-g)}_{|n| \text{ fois}}$$

Donc on a la notation

$$\forall m, n \in \mathbb{Z} (m+n) \cdot g = m \cdot g + n \cdot g$$

3 Sous-Groupe

Definition 13 (Sous-groupe)

Soit $(G, \star, e_G, \cdot^{-1})$ un groupe. Un sous-groupe $H \subset G$ est un sous-ensemble de G tq

1. $e_G \in H$

2. H est stable par la loi de composition

$$\forall h, h' \in H, h \star h' \in H$$

3. H est stable par l'inversion

$$\forall h \in H, h^{-1} \in H$$

$(H, \star, e_G, \cdot^{-1})$ forme un groupe

Proposition 11 (Critere de Sous-groupe)

Pour montrer que $\emptyset \neq H \subset G$ est un sous groupe il suffit de verifier l'une ou l'autre de ces proprietes :

1. a. $\forall h, h' \in H, h \star h' \in H$
b. $\forall h \in H, h^{-1} \in H$
2. $\forall h, h' \in H, h \star h'^{-1} \in H.$

Preuve

Montrons que H verifie le point 1 de la definition.

Comme $H \neq \emptyset$ il existe $h \in H$. Par hypothese $h \star h^{-1} \in H$.

On verifie la stabilite par inversion

Soit $h \in H$ et par hypothese $e_G \in H$ $e_G \star h^{-1} \in H$

On verifie la stabilite par produit

Soit $h, h' \in H$ alors $(h')^{-1} \in H$ et $h \star ((h')^{-1})^{-1} \in H$. Or

$$((h')^{-1})^{-1} = h' \Rightarrow h \star h' \in H \quad \square$$

Exemple

$(G, \cdot) g \in G$ et $g^{\mathbb{Z}} = \exp_g(\mathbb{Z}) = \{g^n, n \in \mathbb{Z}\}$ Forme un sous groupe.

Preuve

Soit $h, h' \in H = g^{\mathbb{Z}}$ alors

$$h = g^m h' = g^{m'} m, m' \in \mathbb{Z}$$

Alors

$$h \cdot h' = g^m \cdot g^{m'} = g^{m+m'} \in g^{\mathbb{Z}}$$

Soit $h \in g^{\mathbb{Z}} h = g^m$ comme $h^{-1} = g^{-m}$ alors $h^{-1} \in g^{\mathbb{Z}}$ \square

Exemple

1. $\{e_G\} \subset G$ est un sous groupe de G on l'appelle le sous groupe trivial de G .
2. $G \subset G$ est un sous groupe
3. $(\mathbb{Z}, +)q \in \mathbb{Z}$
4. $q \cdot \mathbb{Z} = \{a, a = q \cdot k, k \in \mathbb{Z}\}$

Preuve

On prouve la derniere propriete

- $0 \in q\mathbb{Z}$ car $0 = q \cdot 0$
- qk et $q \cdot k' \in q\mathbb{Z} \Rightarrow qk + qk' = q(k + k') \in q \cdot \mathbb{Z}$
- $qk \in q\mathbb{Z}$ □

Theorème 14 (Sous groupe de \mathbb{Z})

Reciproquement tout sousgroupe de \mathbb{Z} est de la forme $q \cdot \mathbb{Z}$.

Preuve

Soit $H \subset \mathbb{Z}$ un sous groupe

- si $h = \{0\}$, $H = 0 \cdot \mathbb{Z}$.
- si $H \neq \{0\}$ soit $q \in H \neq 0$

Alors, sans perte de generalite, on peut supposer que $q > 0$ (si $q < 0$ on remplace q par $-q \in H$)

Sans perte de generalite on peut supposer que q est le plus petit el strictement positif contenu dans H

$$q = q_{min} = \min(h \in H, h > 0)$$

On va montrer que $H = q\mathbb{Z}$.

Soit $h \in H$ par division euclidienne il existe $k \in \mathbb{Z}$ et $r \in \{0, \dots, q-1\}$ tq

$$\begin{aligned} h &= qk + r \\ r &= h - qk \in H \end{aligned}$$

□

Donc $0 \leq r < q \Rightarrow r = 0$ par def de q .

Donc $h = q \cdot k \in q\mathbb{Z}$.

3.1 Groupe engendre par un ensemble

Proposition 15 (Intersection de sous-groupes)

Soit G un groupe et $H_1, H_2 \subset G$ deux sous groupes alors $H_1 \cap H_2$ est un sous groupe. Plus généralement l'intersection de sous groupes est un sous-groupe.

Preuve

Cas $H_1 \cap H_2$. On veut montrer que c'est un sous groupe. On utilise la deuxième version du critère de la proposition 11.

$$\forall h, h' \in H_1 \cap H_2 \Rightarrow h \star h'^{-1} \in H_1 \cap H_2$$

Comme $h, h' \in H_1$ $h \star h'^{-1} \in H_1$ et $h, h' \in H_2$ $h \star h'^{-1} \in H_2$

Donc $h \star h'^{-1} \in H_1 \cap H_2$

$\Rightarrow H_1 \cap H_2$ est un sous-groupe □

Definition 14 (Sous-groupe engendre)

G un groupe et $A \subset G$ un sous-ensemble de G .

Le sous-groupe engendré par A , noté $\langle A \rangle \subset G$ est par définition le plus petit sous groupe de G contenant A .

Soit

$$G_A = \{H \subset G, H \text{ est un sous groupe et } A \subset H\}$$

G_A est non-vidé car il contient G .

Par la proposition précédente, on considère

$$\langle A \rangle := \bigcap_{H \in G_A} H$$

Par la proposition cette intersection est un sous groupe qui contient A et c'est le plus petit possible au sens où si $H \subset G$ est un sous groupe contenant A alors

$$\langle A \rangle = \bigcap_{H \in G_A} H \subset H'$$

Exemple

Si $g \in G$ $\langle \{g\} \rangle = g^{\mathbb{Z}} = \{g^n, n \in \mathbb{Z}\}$

Lecture 4: Groupes et Anneaux

Mon 28 Sep

Theorème 17

Soit $A \subset G$ un ensemble, si $A = \emptyset$ alors $\langle A \rangle = \{e_G\}$, sinon on pose

$$A^{-1} = \{g^{-1}, g \in A\} \subset G$$

l'image de A par l'inversion alors

$$\langle A \rangle = \{g_1 \star \dots \star g_n, g_i \in A \cup A^{-1}\}$$

En d'autres termes, $\langle A \rangle$ est l'ensemble des elements de G qu'on peut former en multipliant ensemble des elements de A et de son invers A^{-1} de toutes les manieres possibles.

Preuve

Pour montrer que c'est $\langle A \rangle$, on procede par double inclusion.

\supset : soit $H \subset G$ un ssgpe tq

$$A \subset H \subset G$$

Alors comme H est stable par \bullet^{-1}

$$A^{-1} \subset H^{-1} = H$$

Donc, $A \cup A^{-1} \subset H$ comme H est stable par \star , si $g_1, \dots, g_n \in A \cup A^{-1}$ Le produit $g_1 \star g_2 \star \dots \star g_n \in H$

Donc $\{g_1 \star g_2 \star \dots \star g_n, g_i \in A \cup A^{-1}\} \subset H$ et donc $\{g_1 \star g_2 \star \dots \star g_n, g_i \in A \cup A^{-1}\} \subset \bigcap_{A \subset H} H \subset \langle A \rangle$

\subset : il suffit de mq $\{\dots\}$ et un sous groupe de G . En effet, $\{g_1 \star \dots \star g_n, n \geq 1, g_i \in A \cup A^{-1}\} \supset A$

