

Math 110 : Algebre Lineaire Avancee

Injectivité / Surjectivité / Bijectivité

X, Y des ens et une app. $f: X \rightarrow Y$.

Def: f est injective ssi $\forall y \in Y$

$f^{(-1)}(\{y\}) = \{x \in X \mid f(x) = y\}$ possède au plus
1 elt.

Def. f est surjective ssi

$$\forall y \in Y \quad f^{(-1)}(\{y\}) = \{x \in X \mid f(x) = y\}$$

possède au moins un elt
(ie. est $\neq \emptyset$)

Df: f est bijective ssi f est injective
et surjective.

$\forall y \in Y \quad f^{(-1)}(\{y\})$ est un singleton
(a exactement un elt)

Notations: $f: X \rightarrow Y$

Si f est injective $f: X \hookrightarrow Y$
 $\backslash \text{hookrightarrow}$

Si f est surjective $f: X \twoheadrightarrow Y$
 $\backslash \text{surj}$
 $: X \mapsto Y \rightarrow \backslash \text{mapsto}$

Si f est bijective $f: X \xrightarrow{\sim} Y$
 $X \simeq Y \quad \backslash \text{simeq}$

Def: on définit l'application réciproque

$f^{-1} : Y \rightarrow X$ qui à tout

$y \in Y$ associe l'unique élément de

$$f^{(-1)}(\{y\}) =: \{f^{-1}(y)\}$$

Si f est bijective

$$\forall y \in Y \quad f^{(-1)}(\{y\}) = \{f^{-1}(y)\}.$$

Involutivité de la Reciproque :

Soit $f: X \hookrightarrow Y$ et $f^{-1}: Y \rightarrow X$

sa reciproque

alors f^{-1} est bijective $f^{-1}: Y \hookrightarrow X$

$$\text{et } (f^{-1})^{-1} = f.$$

Composition d'applications: 3 ens X, Y, Z

$$f: X \rightarrow Y \quad g: Y \rightarrow Z$$

$$x \in X \xrightarrow{f} f(x) \in Y \xrightarrow{g} g(f(x)) \in Z$$

on a ainsi défini une application entre
 X et Z notée

$$g \circ f: X \rightarrow Z$$

definie pour $x \in X$ par

$$g \circ f(x) = g(f(x)) \in Z$$

On l'appelle la composée de f et g .

la composition des application defini
une application

$$\begin{aligned} \circ: \text{Hom}_{\text{ENS}}(Y, Z) \times \text{Hom}_{\text{ENS}}(X, Y) &\longrightarrow \text{Hom}_{\text{ENS}}(X, Z) \\ (g, f) &\longrightarrow g \circ f \end{aligned}$$

Propriétés de la Composition

Associativité: $f: X \rightarrow Y, g: Y \rightarrow Z, h: Z \rightarrow T$

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

Utilisation: $f: X \rightarrow X \quad f \circ f: X \xrightarrow{f} X \xrightarrow{f} X$

$$f \circ f \circ f: X \xrightarrow{f} X \xrightarrow{f} X \xrightarrow{f} X$$

$$f \circ f = f^2 \quad f \circ f \circ f = f^3$$

$$\underbrace{f \circ f \circ \dots \circ f}_{k \text{ fois}} = f^k$$

$(f^k)_{k \geq 1}$ collection
d'applications
de X vers X

$$f^k \circ f^l = f^{k+l}$$

$$f^0 := \text{Id}_X$$

$$\text{Id}_X: x \in X \rightarrow x \in X$$

Element Neutre:

$$f: X \rightarrow Y$$

$$I_{d_X}: x \in X \rightarrow x \in X$$

$$I_{d_Y}: y \in Y \rightarrow y \in Y$$

$$f \circ I_{d_X} = f, \quad I_{d_Y} \circ f = f$$

Simplification: $f: X \xrightarrow{\sim} Y$ (bije)

$f^{-1}: Y \rightarrow X$ la réciproque.

