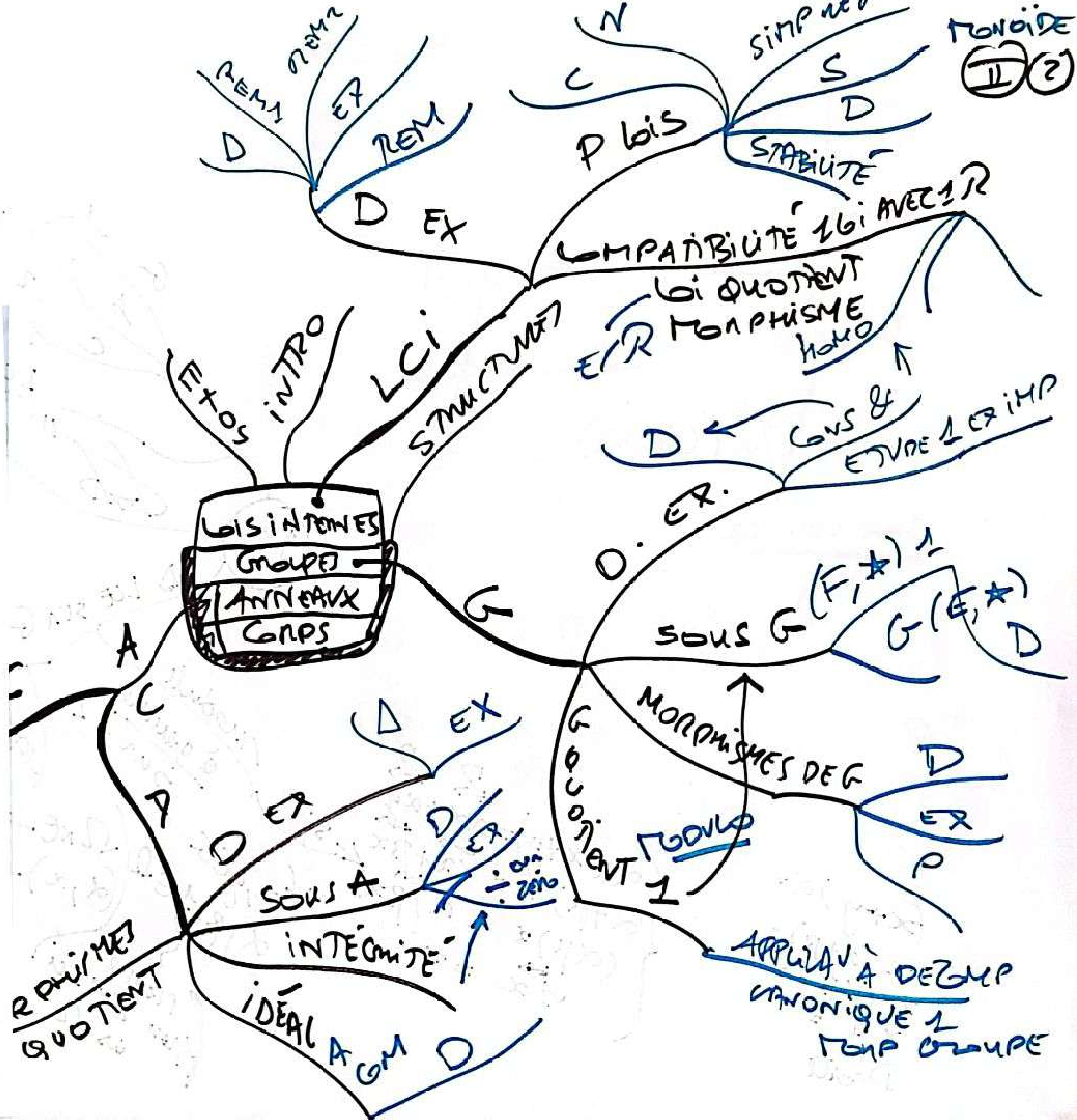
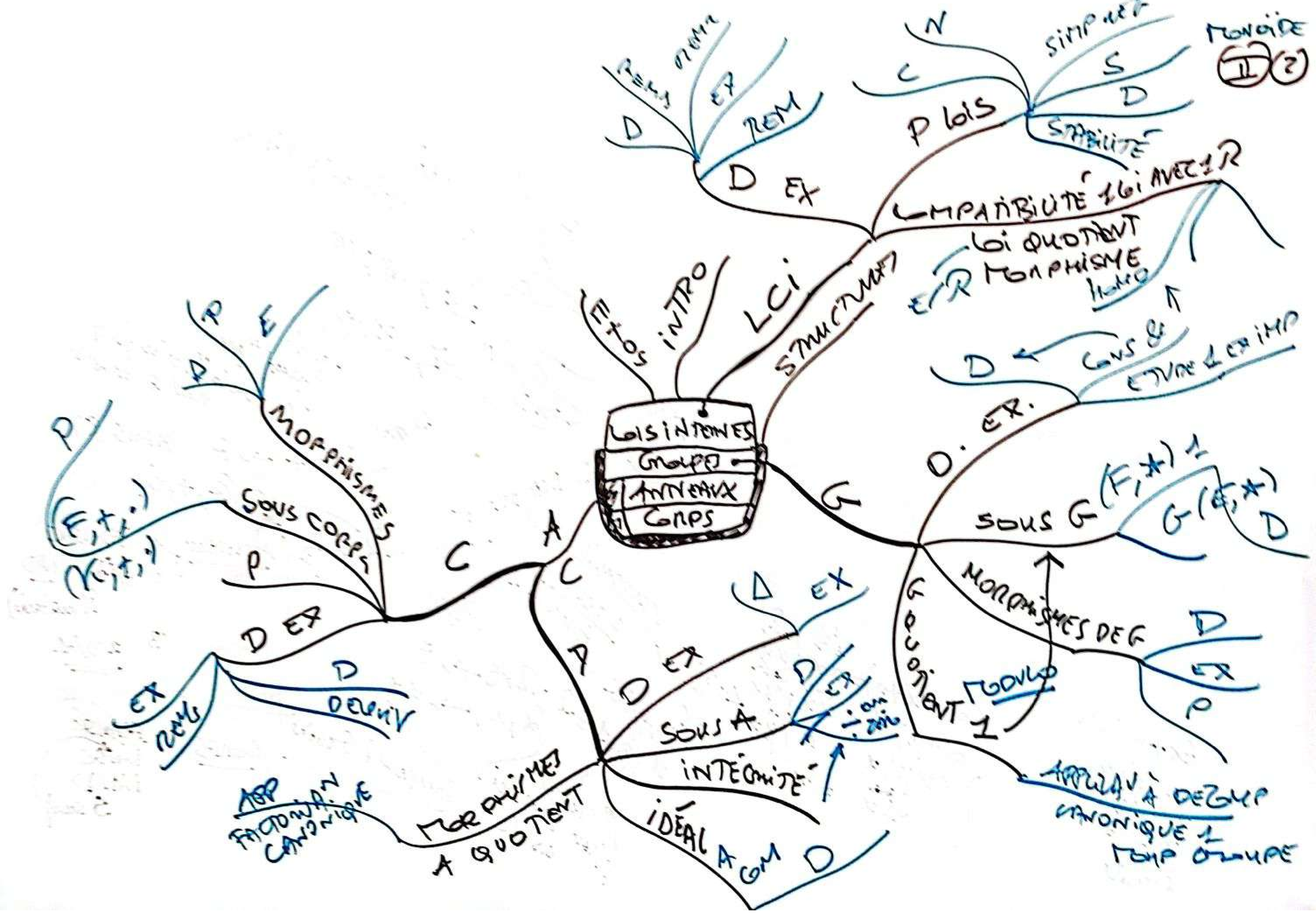
(I)