Critere de ss-groupe :

a) Soit $g \in A \Rightarrow g^{-1} \in A^{-1}, g \star g^{-1} = e_G \in \{g_1 \star \dots \star g_n, \dots\}$

b) Soit $g = g_1 \star g_2 \star \dots \star g_n$ et $g' = g'_1 \star g'_2 \star \dots \star g'_n$

$$n, n' \geq 1, g_i, g'_j \in A \cup A^{-1}$$

Alors

$$g \star g' = g_1 \star \dots \star g_n \star g'_1 \star \dots \star g'_n \in \{\dots\}$$

c) soit $g = g_1 \star \dots \star g_n$ comme ci-dessus

$$g^{-1} = g_n^{-1} \star g_{n-1}^{-1} \star \dots \star g_1^{-1} \in \{\dots\}$$

$\{\dots\}$ est un sousgroupe de G contenant A donc il contient $\langle A \rangle$. □

3.2 Morphismes de Groupes

Definition 15 (Morphisme de Groupe)

Soient (G, \star) et (H, \bullet) deux groupes, un morphisme de groupes $\phi : G \rightarrow H$ est une application telle que

$$\forall g, g' \in G, \phi(g \star g') = \phi(g) \bullet \phi(g')$$

Theorème 18

Soit $\phi : G \rightarrow H$ un morphisme de groupes alors

1. $\phi(e_G) = e_H$
2. $\forall g \in G, \phi(g^{-1}) = \phi(g)^{-1}$

$$3. \forall g, g' \in G, \phi(g \star g') = \phi(g) \bullet \phi(g')$$

Preuve

Il suffit de demontrer 1 et 2, 3 est vrai par definition.

1)

Soit $g \in G, \phi(g) = \phi(g \star e_G) = \phi(g) \bullet \phi(e_G)$.

Donc $\phi(g) = \phi(g) \star \phi(e_G)$ et donc

$$\begin{aligned} h &= h \bullet \phi(e_G) \\ h^{-1} \bullet h &= h^{-1} \bullet h \bullet \phi(e_G) \end{aligned}$$

2)

$$\begin{aligned} \phi(g) \bullet \phi(g)^{-1} &= e_H \\ \phi(g) \bullet \phi(g^{-1}) &= \phi(g \star g^{-1}) \\ &= \phi(e_G) = e_H \end{aligned}$$

On conclut en utilisant l'unicite de l'inverse

$$\phi(g^{-1}) = \phi(g)^{-1} \quad \square$$

Definition 16 (Notations)

- $\text{Hom}_{Gr}(G, H)$ l'ensemble des morphismes de groupe entre G et H .
- $\text{End}_{Gr}(G) = \text{Hom}_{Gr}(G, G)$ les endomorphismes du groupe G .
- $\text{Isom}_{Gr}(G, H)$ l'ensemble des morphismes bijectifs
- $\text{Aut}_{Gr}(G) = \text{Isom}_{Gr}(G, G)$ l'ensembles des automorphismes du groupe G .

Exemple

—

$$e_H : \begin{cases} G \rightarrow H \\ g \rightarrow e_h \end{cases}$$

— Soit $g \in G$

$$\exp_G : \begin{cases} \mathbb{Z} \rightarrow G \\ n \rightarrow g^n \end{cases}$$

Si G est commutatif note additivement

$$\bullet.g : \begin{cases} \mathbb{Z} \rightarrow G \\ n \rightarrow n.g \end{cases}$$

Conjugaison dans un groupe : (G, \cdot)

$$h \in G$$

$$Ad_h : \begin{cases} G \rightarrow G \\ g \rightarrow h.g.h^{-1} \end{cases}$$

Preuve

On veut montrer que $\forall g, g' \in G$

$$Ad_h(g.g') = Ad_h(g).Ad_h(g')$$

$$\begin{aligned} Ad_h(g).Ad_h(g') &= (h.g.h^{-1}).(h.g'.h^{-1}) \\ &= h.g.h^{-1}.h.g'.h^{-1} \\ &= h.g.e_G.g'.h^{-1} &= h.g.g'.h^{-1} = Ad_h(g.g') \end{aligned}$$

Terminologie :

$$Ad_h(g) = h.g.h^{-1} \quad \square$$

Le conjugué de g par g .

Remarque

$Ad_h : G \rightarrow G$ est bijectif. Ad_h admet une application réciproque qui est Ad_h^{-1}

Preuve

$$Ad_{h^{-1}} \circ Ad_h = Id_G$$

$$Ad_h \circ Ad_{h^{-1}} = Id_G$$

Il suffit de montrer le premier.

$$\begin{aligned} Ad_{h^{-1}} \circ Ad_h(g) &= h^{-1}.(h.g.h^{-1}).h \\ &= h^{-1}.h.g.h^{-1}.h \\ &= g = Id_G(g) \end{aligned}$$

$$\text{car } (h^{-1})^{-1} = h \quad \square$$

$$\forall h \in G,$$

$$Ad_h \in Aut_{Gr}(G)$$

Proposition 21

Soient $(G, \star), (H, *), (K, \bullet)$ des groupes et $\phi : G \rightarrow H$ et $\psi : H \rightarrow K$ des morphismes de groupes alors la composée $\psi \circ \phi : G \rightarrow K$ est un morphisme de groupes

Preuve

On veut montrer que

$$\psi \circ \phi(g \star g') = ? \psi \circ \phi(g) \bullet \psi \circ \phi(g')$$

on a :

$$\begin{aligned} \psi \circ \phi(g \star g') &= \psi(\phi(g \star g')) \\ &= \psi(\phi(g) * \phi(g')) \\ &= \psi(\phi(g)) \bullet \psi(\phi(g')) \end{aligned} \quad \square$$

Proposition 22

Soit $\phi : G \rightarrow H$ un morphisme de groupe bijectif alors l'application reciproque ϕ^{-1} est un morphisme bijectif.

Preuve

Soit $\phi : G \rightarrow H$ un morphisme de groupe bijectif (en tant qu'application), on veut montrer que $\phi^{-1} : H \rightarrow G$ verifie

$$\phi^{-1}(h \star h') = ? \phi^{-1}(h) * \phi^{-1}(h'), \forall h, h' \in H$$

On calcule

$$\begin{aligned} \phi(\phi^{-1}(h) * \phi^{-1}(h')) &= \phi(\phi^{-1}(h)) \star \phi(\phi^{-1}(h')) \\ &= h \star h' \\ \Rightarrow \phi^{-1}(h) * \phi^{-1}(h') & \end{aligned} \quad \square$$

est un antecedent de $h \star h'$ mais le seul antecedent de $h \star h'$ c'est $\phi^{-1}(h \star h')$
 $\Rightarrow \phi^{-1}(h) * \phi^{-1}(h') = \phi^{-1}(h \star h')$

Definition 17 (Groupes Isomorphes)

Soient G et H deux groupes si

$$Isom_{gr}(G, H) \neq \emptyset$$

On dit que G et H sont isomorphes (comme groupes)

$$G \simeq_{Gr} H$$

et si $Isom_{gr}(G, H) \neq \emptyset$ alors $Isom_{Gr}(H, G) \neq \emptyset, H \simeq_{Gr} G$

La relation “etre isomorphe” dans la categorie des groupes est une relation d'equivalence :

- $G \simeq_{Gr} G$ ($Isom_{Gr}(G, G) \ni Id_G$)
- Si $G \simeq_{Gr} H \Rightarrow H \simeq_{Gr} G$

— Si $G \simeq_{Gr} H$ et $H \simeq_{Gr} K \Rightarrow G \simeq_{Gr} K$

Exemple

Le groupe des automorphismes d'un groupe

$$Aut_{Gr}(G) = Isom_{Gr}(G, G) \subset Bij(G)$$

Theorème 24

$Aut_{Gr}(G)$ est un sous-groupe de $(Bij(G), \circ, Id_G, \bullet^{-1})$

Preuve

Si ϕ et $\psi \in Isom_{Gr}(G, G)$, alors $\psi \circ \phi$ est un morphisme et $\psi \circ \phi$ est bijectif

$\Rightarrow \psi \circ \phi \in Isom_{Gr}(G, G)$

Si $\phi \in Isom_{Gr}(G, G) \cup Bij(G, G)$ alors ϕ^{-1} est un morphisme donc

$$Isom_{Gr}(G, G) = Aut_{Gr}(G) \quad \square$$

Lecture 5: Noyau et Image

Tue 29 Sep

4 Noyau et Image

Proposition 25

Soit $\phi \in Hom_{Gr}(G, H)$ un morphisme de groupes.

