Chapitre 8

Théorie des ensembles

Groupes et relations

Georg CANTOR (1845 – 1918)

Évariste GALOIS (1811 – 1832)

Galois

Figure romantique des mathématiques par excellence, il meurt à 20 ans dans un duel amoureux. La veille de sa mort, il rédige un testament mathématique où il couche sur le papier certaines de ses idées. Il révolutionne les mathématiques. Ses idées, très profondes, sont encore extrêmement influentes dans les mathématiques contemporaines. Il est à l'origine de la théorie des groupes et de la théories des corps.

Cantor

La théorie des ensembles telle qu'on la pratique aujourd'hui est principalement l'œuvre de Georg Cantor, mathématicien allemand. Ses idées sur l'infini, qui sont aujourd'hui complètement admises, lui valurent l'hostilité de beaucoup de ses contemporains.

C'est le premier à avoir compris (et démontré) que :

- *deux ensembles infinis n'ont pas forcément « la même taille » ;*
- *il y a une infinité de « tailles » possibles pour les ensemble infinis ;*
- $\mathbb{N}$ *et* $\mathbb{N}^2$ *« ont la même taille » ;*
- $\mathbb{N}$ *et* $\mathbb{R}$ *« n'ont pas la même taille ».*

C'est le premier à avoir énoncé l'hypothèse du continu : $\aleph_1 = 2^{\aleph_0}$.

Chapitre 8: Groupes et relations

I. Lois internes, groupes

1) Lois

Déf : Soit E ens.
Une loi de composition interne (lci) sur E est une application de $E \times E$ dans E
$$m : E \times E \to E$$

Rq !! : Si $m : E \times E \to E$ est une lci et si $x, y \in E$
on notera $x \cdot y = m((x,y))$

2) Exemples

. $\mathbb{R} \times \mathbb{R} \to \mathbb{R}$
$(x,y) \mapsto x + y$

. $\mathbb{R} \times \mathbb{R} \to \mathbb{R}$
$(x,y) \mapsto \max(x,y)$

. $\mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$
$(n,m) \mapsto \mathrm{pgcd}(n,m)$

. $M_n(\mathbb{R}) \times M_n(\mathbb{R}) \to M_n(\mathbb{R})$
$(M,N) \to MN$

. Soit E un ens.
$\mathcal{P}(E) \times \mathcal{P}(E) \to \mathcal{P}(E)$
$(A,B) \mapsto A \cap B$

. $\mathcal{F}(E,E) \times \mathcal{F}(E,E) \to \mathcal{F}(E,E)$
$(f,g) \mapsto g \circ f$

. $\mathbb{R}^2 \times \mathbb{R}^2 \to \mathbb{R}^2$
$$\left(\begin{pmatrix} x \\ y \end{pmatrix}, \begin{pmatrix} a \\ b \end{pmatrix}\right) \mapsto \begin{pmatrix} x+a \\ y+b \end{pmatrix}$$

. $n \geq 1$
$\mathbb{R}^n \times \mathbb{R}^n \to \mathbb{R}^n$
$$\left(\begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}, \begin{pmatrix} y_1 \\ \vdots \\ y_n \end{pmatrix}\right) \mapsto \begin{pmatrix} x_1 + y_1 \\ \vdots \\ y_n + x_n \end{pmatrix}$$

. $p \in \mathbb{N} \cup \{\infty\}$, I intervalle

$$\begin{aligned} \mathcal{C}^p(I,\mathbb{R}) \times \mathcal{C}^p(I,\mathbb{R}) &\longrightarrow \mathcal{C}^p(I,\mathbb{R}) \\ (f,g) &\longmapsto f+g \end{aligned}$$

3) Associativité

Déf: Soit E ens. et soit $m : E \times E \to E$ une lci.
On dit que m est associative ssi$\overset{\Delta}{}$
$\forall x, y, z \in E \;,\; m\Big(\big(x, m((y,z))\big)\Big) = m\Big(\big(m((x,y)), z\big)\Big)$

Ie : $\forall x, y, z \in E,\; x \cdot (y \cdot z) = (x \cdot y) \cdot z$

Exemples:

. $+$ sur $\mathbb{R}$
$\times$ sur $\mathbb{R}$ sont associatives

. Mq $\mathcal{F}(E,E) \times \mathcal{F}(E,E) \to \mathcal{F}(E,E)$ est associative
$f \cdot g \to g \circ f$

démo: Soient $f, g, h : E \to E$
Mq $h \circ (g \circ f) = (h \circ g) \circ f$
C'est une $\forall$ assertion
Soit $x \in E$
On calcule :
$[h \circ (g \circ f)](x) = h\big((g \circ f)(x)\big)$