(2) Lois internes
Groupes. Anneaux. Corps.




LOIS INTERNES
GROUPES
ANNEAUX
CORPS
EXOS
INTRO
LCI
STRUCTURES
D EX
D
EX
REM
P LOIS
N
C
S
D
STABILITÉ
MONOÏDE
COMPATIBILITÉ LOI AVEC R
LOI QUOTIENT
MORPHISME
G
D. EX.
D
SOUS G
(F,*) 1
G(E,*)
D
MORPHISMES DE G
D
EX
P
G QUOTIENT
MODULO
1
CANONIQUE 1
A
C
P
D EX
SOUS A
D
EX
INTÉGRITÉ
IDÉAL
A COM
D
MORPHISMES
A QUOTIENT
FACTORISATION CANONIQUE
C
MORPHISMES
P
E
P
SOUS CORPS
(E,+,.)
(K,+,.)
P
D EX
EX
REMS
D

2 LI G A C

intro

- E ev ~~bo~~ bis verif P

verif "Base"

$\longrightarrow$ un gd nb aut P_s que l'on
autom

pouvo utiliser ds calculs

- ex GC $(\overrightarrow{v}, +)$
PLAN

- formellent cal ident

bien distinguer elts ds ≠ Ens

= entre elt metre differents
jamais

ni composer la def ....