— Soit $K \subset G$ un sous groupe alors $\phi(K) \subset H$ est un sous-groupe. En particulier l'image de ϕ ,

$$Im(\phi) = \phi(G)$$

— Soit $L \subset H$ un sous-groupe de H , alors l'image inverse

$$\phi^{-1}(L) = \{g \in G, \phi(g) \in L\} \subset G$$

est un sous-groupe de G . En particulier, $\phi^{-1}(\{e_H\})$ est un sous-groupe

Preuve

Soit $K \subset G$ un sous-groupe.

Soit

$$h, h' \in \phi(K)$$

On veut montrer que $h \star h'^{-1} \in \phi(K)$.

Il existe $k, k' \in K$ tel que $\phi(k) = h, \phi(k') = h'$

$$\begin{aligned} h \star h'^{-1} &= \phi(k) \star \phi(k')^{-1} \\ &= \phi(k) \star \phi(k'^{-1}) \end{aligned}$$

$$= \phi(k * k'^{-1}), \quad k * k'^{-1} \in K$$

car K sous-groupe.

$$h * h'^{-1} \in \phi(K)$$

Soit $L \subset H$ un sous-groupe, on veut montrer que

$$\phi^{-1}(L) \subset G$$

est un sous-groupe Soient $g, g' \in \phi^{-1}(L)$, alors $\phi(g) = h \in L, \phi(g') = h' \in L$

$$g * g'^{-1} \in \phi^{-1}(L)?$$

on a

$$\begin{aligned} \phi(g * g'^{-1}) &= \phi(g) * \phi(g')^{-1} \\ &= h * h'^{-1} \in L \text{ car } L \text{ sous-groupe} \end{aligned} \quad \square$$

Definition 18

Le sous-groupe $\phi^{-1}(\{e_H\})$ s'appelle le noyau de ϕ et est noté

$$\ker(\phi) = \phi^{-1}(\{e_H\}) = \{g \in G, \phi(g) = e_H\}$$

L'importance du noyau vient du fait qu'il permet de tester facilement si un morphisme est injectif.

Theorème 26 (Critère d'injectivité)

Soit $\phi \in \text{Hom}_{Gr}(G, H)$ un morphisme de groupes alors les propriétés suivantes sont équivalentes

- ϕ est injectif
- $\ker(\phi) = \{e_G\}$

Preuve

1 \rightarrow 2

si ϕ est injectif, l'image réciproque de $\{e_H\}$ possède au plus un seul élément.

Mais comme ϕ est un morphisme $\phi(e_G) = e_H \Rightarrow \phi^{-1}(\{e_H\}) = \{e_G\}$

2 \rightarrow 1

On se donne $h \in H$ et on veut montrer que $\phi^{-1}(\{h\}) = \{g \in G, \phi(g) = h\}$ n'a pas plus d'un élément.

Si $\phi^{-1}(\{h\}) = \emptyset$ OK

Si $\phi^{-1}(\{h\}) \neq \emptyset$, soient $g, g' \in \phi^{-1}(\{h\})$ on veut montrer que $g = g'$.

Par définition, $\phi(g) = \phi(g') = h$

$$\phi(g) * \phi(g')^{-1} = e_H$$

$$= \phi(g * g'^{-1}) \text{ car } \phi \text{ morphisme}$$

Donc, $g * g'^{-1} \in \ker(\phi) = \{e_G\}$,

$$\Rightarrow g * g'^{-1} = e_G \Rightarrow g = g' \quad \square$$

Exemple

Ordre d'un element

Soit $g \in G$ groupe

$$\exp_g : \mathbb{Z} \rightarrow G, n \in (\mathbb{Z}, +) \rightarrow g^n \in G$$

est un morphisme de groupes.

$$\ker(\exp_g) \subset \mathbb{Z}q, q \in \mathbb{Z}$$

Si $q = 0$, $\ker(\exp_q) = \{0\}$

$$\Rightarrow \mathbb{Z} \rightarrow G$$

$n \rightarrow g^n$ est injective

\mathbb{Z} est isomorphe à $g^{\mathbb{Z}}$ ($\mathbb{Z} \simeq g^{\mathbb{Z}}$)

$$G \supset g^{\mathbb{Z}} \simeq \mathbb{Z}$$

donc g est d'ordre infini.

Si $q > 0$, alors

$$g^{\mathbb{Z}} = \{g^0 = e_G, g, g^2, \dots, g^{q-1}\}$$

est un sous-groupe de cardinal q (à démontrer en exercice) et donc G contient un sous-groupe d'ordre q

$$q := \text{ordre de } g = \text{ord}(g)$$

q est le plus petit entier > 0 tel que

$$g^q = e_G$$

Exemple (Conjugaison)

$G \ni h$

$$\text{Ad}_h : g \rightarrow h.g.h^{-1}$$

On a montré que $\text{Ad}_h \in \text{Aut}_{\text{Gr}}(G)$

On considère l'application

$$h \in G \rightarrow \text{Ad}_h \in \text{Aut}_{\text{Gr}}(G)$$

Cette application est un morphisme de groupes :

On doit verifier que : $\forall h, h' \in G$

$$Ad_{h.h'} = Ad_h \circ Ad_{h'}$$

On veut montrer que pour tout $g \in G$

$$Ad_{h.h'} = Ad_h(Ad_{h'}(g))$$

$$\begin{aligned} h.h'.g.(h.h')^{-1} &= h.h'.g.h'^{-1}.h^{-1} \\ &= h.(h'.g.h'^{-1}).h^{-1} \\ &= Ad_h(Ad_{h'}(g)) \\ \ker(Ad) &= \{h \in G | Ad_h = Id_G\} \\ &= \{h \in G | \forall g \in G Ad_h(g) = g\} \\ &= \{h \in G | \forall g \in G, h.g.h^{-1} = g\} \\ h.g.h^{-1} = g &\iff h.g = g.h \end{aligned}$$

On dit que h commute avec g .

$$\begin{aligned} \ker(Ad) &= \{ \text{l'ensemble des } h \text{ dans } G \text{ qui commutent avec tous les elements de } G \} \\ &= \text{Centre de } G \\ &= Z(G) = Z_G \end{aligned}$$

Z_G est un groupe commutatif de G

Exemple (Translation)

Soit $h \in G$ la translation a gauche par h

$$t_h : \begin{cases} G \rightarrow G \\ g \rightarrow h.g \end{cases}$$

Attention t_h n'est pas un morphisme de groupes, car l'element neutre ne va pas sur lui meme (sauf si $h = e_G, t_h = t_{e_G} = Id_G$)

Par contre t_h est bijective de reciproque $t_{h^{-1}}$

$t_\bullet : h \in G \rightarrow t_h \in \text{Bij}(G)$ est un morphisme de groupe injectif, l'image s'appelle le groupe des translations (a gauche) de G .

Donc $G \simeq t_G \subset \text{Bij}(G)$

Tout groupe G abstrait peut s'identifier (est isomorphe) a un sous-groupe d'un groupe de bijections d'un ensemble.