- $f^{-1} \circ f: X \xrightarrow{f} Y \xrightarrow{f^{-1}} X$. $f^{-1} \circ f = \text{Id}_X$

- $f \circ f^{-1}: Y \xrightarrow{f^{-1}} X \xrightarrow{f} Y$ $f \circ f^{-1} = \text{Id}_Y$

Involutivité de la réciproque (bis)

$$\begin{array}{ccc} \bullet^{-1} : \text{Bij}(X, Y) & \longrightarrow & \text{Bij}(Y, X) \\ & \searrow & \uparrow \\ & & f^{-1} \end{array}$$

• $^{-1}$ est bijective et sa réciproque

$$(\bullet^{-1})^{-1} : \text{Bij}(Y, X) \longrightarrow \text{Bij}(X, Y)$$

• $^{-1}$ est bijective et sa réciproque

$$(\cdot^{-1})^{-1} : \text{Bij}(Y, X) \longrightarrow \text{Bij}(X, Y)$$

C'est l'application réciproque

$$g \in \text{Bij}(Y, X) \longrightarrow g^{-1} \in \text{Bij}(X, Y)$$

l'involutive de la réciproque : $(f^{-1})^{-1} = f \iff$ de $\cdot^{-1}$ simplifie

LEMME 1.1. Soient des applications $f : X \mapsto Y$ et $g : Y \mapsto Z$. Si

(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: on veut mq $(g \circ f)^{-1} = f^{-1} \circ g^{-1}$

cad on veut mq $\forall z \in Z$

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

$x \in X$ $x' \in X$?
on veut mq $x = x'$?

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

on calcule

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

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

$$= g(g^{-1}(z))$$

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

$$x = x'.$$



- x' est envoye sur z par la bij $g \circ f$
- x est envoy sur z par la bij $g \circ f$

Cardinal d'un ensemble

Def: Soient X et Y des ensembles
On dit que X et Y ont $\hat{m}$ cardinal
et on le note $|X| = |Y|$
si il existe une bijection $f: X \cong Y$.

PROPOSITION 1.2. La relation "avoir le meme cardinal" a la proprietes suivantes

(1) Reflexivite: $|X| = |X|$

(2) Symetrie: $|X| = |Y| \implies |Y| = |X|$,

(3) Transitivite: $|X| = |Y|$ et $|Y| = |Z| \implies |X| = |Z|$.

Preuve: $\text{Id}_X: X \xrightarrow{\sim} X$ est une bijection.

Symetrie: $|X| = |Y| \quad \exists f: X \xrightarrow{\sim} Y$

alors la reciproque existe $f^{-1}: Y \xrightarrow{\sim} X$ et c'est
une bijection de Y vers $X \implies |Y| = |X|$

transitive: $|X| = |Y| \quad \exists f: X \xrightarrow{\sim} Y$

$|Y| = |Z| \quad \exists g: Y \xrightarrow{\sim} Z$

$g \circ f: X \xrightarrow{\sim} Z$ et donc $|X| = |Z|$.



Ensembles finis, infinis, dénombrables

Def: un ensemble X est fini si il est soit $\emptyset$ ou si il est en bijection avec un ensemble de la forme $\{1, 2, \dots, n\} \in \mathbb{N}$ pour $n \geq 1$.

On écrit alors $|X| = |\{1, \dots, n\}| = n$
et si $X = \emptyset$ $|X| = 0$

$$f: X \simeq \{1, 2, \dots, n\}$$

la réciproque $f^{-1}: \{1, \dots, n\} \rightarrow X$

réalise une énumération des elts de X

: on pose $x_1 = f^{-1}(1), x_2 = f^{-1}(2), \dots, x_n = f^{-1}(n)$

et on a $X = \{x_1, \dots, x_n\}$.

Si X n'est pas fini on dit X est infini.

et on note $|X| = \infty$.

Ex: $\mathbb{N}$ est infini.

Def: on dit qu'un ensemble X est dénombrable
si X est soit fini soit $|X| = |\mathbb{N}|$.