Or $(g \circ f)(x) = g\big(f(x)\big)$

donc $\left[h \circ (g \circ f)\right](x) = h\left(g\left(f(x)\right)\right)$

$\bullet \left[(h \circ g) \circ f\right](x) = (h \circ g)(f(x))$

$= h\left(g\left(f(x)\right)\right)$

d'où l'égalité ■

<u>Loi qui n'est pas associative</u>

$\mathbb{R} \times \mathbb{R} \to \mathbb{R}$
$(x, y) \mapsto x - y$

Soient $x, y, z \in \mathbb{R}$, on a :

$(x - y) - z = x - y - z$ et $x - (y - z) = x - y + z$

Ainsi, la soustraction est une lci non associative

<u>Notation :</u>
Si E est un ens. et $\cdot$ une lci
alors pour $x \in E$ et $n \in \mathbb{N}^*$, on note

$$x^n = \underbrace{x \cdot x \cdot x \cdot \ldots \cdot x}_{n \text{ fois}}$$

<u>Fait :</u> $x^n \cdot x^m = x^{n+m}$

Rq : • En général, une lci abstraite est notée multiplicative

. Quand la loi est notée additivement

On note plutôt $nx = x + x + \dots + x$

4) Commutativité

On dit qu'une loi est commutative $\overset{\Delta}{\text{ssi}}$

$$\forall x, y \in E, \quad x \cdot y = y \cdot x$$

Ex : . $M_n(\mathbb{R}) \times M_n(\mathbb{R}) \to M_n(\mathbb{R})$

$$M, N \mapsto MN$$

n'est pas commutative mais est associative

. la composition n'est pas commutative

Par ex, si $a, b \in E$ avec $a \neq b$ alors $\tilde{a} \circ \tilde{b} \neq \tilde{b} \circ \tilde{a}$

5) Neutre d'une loi

Déf : Soit E un ens muni d'une loi .

Soit $e \in E$

On dit que e est un neutre pour la loi

$\overset{\Delta}{\text{ssi}}$ $\forall x \in E$, $\underset{(*)}{x \cdot e = x}$ et $\underset{(**)}{e \cdot x = x}$

Rq : on a alors $e \cdot e = e$

Rq : . Quand la loi est commutative, on pourra le noter $+$ et le neutre sera noté 0_E

Prop : Soit E ens. et $\cdot$ une lci
Soient $e_1, e_2 \in E$ des neutres pour $\cdot$
alors $e_1 = e_2$

démo : on a $e_1 \cdot e_2 = e_1$ d'après (*) pour e_2 et $x = e_1$

et $e_1 \cdot e_2 = e_2$ d'après (**) pour e_1 et $x = e_2$

donc $e_1 = e_2$

Rq : Si le neutre existe, on le note e_E ou 1_E

Exemple : Dans $\mathcal{F}((E,E),\circ)$

le neutre existe, c'est Id_E

Rq : . le neutre n'existe pas toujours

Rq : a) 0 est le neutre de $pgcd(\cdot,\cdot)$
b) dans $(\mathcal{P}(E), \cap)$ le neutre est E
c) dans $(\mathcal{P}(E), \cup)$ le neutre est $\emptyset$
d) dans $(M_n(\mathbb{R}), \times)$ le neutre est I_n
e) dans $(\mathbb{R}^n, +)$ est $\begin{pmatrix} 0 \\ \vdots \\ 0 \end{pmatrix}$

Rq : Par convention, on pose $x^0 = 1_E$ si $x \in E$ et si $\cdot$ admet un neutre

D'où $\forall x \in \mathbb{C}, x^0 = 1$
$\forall f : E \to E, f^0 = Id_E$
$\forall M \in M_n(\mathbb{R}), M^0 = I_n$

6) Inverses

Déf : Soit E un ens.
Soit $\cdot$ une loi associative admettant un neutre e
Soit $x \in E$, soit $a \in E$

1) On dit que a est inverse de x à gauche (pour $\cdot$) $\overset{\Delta}{\text{ssi}}$ $a \cdot x = e$

2) ——— à droite ———
$\overset{\Delta}{\text{ssi}}$ $x \cdot a = e$

3) On dit que a est inverse de x $\overset{\Delta}{\text{ssi}}$ a est inverse de x à gauche et à droite.

