Algebre Lineaire I

David Wiedemann

Table des matières

List of Theorems

Lecture 1: Le language des Ensembles

Mon 14 Sep

1 Le language des Ensembles

Le terme "Algebre" est derive du mot arabe al-jabr tire du tire 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.

$$\begin{aligned} 2x &= 4 && \quad \mid +4 \\ x &= \frac{4}{2} = 2 && \quad \mid : 2 \end{aligned}$$

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 $\mid$

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'elements "appartenant" a E

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

1.2.1 Exemples

- $\emptyset$ ne contient aucun element

- $\mathbb{N} = \{0, 1, 2\}$

- $\mathbb{Z} = \{-2, -1, 0, 1, 2\}$

- $\mathbb{Q} = \{\frac{p}{q} | p, q \in \mathbb{Z}, q \neq 0\}$
- $\mathbb{R}$, nombres réels, nombres complexes.

1.3 Sous-Ensembles

Un sous-ensemble A d'un ensemble E est un ensemble t.q. tout element de A appartient a 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 egaux si ils ont les mêmes élements, 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'etait le cas, on considererait

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

Cet ensemble Ncont est-il contenu dans lui meme ou pas ?

1.4.1 Exercice

Ncont est il contenu dans lui meme ou pas ? $\lightning$

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.

— $A \cap B = \{e \in E | e \in Ae \in B\}$
Difference : $A - B$ ou $A \setminus B$

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

Difference symmetrique :

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

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

On peut noter une grande reunion ainsi :

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

1.6 $\times$: Produit cartesien

Si A et B sont des ensembles

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

On peut bien sur iterer

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

1.7 Applications entre ensembles

Soient X et Y deux ensembles.

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

$$f : X \to Y$$

$$\begin{tikzcd} & Y \arrow[dr] & \\ X \arrow[ur] \arrow[rr, dotted] & & Z \end{tikzcd}$$

FIGURE 1 – Schema de la composition de 2 applications

1.7.1 Graphe

Se donner une application

$$f : X \to Y$$

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

$$f : X \to Y$$

$$g : Y \to Z$$

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

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

$$(g \circ f) : X \longrightarrow Z \circ h : Z \longrightarrow W$$
$$\Rightarrow h \circ (g \circ f)$$

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

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 $\mathcal{P}(X), \mathcal{P}(Y)$.

— $Im(f) : \mathcal{P}(X) \longrightarrow \mathcal{P}(Y)$
  $A \subset X \longrightarrow Im(f)(A) = f(A)$
  C'est ce qu'on appelle l'image de A par f

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

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

— Preimage de f : $Preim(f)$:

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

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

<u>Exemples</u>

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

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

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

$$\text{“}f'' : X \mapsto Y$$
$$x \mapsto f(x)$$

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
$C : \mathbb{N} \times \mathbb{N} \mapsto \mathbb{N}$
$(m, n) \simeq \frac{1}{2}((m+n)^2 + m + 3n)$
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 $f :\twoheadrightarrow Y$ 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*

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

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. $\square$

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

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

$\Rightarrow x$ 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 note

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

Definition 5 (Notations Surjection)
L'ensemble des applications surjectives sera note

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

Definition 6 (Notations Bijection)
L'ensemble des applications bijectives sera note

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

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 :

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

$\circ$ 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 (appellee loi de composition interne) $\star$ tq*

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

- *d'un element $e_G \in G$ (element neutre)*

- *de l'application d'inversion $\cdot^{-1}$*

$$\cdot^{-1} : \begin{array}{c} G \mapsto G \\ g \mapsto g^{-1} \end{array}$$

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* $\star$ *possede la propriete supplementaire de commutativite :*

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

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

Lecture 3: Groupes, Anneaux, Corps

Tue 22 Sep

$\exists \sigma, \tau \in Bij(x)$ 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 notee* $+$.
- *L'element neutre sera note* 0_G.
- *L'inversion sera appele oppose et notee* $-g g + (-g) = 0_G$.

Proposition 9 (Lois de Groupe)

- *Involutivite de l'inversion :* $\forall g, (g^{-1})^{-1} = g, g^{-1} \star g = e_G$.
- *L'element neutre est unique, si* $\exists e'_G$ *tq* $g \in G$ *verifiant* $g \star e'_G = g$, *alors* e'_G *est l'element neutre.*
- *Unicite de l'inverse : si* $g' \in G$ *verifie* $g \star g' = e_G$, *alors* $g' = g^{-1}$.
- *On a* $(g \star g')^{-1} = g'^{-1} \star g^{-1}$

Preuve
La preuve de toutes les proprietes est donnee dans le support de cours.
On montre l'unicite de l'element neutre.
Si e'_G *est telle que pour un certain* $g \in G$, *tq*

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

Alors on $\star$ *a 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* $(g \star g')^{-1}$. □

Definition 10 (Notation exponentielle)
$(G, \cdot)$ *un groupe et* $g \in G$. *On peut :*

$$g \to g^{-1} \;\; g \cdot g, g \cdot g \cdot g, g \cdot g \cdot g \cdot g \ldots$$