Si non X est non dénombrable ou indénombrable.

la notion de dénombrabilité est importante
car il existe des ensembles non dénombrables.

Exemples:

Soit X ens alors $|\mathcal{P}(X)| = |\{0,1\}^X|$

(en particulier si X est fini et $|X| = n$)
alors $|\mathcal{P}(X)| = 2^n$

$$\{0,1\}^X = \mathcal{F}(X, \{0,1\})$$

La bijection est donnée par l'application
fonction caractéristique

$$A \subset X \mapsto 1_A : x \in X \mapsto 1_A(x) = \begin{cases} 1 & \text{si } x \in A \\ 0 & \text{sinon} \end{cases}$$

$1_\bullet : A \mapsto 1_A$ est une bijection
entre $\mathcal{P}(X)$ et $\{0, 1\}^X$

- $\mathbb{Z}$ est dénombrable.
- $\mathbb{N} \times \mathbb{N}$ est dénombrable
- $\forall k \geq 1 \quad \mathbb{N}^k$ est dénombrable.
- $\mathbb{Q}$ est dénombrable
$$\mathbb{Q} = \left\{ \frac{a}{b} \mid a \in \mathbb{Z} \quad b \in \mathbb{N} - \{0\} \right\}$$
- $|X| = |Y| = |\mathbb{N}| \Rightarrow |X \times Y| = \mathbb{N}$

Thm (Cantor) Si X est dénombrable infini
alors $\mathcal{P}(X)$ n'est pas dénombrable

Preuve: Ops $X = \mathbb{N}$ pour montrer que

$\mathcal{P}(X)$ n'est pas dénombrable il suffit
de mg $\{0, 1\}^{\mathbb{N}}$ n'est pas dénombrable

$$|\mathcal{P}(\mathbb{N})| = |\{0, 1\}^{\mathbb{N}}|$$

Supposons qu'il existe

$f: \mathbb{N} \xrightarrow{\sim} \{0,1\}^{\mathbb{N}}$ une bijection.

pour tout $n \in \mathbb{N}$ il existe $f_n: \mathbb{N} \rightarrow \{0,1\}$
 $m \mapsto f_n(m) \in \{0,1\}$

$f_n(\cdot) = (f_n(m))_{m \geq 0}$ est une suite
de 0 et de 1.

Comme $f_\bullet$ est une bijection pour toute
suit $(a_m)_{m \geq 0}$ a valeurs de $\{0, 1\}$, il

existe un certain n (unique)
dependant de $(a_\bullet)$

tg

$$\forall m \geq 0 \quad f_n(m) = a_m.$$

Considérons la suite $(C_m)_{m \geq 0}$
définie comme suit

$$C_m = \begin{cases} 0 & \text{si } f_m(m) = 1 \\ 1 & \text{si } f_m(m) = 0 \end{cases}$$

$(C_m)_{m \geq 0}$ est une suite à valeurs dans $\{0, 1\}$

$$(C_m)_{m \geq 0} = (f_{n_0}(m))_{m \geq 0}$$

pour un certain $n_0 \geq 0$

Quelle est la valeur de $f_{n_0}(n_0) \in \{0, 1\}$

si $f_{n_0}(n_0) = 0 = C_{n_0} = 1$ Contradiction

si $f_{n_0}(n_0) = 1 = C_{n_0} = 0$ Contradiction

il n'existe pas de bijection f . $\square$

Conséquence du Thm de Cantor

Thm : $\mathbb{R}$ n'est pas dénombrable

- $[0,1[$ n'est pas dénombrable

a un nb réel $x \in [0,1[$ on associe son développement en base 2

$$x = \underline{0},010100010.$$

ou le développement ne se termine pas
c'est-à-dire qu'il y a une suite infinie de 1

Le Thm de Cantor-Bernstein - Schroeder

PROPOSITION 1.1. Soient X et Y des ensembles finis possédant respectivement $|X|$ et $|Y|$ éléments et $f : X \mapsto Y$ une application entre ces ensembles. On a les propriétés suivantes

- Si $f : X \hookrightarrow Y$ est injective alors $|X| \leq |Y|$.
- Si $f : X \twoheadrightarrow Y$ est surjective alors $|X| \geq |Y|$.
- Si $f : X \hookrightarrow Y$ est injective et $|X| \geq |Y|$ alors $|X| = |Y|$ et f est bijective.
-
- Si $f : X \twoheadrightarrow Y$ est surjective et $|X| \leq |Y|$ alors $|X| = |Y|$ et f est bijective.