5 Anneaux

Definition 19 (Anneaux)

Un anneau $(A, +, \cdot, 1_A)$ est la donnée, d'un groupe commutatif $(A, +)$ (note additivement) d'élément neutre noté 0_A , d'une loi de composition interne (dite de multiplication)

$$\bullet \bullet \begin{cases} A \times A \rightarrow A \\ (a, b) \rightarrow a.b \end{cases}$$

et d'un élément unité $1_A \in A$ ayant les propriétés suivantes

1. Associativité de la multiplication

$$\forall a, b, c \in A, (a.b).c = a.(b.c) = a.b.c$$

2. Distributivité

$$\forall a, b, c \in A (a + b).c = a.c + b.c, c.(a + b) = c.a + c.b$$

3. Neutralité de l'unité

$$\forall a \in A, a.1_A = 1_A.a = a$$

Un anneau est dit commutatif si de plus la multiplication est commutative

$$\forall a, b \in A, a.b = b.a$$

Lemme 30

Pour tout $a, b \in A$, on a

$$0_A.a = a.0_A = 0_A$$

On dit que l'élément neutre de l'addition 0_A est absorbant. Pour l'opposé, on a

$$(-a).b = -(a.b) = a.(-b)$$

Preuve

$\forall a \in A$

$$a = a.1_A = a.(1_A + 0_A)$$

$$= a.1_A + a.0_A$$

$$0_A = a.0_A$$

□

Exemple

— L'anneau nul : $\{0\}$

- $\mathbb{Z}, (\mathbb{Q}, +, \bullet), (\mathbb{R}, +, \bullet)$
- $\mathcal{F}(X, \mathbb{R})$ des fonctions d'un ensemble X a valeurs dans \mathbb{R} .

$$+ : f + g : x \in X \rightarrow f(x) + g(x) = (f + g)(x)$$

$$0_{\mathcal{F}(X, \mathbb{R})} : x \rightarrow 0 \in \mathbb{R}$$

$$1_{\mathcal{F}(X, \mathbb{R})} : x \rightarrow 1 \in \mathbb{R}$$

$(\mathcal{F}(X, A), +, \bullet)$ est un anneau (commutatif si A commutatif) generalisation du cas des fonctions reelles

- $\mathbb{R}[x] = \{P(x) = a_0 + a_1x + \dots + a_dx^d, a_0, a_1, \dots, a_d \in \mathbb{R}, d \geq 0\}$
- $A[x] = \{P(x) = a_0 + a_1x + \dots + a_dx^d, a_0, \dots, a_d \in A, d \geq 0\}$
Anneau des polynomes a coefficients dans A .
- $(M, +)$ un groupe commutatif

$$\text{End}(M) = \text{End}_{Gr}(M) = \text{Hom}_{Gr}(M, M)$$

$$+ : \psi, \phi \in \text{End}(M)$$

$$\phi + \psi : m \rightarrow \phi(m) + \psi(m)$$

Soient $\phi, \psi \in \text{End}(M)$

$$\phi \circ \psi \in \text{End}(M)$$

$$0_{\text{End}(M)} : m \in M \rightarrow 0_M \in M$$

$$1_{\text{End}(M)} : Id_M : m \in M \rightarrow m \in M$$

$(\text{End}(M), +, \circ, 0_M, Id_M)$ est un anneau

Lecture 6: Anneaux 2

Mon 05 Oct

Preuve

Soit $\phi, \psi \in \text{End}_{Gr}(M)$, on veut montrer que

$$\phi + \psi \in \text{End}_{Gr}(M)$$

Pour vérifier cela, on utilise le critère de morphisme : $\forall m, m' \in M$, alors

$$(\phi + \psi)(m + m') = (\phi + \psi)(m) + (\phi + \psi)(m')$$

$$\begin{aligned} (\phi + \psi)(m + m') &= \phi(m + m') + \psi(m + m') \\ &= \phi(m) + \psi(m') + \psi(m) + \psi(m') \end{aligned}$$

$+$ est commutative

$$\begin{aligned} &= \phi(m) + \psi(m') + \phi(m') + \psi(m') \\ &= (\phi + \psi)(m) + (\phi + \psi)(m') \end{aligned}$$

Soit $\phi, \psi, \psi' \in \text{End}_{Gr}(M)$ on veut montrer que

$$\phi \circ (\psi + \psi') = \phi \circ \psi + \phi \circ \psi'$$

On veut montrer que $\forall m \in M$

$$\phi \circ (\psi + \psi')(m) = (\phi \circ \psi + \phi \circ \psi')(m)$$

$$\begin{aligned} \phi((\psi + \psi')(m)) &= \phi(\psi(m) + \psi'(m)) \\ &= \phi(\psi(m)) + \phi(\psi'(m)) \\ &= (\phi \circ \psi + \phi \circ \psi')(m) \end{aligned}$$

Reste à faire : associativité de +
 0_M est l'élément neutre de +
 Id_M est l'unité pour \circ

□

5.1 Élément inversible

Definition 20 (Element Inversible)

Un element $a \in A$ est inversible si il existe $b \in A$ tel que

$$a.b = b.a = 1_A.$$

On dit alors que b est un inverse de a (pour la multiplication).

Remarque

Si l'inverse existe, l'inverse est unique, et on le note a^{-1} .

Notation :

On note A^\times l'ensemble des éléments inversibles de A .

Proposition 33

Soit A^\times l'ensemble des éléments inversibles, alors

$$(A^\times, \cdot, 1_A, \bullet^{-1})$$

forme un groupe : le groupe des éléments inversibles de A .

Exemple

- $\mathbb{Z}^\times = \{\pm 1\}$, $\mathbb{Q}^\times = \mathbb{Q} \setminus \{0\}$
- $\mathbb{R}^\times = \mathbb{R} \setminus \{0\}$
- $\mathcal{F}(X, \mathbb{R})^\times = \{f : X \rightarrow \mathbb{R} \mid f(x) \neq 0_{\mathbb{R}} \text{ pour tout } x \in X\}$
- $\mathbb{R}[x]^\times = \{a_0 \mid a_0 \in \mathbb{R}^\times\}$
- $\text{End}_{Gr}(M)^\times = \text{Aut}_{Gr}(M) = \text{Isom}_{Gr}(M, M)$

5.2 Sous-Anneau

Definition 21 (Sous-Anneau)

Soit $(A, +, \cdot)$ un anneau. Un sous-anneau $B \subset A$ est un sous-groupe de $(A, +)$ qui est

- soit le sous-groupe trivial $\{0_A\}$,
- soit qui contient l'unité 1_A et qui est stable par \cdot :

$$\forall b, b' \in B, b \cdot b' \in B$$

Ainsi $(B, +, \cdot)$ est un anneau.

Lemme 35 (Critère de sous-anneau)

Soit $(A, +, \cdot)$ un anneau et $B \subset A$ un sous-ensemble non-vidé alors B est un sous-anneau ssi $B = \{0_B\}$ ou bien $1_A \in B$ et

$$\forall b, b', b'' \in B, b \cdot b' - b'' \in B$$

Preuve

Si $B = \{0_A\}$ c'est un sous-anneau.

Sinon $1_A \in B$ si on prend $b \in B$ alors

$$0_A = 1_A \cdot b - b \in B$$

Alors

$$\forall b, b' \in B$$

$$b - b' = 1_A \cdot b - b' \in B$$

Donc $(B, +)$ est un sous-groupe.

Soient $b, b' \in B$ alors

$$b \cdot b' - 0_A \in B$$

□

$$= b \cdot b'.$$

Exemple

- $\{0_A\} \subset A \subset A$
- $\mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}$
- A un anneau

$$A.Id_A := \{a.Id_A : b \mapsto a \cdot b\} \subset End_{Gr}(A).$$

est un sous-anneau

5.3 Morphismes d'anneaux

Definition 22 (Morphisme d'anneaux)

Soient $(A, +, \cdot)$, et $(B, +, \cdot)$ des anneaux. Un morphisme d'anneaux $\phi : A \mapsto B$ est un morphisme de groupes commutatif $\phi : (A, +) \mapsto (B, +)$ tel que

$$\phi(1_A) = 1_B \text{ ou bien } \phi(1_A) = 0_B$$

$$\forall a, a' \in A, \phi(a.a') = \phi(a).\phi(a')$$

Remarque

Si $\phi(1_A) = 0_B$ alors $\phi = 0_B$

Alors $\forall a \in A$

$$\begin{aligned}\phi(a) &= \phi(a.1_A) \\ &= \phi(a)\phi(1_A) = 0_B\end{aligned}$$

Notation : On note les morphismes d'anneaux de A vers B

$$Hom_{Ann}(A, B), End_{Ann}(A) = Hom_{Ann}(A, A), Isom_{Ann}(A, B), Aut_{Ann}(A) = Isom_{Ann}(A, A)$$

Exemple (Le morphisme canonique)

Le morphisme canonique :

$$Can_A : (\mathbb{Z}, +, \cdot) \rightarrow (A, +, \cdot)$$

$$n \rightarrow n.1_A = 1_A + 1_A + \dots + 1_A \text{ } n \text{ fois si } n \geq 0 \text{ et } -n \text{ fois si } n < 0$$

est un morphisme d'anneaux.