≠ P R équiv

1) LCI

D the a $E \times E \xrightarrow{ok} E$

oc

(a, b) de $E^2 \xrightarrow{\text{un}}$ c unique

$c = a \perp b$

composé

R1 $c = f((a, b))$

R2

∀

et une seule

- N ou ÷ R ~~LCI~~

3-5

$\mathbb{R}^2$ $(x, 0) \longrightarrow$ ~~x~~

Li ds $\mathbb{R}^*$

De m s'ennuer unicité

Pourrait par ex

tentative de lois P affine

$(O, \vec{i}, \vec{j})$

"Somme" de points

$M(x_1, y_1)$

$N(x_2, y_2)$

$S(x_1+x_2 ; y_1+y_2)$

$\nearrow$ ≠ repère — Good $\nearrow$

$\nearrow$ (M, N) — plus résultats

$\cancel{LC}$

- résultat ∈ à E, ne pas oublier les autres conditions

Ex + x $\mathbb{N}$ $\mathbb{Z}$ $\mathbb{D}$ $\mathbb{Q}$ $\mathbb{R}$

- $\mathcal{P}(E)$ ∩ ∪ Δ

Par contre ⊂ ∁ — $\mathcal{P}(E) \to \mathcal{P}(E)$

Rel $\cancel{LC}$

$\times$ $\mathcal{P}(E) \times \mathcal{P}(E)$

- E F F ⊄ E

o $\cancel{LC}$ ds $\mathcal{F}(E, F)$

car E ou rien = E déj 2 ...

et si $f : E \to F$

$g : E \to F$

~~...~~ par contre on peut déf

loi o ds $\mathcal{F}(E)$

- si $F = \mathbb{R}$

R résultat ne dépend pas du choix de la rep^n des élts

∅ ne peut ê assignée par un ∞é de proc equiv.

Supposons que nous définissions

$\perp$ $\quad \frac{a}{b} \perp \frac{c}{d} = \frac{a+c}{b+d}$

- D ds loi quotient E/R

supposé ce ? classes ne dép du choix des représentants de la classe

• ~~+~~

$\forall (a,b,c) \in E^3,\ (a \perp b) \perp c = a \perp (b \perp c)$

~~nat~~ $= a \perp (\underline{c \perp b})$

• C $\quad a \perp b = b \perp a$ avant N

• N est

un elt e ssi N pour $\perp$

$\exists$

$\boxed{x \perp e = e \perp x = x}$

bref ~~x~~ on peux chercher si l $\exists$

$e \in E$ tq $x \perp e = x$

vérifier 2ème = et aussi (V)

P e unique

Ex $\quad 0 \ +\quad \mathbb{N}\ \mathbb{Z}\ \mathbb{D}\ \mathbb{Q}\ \mathbb{R}$

$\quad 1 \ \times$

$\emptyset \cup \mathcal{P}(E) \qquad A \cup \emptyset = \emptyset \cup A = A$

$E \cap$

$Id_E \circ \mathcal{F}(E)$

car $\forall f \in \mathcal{F}(E)$,

on a $f \circ Id_E = Id_E \circ f = f$

car

$\forall x \in E\ (f \circ Id_E)(x) = f[Id_E(x)]$

$= f(x)$

$= Id_E[f(x)] = f(x)$

• Simplifiable ou Regulier Elt

D à a, G $\forall b, c\ \ a \perp b = a \perp c$

$\Downarrow$

G+D = régulier $\qquad b = c$

Ex

- tt réel est simplifiable pour +

$a + b = a + c \Rightarrow b = c$

- ——— $\underline{\text{s}\neq 0}$ ——— $\times$

$\forall a \in \mathbb{R}^*$

$a \times b = a \times c \Rightarrow b = c$

0 ~~simp~~ pr $\times$

$0 \times 2 = 0 \times 3$ or $2 \neq 3$

- $\mathcal{P}(E)$ aucun elt of E n'est simpl

pr $\cap$

$\emptyset$

— $\cup$

- $\mathcal{F}(E)$ seule f bij (donc permutation)

Sont les elts simplifiables pr $\circ$

en effet si f est bij f^{-1} existe

or $f \circ g = f \circ h \Rightarrow f^{-1} \circ (f \circ g) = f^{-1} \circ (f \circ h)$

$\Rightarrow$ ...