DÉFINITION 1.12. Soient X et Y deux ensembles. Si il existe une application injective entre X et Y , $\phi : X \hookrightarrow Y$, on dit que le cardinal de X est plus petit que celui de Y et on note cette relation $|X| \leq |Y|$. Si de plus $|X| \neq |Y|$, on le note $|X| < |Y|$.

La relation $|X| \leq |Y|$ est réflexive

$|X| \leq |X|$: l'identité Id_X est injective.

et transitive : $|X| \leq |Y|$ et $|Y| \leq |Z|$ alors

$|X| \leq |Z|$.

si $|X| \leq |Y|$: $\exists f : X \hookrightarrow Y$ et $|Y| \leq |Z| \exists g : Y \hookrightarrow Z$
 $g \circ f : X \hookrightarrow Z$ $g \circ f$ est injective. $|X| \leq |Z|$

et ce que $\leq$ est antisymétrique

si $|X| \leq |Y|$ et $|Y| \leq |X|$

$$\Rightarrow |X| = |Y|$$

si il existe $f: X \hookrightarrow Y$ et $g: Y \hookrightarrow X$

alors il exist $h: X \xrightarrow{\sim} Y$

OK si X et Y sont finis.



THE
WARNING



C'est un Theoreme pas evident!

THÉORÈME (Cantor-Bernstein-Schroeder). *Soit X et Y deux ensembles (pas nécessairement finis). Si il existe une injection $\phi : X \hookrightarrow Y$ et une injection $\psi : Y \hookrightarrow X$ alors il existe une bijection $\varphi : X \simeq Y$. En d'autres termes*

$$|X| \leq |Y| \text{ et } |Y| \leq |X| \iff |X| = |Y|.$$

Hypothèse du continu

Q (Cantor) On sait que $|\mathbb{N}| < |\mathbb{R}| = |\mathcal{P}(\mathbb{N})|$

Est ce que $\mathbb{R}$ est le plus petit ensemble
de cardinal strictement plus grand que $|\mathbb{N}|$?

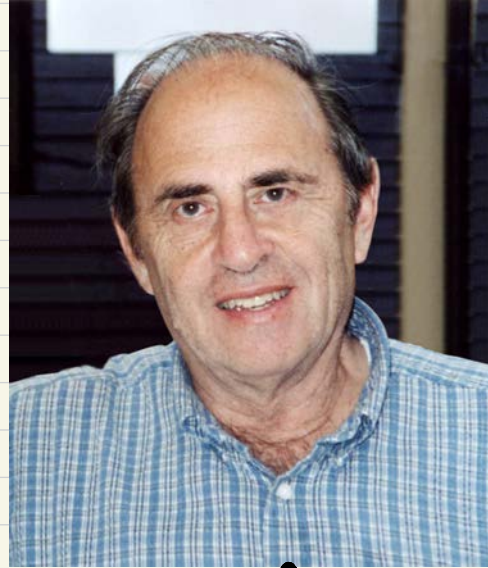
$\exists \kappa_1$ tq $|\mathbb{N}| < |\kappa_1| < |\mathbb{R}|$?

Hypothèse du Continu: $\aleph_1$ est bien le + petit.
dans la Théorie ZFC.