On doit vérifier que Can_A est un morphisme entre les groupes additifs.

On doit montrer que $\forall m, n \in \mathbb{Z}$

$$(m \times n).1_A = m.(n.1_A)$$

si m et $n \geq 0$

$$\begin{aligned}(m \times n).1_A &= \underbrace{1_A + \dots + 1_A}_{m \times n \text{ fois}} \\ &= \underbrace{1_A + \dots + 1_A}_{n \text{ fois}} + \underbrace{1_A + \dots + 1_A}_{n \text{ fois}} \text{ } m \text{ fois} \\ &= m.(n.1_A)\end{aligned}$$

5.4 Noyau/Image

Proposition 39 (Noyau d'un morphisme d'anneau)

Soient $\phi \in Hom_{Ann}(A, B)$ un morphisme alors $\phi(A) \subset B$ est un sous-anneau. Par ailleurs le sous-groupe $\ker(\phi)$ est stable par multiplication par A :

$$\forall a \in A, k \in \ker(\phi) a.k \in \ker(\phi)$$

Preuve

Soit $k \in \ker \phi, a \in A$

$$a.k \in \ker \phi?$$

$$\phi(a.k) = \phi(a).\phi(k) = \phi(a).0_B = 0_B$$

□

Theorème 40

$\phi(A) \subset B$ est un sous-anneau de B .

Preuve

Si $\phi(1_A) = 0_B \Rightarrow \phi = \underline{0}_B$ et donc $\phi(A) = \{0_B\} \subset B$

Sinon $\phi(1_A) = 1_B$. $B' = \phi(A)$ alors $1_B \in B'$, $\phi(A)$ est un sous-groupe de $(B, +)$

Soit $b, b' \in B' = \phi(A)$.

$$b = \phi(a), b' = \phi(a')a, a' \in A$$

Alors

$$b.b' = \phi(a).\phi(a') = \phi(a.a') \text{ car } \phi \text{ est un morphisme d'anneaux} \quad \square$$

5.5 Modules sur un Anneau**Definition 23 (Modules sur un Anneau)**

Soit A un anneau, un A -module (à gauche) est un groupe commutatif $(M, +)$ muni d'une loi de multiplication externe

$$\bullet * \bullet : A \times M \mapsto M$$

$$(a, m) \mapsto a * m$$

(appelée multiplication par les scalaires) ayant les propriétés suivantes

— Associativité : $\forall a, a' \in A, m \in M$,

$$(a.a') * m = a.(a' * m).$$

— Distributivité : $\forall a, a' \in A, m, m' \in M$,

$$(a + a') * m = a * m + a' * m, a * (m + m') = a * m + a * m'.$$

— Neutralité de 1_A : $\forall m \in M$,

$$1_A.m = m$$

Exemple

— $\{0_A\} \subset A$ est un A -module

— A est un A -module

— $(M, +)$ = groupe commutatif est canoniquement un \mathbb{Z} -module

$$\begin{aligned} \mathbb{Z} \times M &\rightarrow M \\ (n, \vec{m}) &\rightarrow n * \vec{m} = \underbrace{\vec{m} + \vec{m} + \dots}_{n \text{ fois}} \end{aligned}$$

Lecture 7: Anneaux Et Modules

Tue 06 Oct

$$A^d = \{(a_1, \dots, a_d) \mid a_1, \dots, a_d \in A\}$$

C'est un A -module : le A -module libre de rang d . Soit

$$\begin{aligned}\vec{x} &= (a_1, \dots, a_d) \\ \vec{x}' &= (a'_1, \dots, a'_d) \\ &\in A^d \\ \vec{x} + \vec{x}' &= (a_1 + a'_1, \dots)\end{aligned}$$

Soit

$$\begin{aligned}a \in A, \vec{x} \in A^d \\ a \cdot \vec{x} &:= (a \cdot a_1, \dots, a \cdot a_d)\end{aligned}$$

On vérifie (en utilisant l'associativité de $(A, +, \cdot)$ et la distributivité dans A) que A^d est un A -module.

$$1_A \cdot \vec{x} = \vec{x}$$

Exemple

— $\phi : A \rightarrow B$, $\ker \phi$ est un A module pour la multiplication dans A .

$$\begin{aligned}\bullet \bullet : A \times \ker \phi &\rightarrow \ker \phi \\ (a, k) &\rightarrow a \cdot k\end{aligned}$$

— $\mathcal{F}(X, A)$ fonctions de X (un ensemble quelconque) à valeurs dans A , on a vu que $\mathcal{F}(X, A)$ un groupe commutatif

$$\begin{aligned}A \times \mathcal{F}(X, A) &\rightarrow \mathcal{F}(X, A) \\ (a, f) &\rightarrow a \cdot f : x \mapsto a \cdot f(x)\end{aligned}$$

Plus généralement, si M est un A -module $\mathcal{F}(X, M)$ est un A -module.

$$\begin{aligned}a \in A, f : X &\rightarrow M \\ a * f : x &\rightarrow a * f(x) \in M\end{aligned}$$

Remarque

Si X possède d éléments

$$\mathcal{F}(X, A) = A^\times \simeq A^d$$

Definition 24 (A-Algebre)

Une A -algebre est un anneau $(B, +, \cdot)$ possédant une structure de A -module qui vérifie la propriété d'associativité suivante :

$$\forall a \in A, b, b' \in B \quad a * (b \cdot b') = (a * b) \cdot b'$$

$\mathbb{R}[x]$ est une \mathbb{R} -algèbre.

5.6 Sous-Module

Definition 25 (Sous-Module)

Un sous-module $N \subset M$ d'un A -module M est un sous-groupe de M qui est stable pour la multiplication par les scalaires

$$\forall a \in A, n \in N, a * n \in N$$

Definition 26 (Ideal)

Un idéal de A est un sous-ensemble $I \subset A$ qui est un sous-module du module A . De manière équivalente, un idéal de A est un sous-groupe $I \subset A$ qui est stable par multiplication par les éléments de A :

$$\forall a \in A, b \in I, a.b \in I$$

Remarque

Tout idéal $I \subset A$ est un noyau d'un morphisme d'anneau.

Lemme 45 (Critère de Sous-Module)

Soit $N \subset M$ un sous-ensemble d'un A -module M alors N est un sous-module de M ssi

$$\forall a \in A, n, n' \in N, a * n + n' \in N.$$

Preuve

Si on prend $a = -1_A$, on a que

$$\begin{aligned} \forall n, n' \in N, -1_A * n + n' &\in N \\ -n + n' &\in N \end{aligned}$$

Donc N vérifie le critère de sous-groupe, donc est un sous-groupe de $(M, +)$.

Comme N est un sous-groupe $0_M \in N$, et $\forall a \in A \forall n \in N$

$$a * n = a * n + 0_M \in N$$

N vérifie les 2 propriétés requises pour être un sous-module. □

Exemple

$\{0_M\} \subset M$ est clairement stable par multiplication

- $d \leq d', A[x]_{\leq d} \leq A[x]_{\leq d'} \leq A[x]$
- $\Delta A = \{(a, \dots, a) = a.(1, \dots, 1)\} \subset A^d$ ΔA est un sous-module de A^d .
- Plus généralement,

$$\vec{x} = (a_1, \dots, a_d), A.\vec{x} = \{a.\vec{x} = (a.a_1, \dots, a.a_d) | a \in A\}$$

est un sous-module de A^d .

