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.

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

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 : $Preim(f)$:

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

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

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

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

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.* □

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

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

$\Rightarrow$ 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 :

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

$\circ$ 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 <u>groupe</u>

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*

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

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

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

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

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* $(g \star g')^{-1}$. $\square$

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

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

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

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

si $n < 0$ *:*

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

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*

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

Si $n < 0$

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

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 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 $h \in g^{\mathbb{Z}} h = g^m$ *a finir* □

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

$$h = qk + r$$
$$r = h - qk \in H$$ □

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* $\square$

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

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

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 16
Si $g \in G \, \langle \{g\} \rangle = g^{\mathbb{Z}} = \{g^n, n \in \mathbb{Z}\}$