Kurt Gödel



Paul Cohen



En 1938 il montre que
l'hypothèse du continu ne peut être réfutée dans ZFC

En 1963, il démontre que
l'Hypothèse du Continu ne peut pas
être prouvée dans ZFC



*"The introduction of the digit 0 or the group concept was general nonsense too,
and mathematics was more or less stagnating for thousands of years
because nobody was around to take such childish steps..."*

Alexandre Grothendieck

Le Groupe Symétrique

Def X ens. le gpe symétrique de X
c'est l'ensemble des bijections de X
vers X

$$\text{Bij}(X, X) = \{f: X \xrightarrow{\sim} X\} = \text{Bij}(X) = G_X$$

Structures supplémentaires

composition: $f, g \in \mathcal{G}_X$ alors

$$g \circ f \in \mathcal{G}_X$$

$$f: X \rightarrow X \quad g: X \rightarrow X$$

$$g \circ f: X \xrightarrow{f} X \xrightarrow{g} X$$

$$\circ: G_X \times G_X \longrightarrow G_X \quad G_X = \text{Bij}(X, X)$$

$$(g, f) \longmapsto g \circ f$$

$g \circ f$ est bien une bij car c'est la composée de 2 bijections.

$\circ$ est associative: $h \circ (g \circ f) = (h \circ g) \circ f$

$$\sim G_X \neq \emptyset \quad \text{Id}_X \in G_X$$

Id_X neutre.

$$\forall f \in G_X \quad f \circ \text{Id}_X = f \quad \text{Id}_X \circ f = f.$$

→ Inversion (Reciproque)

$f \in G_X$ se réciproque $f^{-1} \in G_X$

$$f \circ f^{-1} = \text{Id}_X = f^{-1} \circ f.$$

Ces 3 structures font de G_X un groupe.

DÉFINITION 2.1. Un groupe $(G, \star, e_G, \cdot^{-1})$ est la donnée d'un quadruple forme de

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

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

- d'un element $e_G \in G$ (appele element neutre),
- d'une application (appele inversion)

$$\begin{array}{ccc} \bullet^{-1} : G & \mapsto & G \\ g & \mapsto & g^{-1} \end{array}$$

ayant les proprietes suivantes:

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

Exemples $(\mathbb{Z}, +, 0, - \bullet)$ est un gpe.

$(\mathbb{N}, +, 0, - \bullet)$ pas un gpe

$(\mathbb{Q}, +, 0, - \bullet)$ $(\mathbb{R}, +, 0, - \bullet)$

$(\mathbb{Z}^* = \{1, -1\}, \times, 1, \bullet^{-1})$ est un gpe

$(\mathbb{Z}^* = \mathbb{Z} - \{0\}, \times, 1, \cancel{\bullet^{-1}})$ pas un gpe

$(\mathbb{Q}^* = \mathbb{Q} - \{0\}, \times, 1, \cdot^{-1})$ est un gpe

$(\mathbb{R}^* = \mathbb{R} - \{0\}, \times, 1, \cdot^{-1})$ ———

- $G = \{e\}$ $e * e := e$ $e^{-1} := e$

$(\{e\}, *, e, \cdot^{-1} = \text{Id}_{\{e\}})$ est un gpe à 1 elt

gpe trivial. ——— $(G_x, \circ, \text{Id}_x, \cdot^{-1})$

Propriétés d'unicité: Soit $(G, *, e, \cdot^{-1})$

un gpe alors on a

- involutivité de l'inversion:

$$\forall g \in G \quad (g^{-1})^{-1} = g$$

- Soit $e' \in G$ tq il existe $g \in G$ vérifiant
 $g * e' = g$ alors $e' = e$.

- unicite de l'inverse: soit $g \in G$ et $g' \in G$
tq $g * g' = e$ alors $g' = g^{-1}$.
(pareil si $g' * g = e$)

- Inverse du produit: $\forall g, g' \in G$
 $(g * g')^{-1} = g'^{-1} * g^{-1}$.