• ~~elts~~ sym $\overline{S}$

a symétrisable à D

si $\exists a'$ tq $\underline{a \perp a' = e}$ | à D

a G

P. C $a' = a''$

. A unique

Not°

$+$ $-a$

$. \times$ a^{-1} $\mathbb{Q}^* \; \mathbb{R}^* \; 1/a$

non a^{-1} a'

P ~~lois~~ lois $\perp \neq$ on a

1) Si a admet un S
Alors a est ~~sy~~ simplifiable

2) Si a b admettent a' b'

$a \perp b$ admet pr sym

$b^{-1} \perp a^{-1}$. $((a \perp b)^{-1} = b^{-1} \perp a^{-1})$.

Sym de $a \perp b$ sera $a^{-1} \perp b^{-1}$
si $\perp$ com
Sinon il faut respecter ordre composition

Ex
$\mathbb{N}$ seul 0 a un S lui-même pr +

$\mathbb{Z} \; \mathbb{D} \; \mathbb{Q} \; \mathbb{R}$ $-a$ / $\mathbb{Z}$ seuls -1 1
1
autres elts n'ont pas
de sym !

$\times$

R

$\exists$ E admet un elt neutre pour $\perp$, e

e est son propre S pour $\perp$

donc E admet un $\perp$ et symétrisable

D $(E, \perp, e)$ / Monoïde
I
A
N

EX $(\mathbb{N}, +, 0)$

$(\mathcal{P}(E), \cap, E)$

$\cup \ \emptyset$

$(\mathcal{F}(E), \circ, Id_E)$

$(\mathbb{Z}, +, 0)$

$(\mathbb{R}^*, \times, 1)$ } $+ S = G$

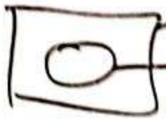
• D $\star / \perp$

~~$(a \star b)$~~ $a \star (b \perp c) = (a \star b) \perp (a \star c)$

$\underline{\text{et}}$ $(b \perp c) \star a = (b \star a) \perp (c \star a)$

• Stabilité d'une SE de E par Li de E

D



E
A Partie stable pour $\perp$

Si $\perp$ interne de A, donc :

$\forall (a, b) \in A^2, \ \underline{a \perp b \in A}$

Cnd suffisante

un comme a et b sont aussi des elts de E

E et $\exists$ un elt unique $a \perp b \in E$ ("reste")

EX $\mathbb{N}$ $+ \times$ de $\mathbb{R}$

P parties stables par une Li $\perp$ interne de E

$\exists$ $\perp$ A ou C, car aussi de A

- e si $e \in A$

Groupes

Compatibilité d'une loi et d'une $\mathcal{R}$

D $E \perp$

$\mathcal{R}$ / sur E

Comp avec $\mathcal{R}$

Si, pour tous $a, b, a', b' \in E$, on a :

$(a \mathcal{R} a'$ et $b \mathcal{R} b') \Rightarrow (a \perp b) \mathcal{R} (a' \perp b')$

Ex

- $\mathbb{R}$ $+$ $\leq$

  $(a \leq a'$ et $b \leq b') \Rightarrow (a+b \leq a'+b')$

- $\mathbb{N}$ $\times$ $\leq$ non ds $\mathbb{R}$

  $-2 \leq -1$ et $1 \leq 3$ or $-2 \geq -3$

- $\mathbb{Z}$ $+$ Cong mod n

  $a \equiv b \iff b-a = 3.k \ (k \in \mathbb{Z})$

...

Loi quotient ★

Définie ds ens quotient $E/\mathcal{R}$

~~D&T~~ T&D

$E \perp$

$\mathcal{R}$ est compatible avec

Alors ceci de $E/\mathcal{R} \times E/\mathcal{R}$

ds $E/\mathcal{R}$

$(\bar{a}, \bar{b})$ $\quad a \perp b$, $\overline{a \perp b}$

on une LCI de $E/\mathcal{R}$

$\bar{\perp}$

$\forall (a,b) \in E^2 \quad \bar{a} \,\bar{\perp}\, \bar{b} = \overline{a \perp b}$

...