Preuve

Soient $a \in A, \vec{v}, \vec{v'} \in A.\vec{x}$

$$\begin{aligned}\vec{v} &= a'.(a_1, \dots, a_d) = a'.\vec{x} \\ \vec{v'} &= a''.(a_1, \dots, a_d) = a''.\vec{x}\end{aligned}$$

Critère de sous-module :

$$a.\vec{v} + \vec{v'} = a.a'.\vec{x} + a''.\vec{x} = (a.a' + a'').\vec{x} \in A.\vec{x} \quad \square$$

5.7 Module engendré par un ensemble**Proposition 47**

Soit M un A -module et M_1, M_2 des sous-modules alors

$$M_1 \cap M_2 \subset M$$

est un sous-module et plus généralement soit $(M_i)_{i \in I}$ une collection de sous-modules alors

$$\bigcap_{i \in I} M_i \subset M$$

est un sous-module.

Definition 27

Soit $X \subset M$ un sous-ensemble d'un A -module, le module engendré par X est le plus petit sous-module de M contenant X (l'intersection de tous les sous-modules contenant X)

$$\langle X \rangle := \bigcap_{X \subset N \subset M} N.$$

Theorème 48

Soit $X \subset M$ un ensemble alors $\langle X \rangle$ est soit le module nul $\{0_M\}$ si X est vide, soit l'ensemble des combinaisons linéaires d'éléments de X à coefficients dans A :

$$\langle X \rangle = CL_A(X) := \left\{ \sum_{i=1}^n a_i * x_i, n \geq 1, a_1, \dots, a_n \in A, x_1, \dots, x_n \in X \right\}.$$

Pour tout $n \geq 1$.

Preuve

$CL_A(X)$ on va montrer que $CL_A(X)$ est un sous-module contenant X

$$\Rightarrow \langle X \rangle \subset CL_A(X)$$

ensuite on va montrer que si $X \subset N \subset M$ est un sous-module contenant X alors

$$\begin{aligned} N &\supset CL_A(X) \\ \Rightarrow CL_A(X) &\subset \langle X \rangle \end{aligned}$$

On utilise le critère de sous-module :

Soit $a \in A, u, v \in CL_A(X)$

$$a * u + v \in CL_A(X)$$

Or

$$\begin{aligned} u &= a_1 x_1 + \dots + a_n x_n, a_i \in A, x_i \in X \\ v &= a'_1 x'_1 + \dots + a'_m x'_m a'_j \in A, x'_j \in X \\ a * u + v &= a.a_1 * x_1 + \dots + a.a_n * x_n + a'_1 * x'_1 + \dots + a'_m * x'_m \in CL_A(X) \end{aligned}$$

$$X \subset CL_A(X)$$

car

$$x = 1_A.x = \text{combinaison linéaire de longueur 1} \quad \square$$

Soit $X \subset N \subset M$ un sous-module et soit $n \geq 1, a_1, \dots, a_n \in A$

$$x_1, \dots, x_n \in X$$

Alors comme N est stable par $*$ et que $x_1, \dots, x_n \in X \subset N$

$$\Rightarrow a_1 * x_1 + \dots + a_n * x_n \in N$$

Lecture 8: Modules et Corps

Mon 12 Oct

5.8 Morphismes de Modules

Definition 28 (Morphismes de Module)

Soit A un anneau et M, N des A -modules, un morphisme de A -modules entre M et N est un morphisme de groupes

$$\phi : M \rightarrow N$$

qui est compatible avec les lois de multiplication externes $*_M$ et $*_N$:

$$\forall a \in A, m \in M, \phi(a *_M m) = a *_N \phi(m)$$

On dit aussi que ϕ est une application A -linéaire.

Remarque

$$\forall a, a' \in A, m, m' \in M$$

$$\phi(a *_M m + a' *_M m') = \phi(a *_M m) + \phi(a' *_M m') = a *_N \phi(m) + a' *_N \phi(m')$$

Lemme 50 (Critere de l'application lineaire)

Soit $\phi : M \rightarrow N$ une application entre deux modules alors ϕ est un morphisme si et seulement si

$$\forall a \in A, m, m' \in M, \phi(a *_M m + m') = a *_N \phi(m) + \phi(m')$$

Preuve

\Rightarrow a été fait ci-dessus.

\Leftarrow :

Si on prend $a = -1_A$, on obtien

$$\forall m, m' \quad \phi(-m + m') = -\phi(m) + \phi(m')$$

en prenant $m = m'$ on obtient $\phi(0) = 0$, et en prenant $a = 1$, on a

$$\phi(m + m') = \phi(m) + \phi(m')$$

$\Rightarrow \phi$ est un morphisme de groupes additifs.

Si on prend $m' = 0_M$

$$\begin{aligned} \phi(a *_M m + 0_M) &= \phi(a *_M m) \\ &= a *_N \phi(m) + \phi(0_M) = a *_N \phi(m) \end{aligned}$$

Proposition 51

Soit $\phi : M \rightarrow N$ un morphisme de A -module et $M' \subset M$ et $N' \subset N$ des sous-modules, alors

$$\phi(M') \subset N \text{ et } \phi^{-1}(N') \subset M$$

sont des sous-modules de M et N respectivement. En particulier

$$\ker \phi = \phi^{-1} \{0_N\} \subset M \text{ et } \text{Im} \phi \subset N$$

Preuve

Comme ϕ est un morphisme de groupes $\phi(M') \subset N$ est un sous-groupe de N et $\phi^{-1}(N') \subset M$ est un sous-groupe de M Reste a vérifier la stabilité par $*$.

On veut montrer que si $m' \in \phi^{-1}(N')$ alors

$$\forall a \in A \quad a *_M m' \in \phi^{-1}(N')$$

$$m' \in \phi^{-1}(N') \Rightarrow \phi(m') \in N'$$

Comme N' est un sous-module

$$a *_N \phi(m') \in N'$$

msid comme ϕ est linéaire

$$a *_N \phi(m') = \phi(a *_M m') \Rightarrow a *_M m' \in \phi^{-1}(N')$$

- Si $M' \subset M$ est un sous-module alors $\phi(M')$ est un sous-module.
- On sait que $\phi(M') \subset N$ est un sous-groupe

Reste à vérifier que $\phi(M')$ est stable par $*$ dans A .

Soit $n' \in \phi(M')$ alors $n' = \phi(m'), m' \in M'$ Soit $a \in A$, $a *_N n' = a *_N \phi(m') = \phi(a *_M m')$

Comme M' est un sous-module

$$a *_M m' \in M' \text{ et donc } a *_N n' = \phi(a *_M m') \in \phi(M')$$

□

Remarque

Le critère d'injectivité s'applique à un morphisme de A -modules est injectif ssi $\ker \phi = \{0_m\}$ C'est vrai parce que c'est vrai quand on voit ϕ comme un morphisme de groupes.

5.9 Structures Algébriques des espaces de morphismes

Definition 29

On note

$$\begin{aligned} \text{Hom}_{A\text{-mod}}(M, N), \text{Isom}_{A\text{-mod}}(M, N) \\ \text{End}_{A\text{-mod}}(M), &= \text{Hom}_{A\text{-Mod}}(M, M) \\ \text{Aut}_{A\text{-mod}}(M) &= \text{GL}_{A\text{-mod}}(M) = \text{Isom}_{A\text{-mod}}(M, M) \end{aligned}$$

les ensembles de morphismes, morphismes bijectifs, d'endomorphismes et d'automorphismes des A -modules M et N

Proposition 53

Soient $\phi : L \rightarrow M$ et $\psi : M \rightarrow N$ des morphismes de A -modules alors $\psi \circ \phi : L \rightarrow N$ un morphisme.