Soit e' tq il existe g avec

$$g * e' = g \implies e' = e$$

$$g * e' = g$$

$$\neg \quad g * g * e' = g * g$$

$$e * e' = e$$

$$e' = e.$$

on veut mq $(g^{-1})^{-1} = g$

on a que $(g^{-1})^{-1} * g^{-1} = e$

et $g * g^{-1} = e$

g est donc un inverse de g^{-1}

$\Rightarrow$ c'est $(g^{-1})^{-1}$ par unicité de l'inverse.

si g' est tq

$$g + g' = e$$

$$g^{-1} * g + g' = g^{-1} * e$$

$$e * g' = g^{-1}$$

$$g = g^{-1}.$$

$$(g * g')^{-1} \stackrel{?}{=} g'^{-1} * g^{-1}$$

On calcule

$$(g'^{-1} * g^{-1}) * (g * g') = e$$

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

$$= g'^{-1} * e * g' = g'^{-1} * g' = e$$

Comme

$$(g'^{-1} * g^{-1}) * (g * g') = e$$

$g'^{-1} * g^{-1}$ est un inverse de $g * g'$
par unicité c'est $g'^{-1} * g^{-1} = (g * g')^{-1}$



Gps Commutatif: Un $\text{grp}(G, *, e, \cdot^{-1})$

est commutatif (abelian)

si $\forall g, g' \in G$

$$g * g' = g' * g.$$

$(\mathbb{Z}, +)$, $(\mathbb{Q}, +)$, $(\mathbb{R}, +)$ sont commutatifs
mais la plupart des gpes ne le sont pas

Ex: $G_X = \text{Bij}(X, X)$ n'est pas commutatif
des que X possède au moins 3 elts

Par exemple

$$\mathcal{G}_3 = \text{Bij}(\{1, 2, 3\})$$

il existe deux permutations

$$\sigma, \tau \in \mathcal{G}_3 \text{ tq } \sigma \circ \tau \neq \tau \circ \sigma.$$

Si X possède plus de 3 elts

$$X = \{x_1, x_2, x_3, \dots\}$$

on prend deux permutations de X
 σ, τ qui agissent de la même manière
que précédemment sur x_1, x_2, x_3
et qui fixes tous les autres elt de X

$$\forall x \in X - \{x_1, x_2, x_3\}$$

$$\sigma(x) = x \quad \tau(x) = x$$

$$\sigma \circ \tau \neq \tau \circ \sigma.$$

Gpe produit $(G, *, e_G, \cdot^{-1})$ et $(H, \times, e_H, \cdot^{-1})$

le gpe produit de G et H est le
gpe dont l'ensemble est

$$G \times H = \{ (g, h) \mid g \in G, h \in H \}$$

la loi de gpe est donnée par

$$(g, h) \boxtimes (g', h') = (g * g', h \times h')$$

l'inversion est

$$(g, h)^{-1} = (g^{-1}, h^{-1})$$

et le neutre est

$$e_{G \times H} = (e_G, e_H).$$

Ordre d'un gpe:

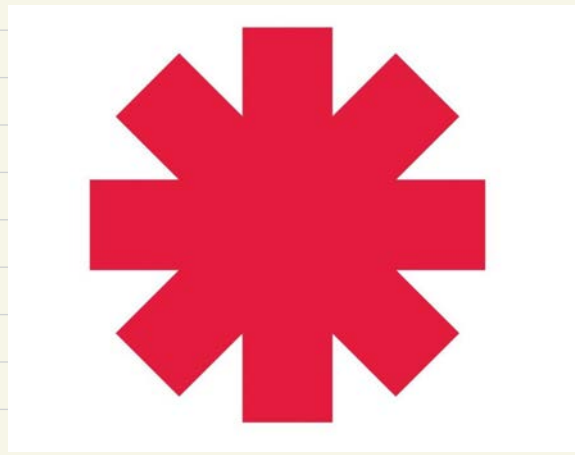
l'ordre d'un gpe G est son
cardinal $|G|$ si G est fini
et sinon $|G| = \infty$

Notations: la plupart du temps si le gpe

est quelconque on notera sa loi avec un
symbol multiplicatif $*$ $\times$ $\cdot$ $\times$ $\boxed{\times}$

si le gpe est commutatif on utilisera
un symbole qui ressemble a une addition

$+$, $\boxed{+}$ $\oplus$...