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

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

si $n < 0$ *:*

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

et $g^0 := e_G$

Exercice 10
Verifier que : $g^{m+n} = g^m \cdot g^n$

Definition 11 (exponentielle)

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

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*

$$n \geq 1 \, \underbrace{g + \ldots + g}_{n \; fois} = n \cdot g$$

Si $n < 0$

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

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 suffite 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*

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

□

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* $h^{-1} \in g^{\mathbb{Z}}$ □

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* $q \cdot k' \in q\mathbb{Z} \Rightarrow qk + qk' = q(k + k') \in q \cdot \mathbb{Z}$

- $qk \in q\mathbb{Z}$ $\square$

> **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 $r \in \{0, \ldots, q - 1\}$ tq

$$h = qk + r$$
$$r = h - qk \in H$$

$\square$

Donc $0 \geq r < q \Rightarrow r = 0$ 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 $< A >\subset G$ 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-videcar 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
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

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

l'image de A par l'inversion alors

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

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 commme 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 $g_1, \ldots, g_n \in A \cup A^{-1}$ Le produit $g_1 \star g_2 \star \ldots \star g_n \in H$

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

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

Critere de ss-groupe :

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

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

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

Alors

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

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

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

$\{\ldots\}$ 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 $\phi : G \to H$ est une application telle que

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

Theorème 18

Soit $\phi : G \to H$ 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

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

□

Definition 16 (Notations)

- $Hom_{Gr}(G, H)$ *l'ensemble des morphismes de groupe entre* G *et* H.
- $End_{Gr}(G) = Hom_{Gr}(G, G)$ *les endomorphismes du groupe* G.
- $Isom_{Gr}(G, H)$ *l'ensemble des morphismes bijectifs*
- $Aut_{Gr}(G) = Isom_{Gr}(G, G)$ *l'ensembles des automorphismes du groupe* G.

Exemple

- $$e_H : \begin{cases} G \to H \\ g \to e_h \end{cases}$$
- *Soit* $g \in G$
$$\exp_G : \begin{cases} \mathbb{Z} \to G \\ n \to g^n \end{cases}$$

Si G *est commutatif note additivement*

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

Conjugaison dans un groupe : $(G, .)$

$$h \in G$$

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

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

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

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

Terminologie :

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

□

Le conjugue de g par g.

Remarque
$Ad_h : G \to G$ *est bijectif.* Ad_h *admet une application reciproque 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.

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

$$= g = Id_G(g)$$

car $(h^{-1})^{-1} = h$ □

$\forall h \in G,$

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

Proposition 21
Soient $(G, \star), (H, *), (K, \bullet))$ *des groupes et* $\phi : G \to H$ *et* $\psi : H \to K$ *des morphismes de groupes alors la composee* $\psi \circ \phi : G \to K$ *est un morphisme de groupes*

Preuve
On veut montrer que

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

on a :

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

> **Proposition 22**
> *Soit $\phi : G \to H$ un morphisme de groupe bijectif alors l'application reciproque ϕ^{-1} est un morphisme bijectif.*

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

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

On calcule

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

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 $Isom_{Gr}(H, G) \neq 0, H \simeq_{Gr} G$

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 $\big(Bij(G), \circ, Id_G, \bullet^{-1}\big)$

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

$$Isom_{Gr}(G, G) = Aut_{Gr}(G)$$

□

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'imaged 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 $\phi(k) = h, \phi(k') = h'$

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

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

car K sous-groupe.

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

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 $\phi(g) = h \in L, \phi(g') = h' \in L$

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

on a

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

Definition 18

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

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

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

Theorème 26 (Critere d'injectivite)

Soit $\phi \in Hom_{Gr}(G, H)$ un morphisme de groupes alors les proprietes suivantes sont equivalentes

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

Preuve

$1 \to 2$

si ϕ est injectif, l'image reciproque de $\{e_H\}$ possede au plus un seul element. Mais comme ϕ est un morphisme $\phi(E_G) = e_H \Rightarrow \phi^{-1}(\{e_H\}) = \{e_G\}$

$2 \to 1$

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

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 definition, $\phi(g) = \phi(g') = h$

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

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

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

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

Exemple
Ordre d'un element
Soit $g \in G$ *groupe*

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

est un morphisme de groupes.

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

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

$$\Rightarrow \mathbb{Z} \to G$$
$$n \to g^n \text{ est injective}$$

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

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

donc g *est d'ordre infini.*
Si $q > 0$*, alors*

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

est un sous-groupe de cardinal q *(a demontrer en exercice) et donc* G *contient un sous-groupe d'ordre* q

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

q *est le plus petit entier* > 0 *tel que*

$$g^q = e_G$$

Exemple (Conjugaison)
$G \ni h$

$$Ad_h : g \to h.g.h^{-1}$$

On a montrer que $Ad_h \in Aut_{Gr}(G)$

On considere l'application

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

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 $g \in G$

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

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

On dit que h commute avec g.