Prop : Soit $x \in E$
Soient $a, b \in E$ qui sont tous les deux inverses de x
alors $a = b$

démo : On a : $a \cdot x = e$ (*)
On multiplie (*) à droite par b.
d'où $(a \cdot x) \cdot b = e \cdot b = b$
$\overset{\shortparallel}{a \cdot (x \cdot b)}$ par associativité
b car e neutre

Or $a \cdot \underbrace{(x \cdot b)}_{= e \text{ car } b \text{ inverse de } x} = a \cdot e = a$ car e neutre

CCL : $a = b$

Ainsi, l'inverse de x, si elle existe est unique.
On le note x^{-1}

. Quand la loi est notée $+$, l'inverse de x s'il existe est noté $-x$

⚠ L'inverse n'existe pas en général

On note Mots l'ens. des mots, on le munit de la concaténation, noté ·

ex : "Anouk" · "Eulalie" = "AnoukEulalie"

Le neutre dans (Mots, ·) existe, c'est le mot vide " "

On a :

$\forall m, m_1, m_2 \in$ Mots, $m \cdot m_1 = m \cdot m_2 \Rightarrow m_1 = m_2$

mais le seul mot inversible est " "

Prop : Soit $x \in E$ inversible (ie admettant un inverse)

alors

1) $\forall a, b \in E$, $x \cdot a = x \cdot b \Rightarrow a = b$

2) $\forall a, b \in E$, $a \cdot x = b \cdot x \Rightarrow a = b$

démo : exo

Prop : Soient $x, y \in E$ inversibles alors $x \cdot y$ est inversible et $(x \cdot y)^{-1} = y^{-1} \cdot x^{-1}$

7) Groupes

Déf : Soit $(G, \cdot)$ un couple où

1) G est un ensemble

2) $\cdot$ est une lci associative

On dit que $(G, \cdot)$ est un groupe ssi

- G possède un neutre, noté e_G
- tout élément $x \in G$ possède un inverse

Exemples

- $(\mathbb{R}, +)$ $\quad 0, -x$
- $(\mathbb{R}^*, \times)$ $\quad 1, \frac{1}{x}$ $\quad$ • $(\mathbb{R}_+^*, \times)$
- $(M_n(\mathbb{R}), +)$ $\quad 0_n, -M$
- $(\mathcal{C}^p(I, \mathbb{R}), +)$ $\quad \tilde{0}, -f$
- $(\{f : E \to E \mid f \text{ bijective}\}, \circ)$ $\quad Id_E, f^{-1}$
- $(\mathbb{K}[X], +)$ $\quad 0, -P$
- $(\mathbb{R}^n, +)$ $\quad 0_{n,1}, \begin{pmatrix} -x_1 \\ \vdots \\ -x_n \end{pmatrix}$
- $(\mathbb{C}, +)$
- $(\mathbb{C}^*, \times)$ $\quad$ • $(\mathbb{U}, \times)$ $\quad$ • $(\mathbb{U}_n, \times)$
- $(\{M \in M_n(\mathbb{R}) \mid M \text{ inversible}\}, \times)$ $\quad$ neutre : I_n, inverse : M^{-1}

  noté $GL_n(\mathbb{R})$

II, Relations

1) Définition

Soit E ens.

Une relation (binaire) sur E est une partie $\mathcal{R}$ de $E \times E$

Si $(x, y) \in \mathcal{R}$ on dit que x est en relation avec y (pour $\mathcal{R}$) et on note $x \mathcal{R} y$. sinon, on note $x \not\mathcal{R} y$

Exemples

En général, au lieu de définir $\mathcal{R}$ en tant que partie de $E \times E$, on donne une cond. néc. et suffisante (CNS) pour que $x \mathcal{R} y$.

. Sur $\mathcal{P}(E)$, on note $A \subset B \overset{\Delta}{\text{ssi}} \forall x \in A, x \in B$

. sur $\mathbb{Z}$,

$$n \mid m \overset{\Delta}{\text{ssi}} \exists k \in \mathbb{Z} : m = kn$$

. sur $\mathbb{R}$

$$x \leq y \overset{\Delta}{\text{ssi}} y - x \in \mathbb{R}_+$$

. sur $\mathbb{Z}$: $n \geq 1$

$$a \equiv b \ (n) \overset{\Delta}{\text{ssi}} n \mid b - a$$

. Sur Ginette

on note $x \mathcal{R} y \overset{\Delta}{\text{ssi}}$ x a déjà parlé à y

A-t-on :

1) $\exists x_0 \in$ Ginette : $\forall x \in$ Ginette, $x \mathcal{R} x_0$

2) $\exists x_0 \in$ Ginette : $\forall x \in$ Ginette, $x_0 \mathcal{R} x$

3) $\forall x \in$ Ginette, $x \mathcal{R} x$

4) $\exists x_0 \in$ Ginette : $x_0 \mathcal{R} x_0$

5) $\forall x, y \in$ Ginette, $x \mathcal{R} y \Rightarrow y \mathcal{R} x$

6) $\forall x \in$ Ginette, $\exists y \in$ Ginette : $x \mathcal{R} y$

7) $\forall x \in$ Ginette, $\exists y \in$ Ginette : $\begin{cases} x \mathcal{R} y \\ x \neq y \end{cases}$