

Algebre Lineaire I

David Wiedemann

Table des matières

1	Le language des Ensembles	4
1.1	Notations	4
1.2	Ensembles	5
1.2.1	Exemples	5
1.3	Sous-Ensembles	5
1.4	$\mathcal{P}(E)$ l'ensemble des sous-ensembles	5
1.4.1	Exercice	6
1.5	Operations sur les ensembles	6
1.6	\times : Produit cartésien	6
1.7	Applications entre ensembles	6
1.7.1	Graphe	7
1.8	Composition/Associativite	7
1.8.1	Associativite	8
1.9	Image,Preimage	8
1.10	Relation de composition par les applications reciproques	11
2	Groupes	13
2.1	Le groupe Symmetrique	13
3	Sous-Groupe	17
3.1	Groupe engendre par un ensemble	18
3.2	Morphismes de Groupes	20

List of Theorems

1	Theorème (Composition de fonctions)	8
	Preuve	8
1	Definition (Injectivite)	9
2	Definition (Surjectivite)	9
3	Definition (Bijectivite)	10
2	Proposition (Injectivite et cardinalite)	10

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

24	Theorème	24
	Preuve	24

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 :

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

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 dû au paradoxe de Russell (Logicien anglais) Si c'était le cas, on considérerait

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

Cet ensemble $Ncont$ 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)

$$f : X \rightarrow Y$$

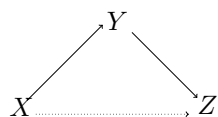


FIGURE 1 – Schema de la composition de 2 applications

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 Associativité

$$f : X \longrightarrow Y$$

$$g : Y \longrightarrow Z$$

$$h : Z \longrightarrow W$$

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 associées 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 : $Preim(f)$:

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

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

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

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

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

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 Symmetrique

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 $e e_G : \forall g \in G, g \star e_G = e_G \star g = g$.
- 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)

- Involutive 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 :

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

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)

$$\exp_g : \begin{array}{l} \mathbb{Z} \rightarrow G \\ n \rightarrow g^n \end{array}$$

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 12

$(G, \cdot) g \in G$ 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 13

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})

Reciproqueme 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 generalement 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 deuxieme version du critere 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 engendre par A , note $\langle A \rangle \subset G$ est par definition 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-vidécar il contient G .

Par la proposition precedente, on considere

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

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

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

Exemple 16

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 19

—

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

— 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 20

$Ad_h : G \rightarrow G$ 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 23

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

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