Autre exemple de symboles
de lois de composition

Notation exponentielle/multiple.

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

$$\overset{1}{g} = g, \quad \overset{2}{g \cdot g = g^2} \quad \overset{3}{g \cdot g \cdot g = g^3}$$

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

$$\overset{0}{g} := e, \quad \text{si } n < 0 \quad \overset{n}{g} := (g^{|n|})^{-1} = (g^{-n})^{-1}$$
$$= \underbrace{g^{-1} \cdot g^{-1} \cdot \dots \cdot g^{-1}}_{n \text{ fois}}$$

$$\forall m, n \in \mathbb{Z} \quad g^{m+n} = g^m \cdot g^n.$$

$$g^{-n} = (g^n)^{-1}.$$

—
Das

Dans un gpe commutatif note additivement
 $(G, +)$ on ecrira pour $n \geq 1$ entier

$$\underbrace{g + g + \dots + g}_{n \text{ fois}} =: n \cdot g$$

$$\begin{aligned} - 0 \cdot g &= e_G, \text{ si } n < 0 \quad n \cdot g = -(|n| \cdot g) = -(\underbrace{(-g) + (-g) + \dots + (-g)}_{|n| \text{ fois}}) \end{aligned}$$

et on a $\forall m, n \in \mathbb{Z}$

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

addition
ds $\mathbb{Z}$

addition ds G

$-g$ c'est l'inverse de g ds G
 $g + (-g) = e_G$

Sous-groupe : Soit $(G, \cdot)$ un gpe

un sousgpe de G est un sous-ensemble non-vide qui muni de la loi de gpe de G restreinte à H est un gpe.

DÉFINITION 2.4. Soit $(G, \star, e_G, \bullet^{-1})$ un groupe. Un sous-groupe $H \subset G$ est un sous-ensemble de G tel que

(1) $e_G \in H$.

(2) H est stable pour la loi de composition interne $\star$:

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

(3) H est stable par l'inversion:

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

et alors

$(H, \star|_{H \times H}, e_G, \bullet|_H^{-1})$ est un gr.

Notation de restriction

$$f: X \longrightarrow Y \quad X' \subset X$$

alors

$$f|_{X'}: X' \longrightarrow Y \quad \text{restriction de } f \text{ à } X'$$
$$x \longmapsto f(x)$$

Exemples: -

$(\mathbb{Z}, +)$ $2\mathbb{Z} = \{2n \mid n \in \mathbb{Z}\}$ = les entiers pairs

$(2\mathbb{Z}, +)$ est un sous-groupe de $\mathbb{Z}$

$$2\mathbb{Z} + 1 = \{2n+1 \mid n \in \mathbb{Z}\} - 0_{\mathbb{Z}} \notin 2\mathbb{Z} + 1$$

- la somme de 2 impairs
n'est pas impair

$(\mathbb{N}, +) \subset (\mathbb{Z}, +)$ n'est pas un ss gpe

l'inverse de 1 ds $\mathbb{Z}$ est $-1 \notin \mathbb{N}$

- $(G, \cdot, e_G, \cdot^{-1})$

- $G \subset G$ est un ss gpe

- $\{e_G\}$ est un ss gpe : le ss gpe trivial
de G

Classification des ss gres de $\mathbb{Z}$

Thm les ss gres de $\mathbb{Z}$ sont les ssens de la
forme $q \cdot \mathbb{Z} = \{qn \mid n \in \mathbb{Z}\}$ pour
 $q \in \mathbb{Z}$.

Preuve: on vérifie que pour $q \in \mathbb{Z}$
 $q\mathbb{Z}$ est un ssgrpe de $\mathbb{Z}$.

- soit $H \subset \mathbb{Z}$ un ssgrpe nq $\exists q \in \mathbb{Z} + q$
 $H = q\mathbb{Z}$.