Preuve

Soit $\phi : L \rightarrow M$, $\psi : M \rightarrow N$ des applications linéaires alors

$$\psi \circ \phi \text{ est linéaire}$$

On sait que $\psi \circ \phi$ est un morphisme de groupes.

Reste à voir que $\forall a \in A, l \in L$

$$\psi \circ \phi(a *_L l) = a *_N \psi \circ \phi(l)$$

$$\psi \circ \phi(a *_L l) = \psi(\phi(a *_L l)) = \psi(a *_M \phi(l)) = a *_N \psi \circ \phi(l) \quad \square$$

Proposition 54

Soient M et N des A -modules alors $\text{Hom}_{A\text{-mod}}(M, N)$ a une structure naturelle de groupe commutatif.

Si de plus A est commutatif alors $\text{Hom}_{A\text{-mod}}(M, N)$ a une structure de A -module

Preuve

Si ϕ et $\psi \in \text{Hom}_{A\text{-mod}}(M, N)$, alors

$$\phi + \psi : m \rightarrow \phi(m) + \psi(m)$$

on sait que $\phi + \psi$ est un morphisme de groupes et on montre que c'est même un morphisme de modules.

$$(\phi + \psi)(a * m) = \phi(a * m) + \psi(a * m) = a * \phi(m) + a * \psi(m) = a * (\phi(m) + \psi(m))$$

Donc $\phi + \psi \in \text{Hom}_{A\text{-mod}}(M, N)$, donc la proposition est prouvée. \square

Théorème 55

Soit M un A -module. L'ensemble $\text{End}_{A\text{-mod}}(M)$ des endomorphismes de M est un sous-anneau de $(\text{End}, +, \circ)$ dont le groupe des unités est

$\text{Aut}_{A\text{-mod}}(M)$;

de plus, si A est commutatif, $\text{End}_{A\text{-mod}}(M)$ possède une structure naturelle de A -module qui en fait une A -algèbre.

$\text{End}_{A\text{-mod}}(M)$ est appelée l'algèbre des endomorphismes du A -module M

Preuve

On utilise le critère du sous-anneau.

On sait que $\phi \circ \psi + \Phi \in \text{End}_{A\text{-mod}}(M)$, et on doit vérifier que c'est compatible avec la loi de multiplication externe $*$

$$\begin{aligned} (\phi \circ \psi + \Phi)(a * m) &= a * (\phi \circ \psi + \Phi)(m) \\ (\phi \circ \psi + \Phi)(a * m) &= \phi \circ \psi(a * m) + \Phi(a * m) \\ &= a * \phi \circ \psi(m) + a * \Phi(m) \\ &= a * (\phi \circ \psi(m) + \Phi(m)) \end{aligned} \quad \square$$

6 Corps

Definition 30 (Corps)

Un corps K est un anneau commutatif possédant au moins deux éléments $0_K \neq 1_K$ et tel que tout élément non-nul est inversible :

$$K^\times = K \setminus \{0_K\}$$

Exemple

- $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ sont des corps.
- \mathbb{Z} n'est pas un corps, car $\mathbb{Z}^\times = \{\pm 1\}$
- $\mathbb{R}(x)$ Le corps des fractions rationnelles à coefficients dans \mathbb{R}

$$= \left\{ f(x) = \frac{P(x)}{Q(x)}, P(x), Q(x) \in \mathbb{R}[x], Q \neq 0 \right\}$$

$$\text{si } f(x) = \frac{P(x)}{Q(x)} \neq 0, f(x)^{-1} = \frac{Q(x)}{P(x)}$$

Proposition 57

Soit K un corps, B un anneau et $\phi \in \text{Hom}_{\text{Ann}}(K, B)$ un morphisme. Alors, si ϕ n'est pas nul ($\phi \neq 0_B$) ϕ est injectif.

$$\phi : K \hookrightarrow B$$

Preuve

Soit $\phi : K \rightarrow B$ un morphisme d'anneaux, supposons $\phi \neq 0_B$.

Il existe $k \in K$ tel que $\phi(k) \neq 0_B$, alors $k \neq 0_K$ (sinon $\phi(k) = 0_B$)

Comme K est un corps, k est inversible et il existe k^{-1} tel que $k.k^{-1} = 1_K$.

Montrons que ϕ est injectif :

c'est à dire que

$$\ker \phi = \{0_K\}.$$

Supposons que non, alors soit $k \in \ker \phi$, tel que

$$\phi(k) = 0_B \text{ et } k \neq 0_K$$

Comme k est inversible

$$\phi(1_K) = \phi(k.k^{-1}) = \phi(k).\phi(k^{-1}) = 0_B$$

Donc si $\ker \phi \neq \{0_K\}$, alors $\phi(1_K) = 0_B$, mais alors $\forall \lambda \in K$

$$\phi(\lambda) = \phi(\lambda.1_K) = \phi(\lambda)\phi(1_K) = 0_B$$

□

Donc $\phi = 0_B$ ce qu'on a exclu. \nmid

6.1 Corps des fractions

Lemme 58

Soit $\{0\} \neq A \subset K$ un sous anneau non-nul commutatif d'un corps K , alors

$$\forall a, b \in A, a.b = 0 \iff a = 0 \text{ ou } b = 0$$

Definition 31

Un anneau commutatif tq si $a.b = 0 \Rightarrow a = 0$ ou $b = 0$ est appelé intègre.

Un corps est toujours intègre.

Preuve

Soit $a, b \in A \subset K$, tel que $a.b = 0_A = 0_K$, supposons que $a \neq 0_K$, alors a admet un inverse dans K , il existe $a^{-1} \in K$ tel que $a^{-1}.a = 1_K$.

$$a.b = 0_K \Rightarrow a^{-1}.a.b = a^{-1}.0_K \Rightarrow b = 0_K \quad \square$$

Lecture 9: Corps

Tue 13 Oct

Proposition 59

Soit A un anneau intègre, alors il existe un corps K et un morphisme d'anneau injectif

$$\iota : A \hookrightarrow K$$

de sorte qu'on peut considérer A comme un sous-anneau de K en identifiant A à $\iota(A) \subset K$ et tel que K a la propriété de minimalité suivante : pour tout corps K' et tout morphisme injectif

$$\iota' : A \hookrightarrow K'$$

de sorte que A peut être identifiée à un sous-corps de K' , il existe un morphisme (nécessairement injectif)

$$\iota' : K \hookrightarrow K'$$

prolongeant le morphisme ι' (ainsi A et K peuvent être vus comme des sous-anneaux de K')

Definition 32

On appelle ce corps K le corps des fractions de A .

Exemple

- $\text{Frac}(\mathbb{Z}) = \mathbb{Q}$
- $\text{Frac}(\mathbb{R}[X]) = \mathbb{R}(X)$ (défini comme avant)

Preuve

Construisons K .

A est intègre.

On considère l'ensemble produit

$$A \times A \setminus \{0\} = \{(a, b) | a, b \in A, b \neq 0_A\}$$

On définit sur cet ensemble une relation.

$(a, b) \sim (a', b')$ si et seulement si $a.b' = a'.b$, la relation \sim est une relation d'équivalence.

- Symétrique : Si $a.b' = a'.b \iff a'.b = a.b' \iff (a', b') \sim (a, b)$
- Reflexive : $(a, b) \sim (a, b) \iff a.b = a.b$
- Transitive : $(a, b) \sim (a', b')$ et $(a', b') \sim (a'', b'') \implies a.b' = a'.b = a''.b' = a'.b' = a''.b'$.

$$\begin{aligned} & \implies ab'b'' = a'b'b'' \\ & \implies a.b''b' = a.b''b' \\ \implies a.b''b' &= a'b''b = a''b'b = a''bb' \\ \implies (ab'' - a''b).b' &= 0_A \end{aligned}$$

Comme A est intègre,

$$ab'' - a''b = 0_A \text{ ou bien } b' = 0_A$$

Donc

$$ab'' - a''b = 0_A$$

Donc $(a, b) \sim (a'', b'')$

Soit $K = A \times A \setminus \{0\} / \sim$ l'ensemble des classes d'équivalences.