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

Z_G est un groupe commutatif de G

Exemple (Translation)
Soit $h \in G$ la translation a gauche par h

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

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 $t_{h^{-1}}$

$t_\bullet : h \in G \to t_h \in Bij(G)$ *est un morphisme de groupe injectif, l'image s'appelle le groupe des translations (a gauche) de G.*
Donc $G \simeq t_G \subset Bij(G)$
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 $(A, +, ., 1_A)$ *est la donee, d'un groupe commutatif* $(A, +)$ *(note additivement)d'element neutre note* 0_A*, d'une loi de composition interne (dite de multiplication)*

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

et d'un element unite $1_A \in A$ *ayant les proprietes suivantes*

1. *Associativite de la mutliplication*

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

2. *Distributivite*

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

3. *Neutralite de l'unite*

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

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'element neutre de l'addition 0_A *est absorbant. Pour l'oppose, on a*

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

Preuve
$\forall a \in A$

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

□

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* $\mathbb{R}$.

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

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

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

$(\mathcal{F}(X, A), +, \bullet)$ *est un anneau (commutatif si* A *commutatif) generalisation du cas des fonctions reelles*
— $\mathbb{R}[x] = \left\{P(x) = a_0 + a_1 x + \ldots + a_d x^d, a_0, a_1, \ldots, a_d \in \mathbb{R}, d \geq 0\right\}$
— $A[x] = \left\{P(x) = a_0 + a_1 x + \ldots + a_d x^d, a_0, \ldots a_d \in Ad \geq 0\right\}$
Anneau des polynomes a coefficients dans A.
— $(M, +)$ *un groupe commutatif*

$$End(M) = End_G r(M) = Hom_{Gr}(M, M)$$

$$+ : \psi, \phi \in End(M)$$
$$\phi + \psi : m \to \phi(m) + \psi(m)$$

Soient $\phi, \psi \in End(M)$

$$\phi \circ \psi \in End(M)$$
$$0_{End(M)} : m \in M \to 0_M \in M$$
$$1_{End(M)} : Id_M : m \in M \to m \in M$$

$(End(M), +, \circ, 0_M, Id_M)$ *est un anneau*

Lecture 6: Anneaux 2

Mon 05 Oct

Preuve

Soit $\phi, \psi \in End_{Gr}(M)$, *on veut montrer que*

$$\phi + \psi \in End_{Gr}(M)$$

Pour vérifier celà, 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 $\phi, \psi, \psi' \in End_{Gr}(M)$ 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 $\circ$ $\square$

5.1 Elément 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

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

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

Exemple
- $\mathbb{Z}^\times = \{\pm 1\}, \mathbb{Q}^\times = \mathbb{Q} \setminus \{0\}$
- $\mathbb{R}^\times = \mathbb{R} \setminus \{0\}$
- $\mathcal{F}(X, \mathbb{R})^X = \{f : X \to \mathbb{R}^\times \subset \mathbb{R} | f(x) \neq 0_\mathbb{R}$ *pour tout* $x \in X\}$
- $\mathbb{R}[x]^\times = \{a_0 | a_0 \in \mathbb{R}^\times\}$
- $End_{Gr}(M)^\times = Aut_{Gr}(M) = Isom_{Gr}(M, M)$

5.2 Sous-Anneau

Definition 21 (Sous-Anneau)
Soit $(A, +, .)$ *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 . :*

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

Ains $(B, +, .)$ *est un anneau.*

Lemme 35 (Critère de sous-anneau)
Soit $(A, +, .)$ *un anneau et* $B \subset A$ *un sous-ensemble non-vide alors* B *est un sous-anneau ssi* $B = \{0_B\}$ *ou bien* $1_A \in B$ *et*

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

Preuve
Si $B = \{0_A\}$ *c'est un sous-anneau.*
Sinon $1_A \in B$ *si on prend* $b \in B$ *alors*

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

Alors

$$\forall b, b' \in B$$
$$b - b' = 1_A.b - b' \in B$$

Donc $(B, +)$ *est un sous-groupe.*
Soient $b, b' \in B$ *alors*

$$b.b' - 0_A \in B \qquad \square$$

$= b.b'$.

Exemple

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

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

est un sous-anneau

5.3 Morphismes d'anneaux

Definition 22 (Morphisme d'anneaux)
Soient $(A, +, .)$*, et* $(B, +, .)$ *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

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

Exemple (Le morphisme canonique)
Le morphisme cannonique :

$$\begin{aligned} Can_A : (\mathbb{Z}, +, .) &\to (A, +, .) \\ n &\to n.1_A = 1_A + 1_A + \ldots + 1_A \ n \text{ fois si } n \geq 0 \text{ et } -n \text{ fois si } n < 0 \end{aligned}$$

est un morphisme d'anneaux.
On doit vérifier que Can_A *est un morphisme entre les groups additifs.*
On doit montrer que $\forall m, n \in \mathbb{Z}$

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

si m *et* $n \geq 0$

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

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

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

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

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

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

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 lles 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*

$$\mathbb{Z} \times M \to M$$
$$(n, \overrightarrow{m}) \to n * \overrightarrow{m} = \underbrace{\overrightarrow{m} + \overrightarrow{m} + \dots}_{n \text{ fois}}$$