Si $H = \{0\}$ c'est bon $H = 0.\mathbb{Z}$

Ops $H \neq \{0\}$

Soit $q \in H - \{0\}$ quitte à renv. q par $-q \in H$ $\wedge$ ops $q \geq 1$
(H est un ssgr)

Prenons q le plus petit des elts de H qui est > 0 . On va m. $H = q\mathbb{Z}$

Soit $h \in H$ (on veut mq $h = qn$ $n \in \mathbb{Z}$)

Par division euclidienne on peut écrire

$$h = qn + r \quad n \in \mathbb{Z} \quad r \text{ le "reste"}$$

$$0 \leq r < q$$

$$h = qn + r \iff h - qn = r$$

$$h = qn + r \iff \underbrace{h}_{\in H} - \underbrace{qn}_{\in H} = \underbrace{r}_{\in H}$$

$$qn = n \cdot q = \underbrace{q + \dots + q}_{n \text{ fois si } n \geq 0} \quad \underbrace{-n \text{ fois si } n < 0}$$

$$0 \leq r < q \text{ et ds } H$$

mais q est le + petit elt de $H > 0$

$$\implies r = 0 \implies h = qn \cdot$$

Exemple $(G, \cdot)$ un gpe

$$g \in G$$

$$g^{\mathbb{Z}} = \{ g^n \mid n \in \mathbb{Z} \} \subset G$$

$g^{\mathbb{Z}}$ est un ssgpe de G .

DÉFINITION 2.5. Soit G un groupe et $g \in G$ un élément de G . L'ordre de g est l'ordre du sous-groupe $g^{\mathbb{Z}} \subset G$ (ou $\mathbb{Z}.g$ si la notation est additive). On le note

$$\text{ord}(g) = |g^{\mathbb{Z}}| \quad (= |\mathbb{Z}.g| \text{ en notation additive}).$$

Prop (Critère de ss gpe) Soit G un gpe
et $H \subset G$ un ssensemble alors

H est un ss gpe de G ssi

— $\forall h, h' \in H$ le produit $h^{-1} \cdot h' \in H$

Preuve: si on prend $h' = h$ on sait que

$$- e_G = h^{-1} \cdot h \in H \Rightarrow e_G \in H$$

- comme on sait que $e_G \in H \quad \forall h \in H$ on
 $h^{-1} = h^{-1} \cdot e_G \in H \Rightarrow H$ est stable par $\bullet^{-1}$

- soit $h, h' \in H$ alors $h^{-1} \in H$ et $(h^{-1})^{-1} \cdot h' \in H$
 $= h \cdot h' \in H.$

Exemple bis :

Thm : Soit G un gpe alors G
"s'identifie naturellement" à un
sous-gpe de $G_G = \text{Bij}(G, G)$.

Thm (Lagrange) Soit G un gpe fini
et $H \subset G$ un ssgrpe alors l'ordre de
 H divise l'ordre de G

$$|H| \mid |G|$$

Cor: Si $|G|$ est premier alors les sous-grps de G sont $\{e_G\}$ et G .

Preuve : si $|G| = p$ et premier les seuls diviseurs de p sont 1 et p
 $\Rightarrow$ les sous-grps de G sont d'ordre 1 ou p .
 $\square$

Cor: Si $|G| = p$ premier pour tout

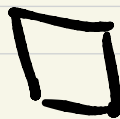
$g \in G - \{e\}$ on a

$$g^{\mathbb{Z}} = \{g^n \mid n \in \mathbb{Z}\} = G$$

Preuve: si $g \neq e$ $g^{\mathbb{Z}} \neq \{e\}$ et

$g^{\mathbb{Z}}$ est un ssgpx de $G \neq \{e\}$

$$g^{\mathbb{Z}} = G$$



Rmq: en particulier si $|G|=p$ premier

G est commutatif car

$G = \langle g \rangle$ et $\langle g \rangle$ est commutatif

$$\left(\begin{array}{cccccc} m & n & m+n & n+m & n & m \\ g \cdot g = g & = g & = g & = g & = g \cdot g \end{array} \right)$$