On note $\frac{a}{b}$ la classe de l'élément (a, b) .

On va munir K d'une addition et d'une multiplication d'un 0_K , d'une 1_K ainsi que

$$\iota : A \hookrightarrow K$$

Il faut maintenant vérifier toutes les propriétés d'un corps.

$$+ : \frac{a}{b} + \frac{a'}{b'} = \frac{ab' + a'b}{bb'}$$

$b.b' \neq 0_A$ vrai car $b, b' \neq 0$ et A intègre.

On doit vérifier que cette définition ne dépend que des classes d'équivalence $\frac{a}{b}$ et $\frac{a'}{b'}$.

Si $(a'', b'') \sim (a', b')$ on veut voir que $\frac{a}{b} + \frac{a'}{b'} = \frac{a}{b} + \frac{a''}{b''}$. On doit vérifier que

$$\underbrace{(ab' + a'b)}_{abb'b'' + a'b^2b''} . bb'' = \underbrace{(ab'' + a'b)}_{abb'b'' + a''b^2b'}. bb'$$

On sait que $a'b'' = a''b'$.

$$\Rightarrow a'b^2b'' = a''b^2b'$$

On fait pareil pour définir la multiplication \times

$$\frac{a}{b} \times \frac{a'}{b'} = \frac{a.a'}{b.b'}$$

et on doit vérifier que si $\frac{a''}{b''} = \frac{a'}{b'}$ alors $\frac{a}{b} \times \frac{a'}{b'} = \frac{a}{b} \times \frac{a''}{b''}$ sachant que $a'b'' = a''b'$.

On vérifie que $+$, \times sont commutatives, associatives, distributives.

On définit $0_K = \frac{0}{1_A}$ et $1_K = \frac{1_A}{1_A}$

Enfin, dire que $\frac{a}{b} \neq 0_K \iff a \neq 0_A$ et alors si $\frac{a}{b} \neq 0_K$ $\frac{b}{a} \times \frac{a}{b} = \frac{1_A}{1_A} = 1_K$.

On a un morphisme injectif

$$\iota : A \hookrightarrow K$$

donné par

$$\iota(a) = \frac{a}{1_A}$$

On vérifie que c'est un morphisme d'anneau et, si $\iota(a) = 0_K = \frac{0_A}{1_A} \iff \frac{a}{1_A} = \frac{0_A}{1_A} \iff a = 0_A$, donc

$$\ker \iota = \{0_A\}$$

donc ι est injectif. □

6.2 Caractéristique des Corps

K un corps,

$$Can_K : \mathbb{Z} \rightarrow A$$

$$n \rightarrow n.1_K = n_K$$

$$\ker(Can_K) = p\mathbb{Z}, p \geq 0$$

Definition 33 (Caractéristique)

L'entier p s'appelle la caractéristique du corps K et se note

$$car(K)$$

Si $p = 0$: $\ker Can_K = \{0_{\mathbb{Z}}\}$, donc Can_K est injectif et donc \mathbb{Z} peut être vu comme sous-anneau de K .

$$n \in \mathbb{Z} \rightarrow n_K \in K$$

Si $n \neq 0, n_K \neq 0$ et $\frac{1}{n_K}$ existe et pour tout $a, b \in \mathbb{Z}, b \neq 0$, on définit

$$\left(\frac{a}{b}\right)_K = a_K/b_K \in K$$

On dispose d'un morphisme injectif

$$Can_K : \mathbb{Q} \hookrightarrow K$$

$$\frac{a}{b} \rightarrow \frac{a_K}{b_K}$$

Si $Car(K) = 0$, le corps \mathbb{Q} est un sous-corps de K .

Lemme 61

Si $\text{car}(K) > 0$, alors $\text{car}(K) = p$ est un nombre premier.

Preuve

Si $p = 1$, $\ker \text{Can}_K = \mathbb{Z}$

$$\Rightarrow \text{Can}_K(1) = 1_K = 0_K \not\equiv$$

Donc $p \geq 2$.

Soit une factorisation

$$p = q_1 \cdot q_2$$

non-triviale ($q_1, q_2 \geq 2$)

$$0_K = \text{Can}_K(p) = \text{Can}_K(q_1 \cdot q_2) = \text{Can}_K(q_1) \cdot \text{Can}_K(q_2)$$

Comme K est intègre, $\text{Can}_K(q_1) = 0_K$

$$q_1 \in \ker \text{Can}_K = p\mathbb{Z}$$

$$q_1 = pk, k \in \mathbb{Z} \setminus \{0\}$$

Donc $q_1 \geq p$ mais comme $q_2 \geq 2$

$$q_2 \leq \frac{p}{2} < p$$

Donc p est premier. □

Definition 34

$$\mathbb{F}_p = \text{Can}_K(\mathbb{Z}) = \mathbb{Z}.1_K$$

Lemme 62

L'anneau \mathbb{F}_p est un corps fini de cardinal p .

Preuve

Si $n \in \mathbb{Z}$ et $k \in \mathbb{Z}$

$$(n + pk)_K = n_K + p_K.k_K = n_K$$

Donc, si $r \in \{0, \dots, p\}$ le reste de la division euclidienne de n par p

$$\mathbb{Z}.1_K = \{0_K, 1_K, \dots, (p-1)_K\}$$

\mathcal{F}_p est de cardinal p .

Il faut montrer que si $0 < i \neq j \leq p-1$

$$i_K \neq j_K$$

mais

$$i_K - j_K = (i - j)_K$$

et comme $0 \leq i, j \leq p-1$, $0 \neq |i-j| < p$ Donc $i-j$ ne peut pas être un multiple de p , donc $i-j \notin \ker \text{Can}_K$ Donc

$$(i-j)_K = i_K - j_K \neq 0_K \quad \square$$

Lemme 63

Un anneau commutatif intègre et fini est un corps

Preuve

exercice \square

\mathbb{F} est intègre car c'est un sous-anneau du corps K et il est fini de cardinal p .

Definition 35

Le corps $\mathbb{Q} \subset K$ si $\text{car}(K) = 0$ ou bien $\mathbb{F}_p \subset K$ (si $\text{car}(K) = p > 0$) s'appelle le sous-corps premier de K .

Remarque

Le corps

$$\mathbb{F}_p \simeq (\mathbb{Z}/p\mathbb{Z}, +, \times)$$

l'anneau des classes de congruences module p

6.3 Arithmétique des corps de caractéristique $p > 0$

Proposition 65

Soit K un corps de caractéristique $p > 0$, alors l'application

$$\begin{aligned} \bullet^p : K &\rightarrow K \\ x &\rightarrow x^p \end{aligned}$$

est un morphisme d'anneaux non-nul (donc nécessairement injectif).

Definition 36

Soit K un corps de caractéristique p , le morphisme d'anneau précédent s'appelle le morphisme de Frobenius (ou simplement le Frobenius) de K se note

$$\text{frob}_p : x \rightarrow x^p$$

Preuve

$\forall x, y \in K$

$$\begin{aligned} (x.y)^p &= x.y.x.y.x.y.x.y \dots \\ &= x^p y^p \end{aligned}$$

$\forall x, y \in K$

$$(x + y)^p = x^p + y^p$$

Comme K est commutatif, on a la formule du binôme de Newton

$$\begin{aligned}(x + y)^p &= \sum_{k=0}^p \binom{p}{k} x^k y^{p-k} \\ &= x^p + y^p + \sum_{k=1}^{p-1} \binom{p}{k} x^k y^{p-k}\end{aligned}$$

Lemme 66

Si $1 \leq k \leq p-1$, alors

$$p \mid \binom{p}{k}$$

Or

$$\binom{p}{k} x^k y^{p-k} = \binom{p}{k} x^k y^{p-k} = 0_K \cdot x^k y^{p-k}$$

□