Str alg de $E \perp$ se transmet à ens quotient muni de la loi quotient $\bar{\perp}$

moyennant d'autres compatibilités

Morphisme = homo

D E F

$\perp$ $*$

E ≠ F [illegible]

Il y a $f : E \to F$

tq im [illegible] f on suppose que $\perp$ [illegible] ?

[illegible] quels $a, b \in$ [illegible]

ce qui s'écrit

$$\boxed{\forall (a,b) \in E^2,\ f(a \perp b) = f(a) * f(b)}$$

Ex $\mathbb{N}\ +\ \mathbb{R}\ \times$

- $f(n) = 2^n$

$\forall (n,m) \in \mathbb{N}^2,\ f(n+m) = 2^{n+m}$

$= 2^n \times 2^m$

$= f(n) \times f(m)$

- $E = F$

$\mathcal{P}(E)\ \cup\ \cap$

$f(A) = \overline{A} = E - A$

$\overline{A \cup B} = \overline{A} \cap \overline{B}$

D

mor bij isomorph

E = F automorph

2) G

(E Lci

$\perp$) $\Leftrightarrow$ 3C sont réalisées :

1) A GrAVS

2) N e

3) S MIAN

C abélien

Grs D 1 P ...

e unique

s unique et $(a\perp b)^{-1} = b^{-1}\perp a^{-1}$ ★

$\forall$ elt est simplifiable = regulier

puisque A et S

$a\perp x = b \quad x = a^{-1}\perp b$

$x\perp a = b \quad x = \boxed{b\perp a^{-1}}$

$\mathbb{Z}+ \quad \mathbb{D}+ \quad \mathbb{Q}+ \quad \mathbb{R}+ \quad \mathbb{Q}^{*},\times \quad \mathbb{R}^{*}\times$

$(\sigma(E), \circ)$ pas $\not\subset$

$(\vec{v}, +)$ N $\vec{0}$ $\Rightarrow$ classe ac (A,4)

$(\mathcal{P}(E), \cup)$ $\not\subset$ sauf si $E = \varnothing$

⚠

$(\mathbb{R}, \times)$ $\not\subset$ car 0 pas inverse pour $\times$

$\Leftrightarrow (E, \perp)$ G

et

$\Leftrightarrow \mathcal{R}$ E comp avec

rel éq sur E

, ~~(E/R)~~ $(E/\mathcal{R}, \top)$ G

. $\mathcal{F}(E, \mathbb{R})$

~~$\forall f \in$~~ $\forall x \in E\ (f+g)(x) = f(x)+g(x)$

$(\mathcal{F}(E, \mathbb{R}), +)$ GC

$\neq 0$ ⚠

Ensuite 1 ex important

EV $\mathbb{R}^n$ - ent positif

$(\mathbb{R}^2, +)$ GC $\quad +\mathbb{R}^n \quad +\mathbb{R}$

Noir

pourrait être tenté

~~[illegible]~~ $\times$ — ~~Lci~~ !

analogie

SG $(F,\star)$ d'un G $(E,\star)$

si G

→ 2 erreurs fréquentes

1ère :

tt SE d'1 G est un SG

$\mathbb{N}$ $(\mathbb{Z},+)$

~~StG~~ + $\cancel{\star}$

2ème :

oublier que F dont on veut démontrer qu'il a pour loi $\star$ est $\subset E$

E, $\star$ Grp

Or nous allons ~~montrer~~ grâce à la P qui suit, voir qu'il est bien + rapide de démontrer que $(F,\star)$ est un SG de $(E,\star)$ que de démontrer que $(F,\star)$ est un G lors $F \subset E$

P CNS pour que $(F,\star)$ soit SG $(E,\star)$ donné

1) $F \neq \emptyset \subset E$

2) F stable par $\star$ (ou $\star$ est interne ds F)

3) tt elt de F a son inverse son sym par $\star$ ds F

$\forall x \in F;\ x \in F \Longrightarrow x' \in F$

Σ $(E,\star)$ GC $\Rightarrow$ $(F,\star)$ SGC de $(E,\star)$

R Σ $(E,\star)$ $\cancel{C}$, on ne peut rien en déduire pour $C^{té}$ G $(F,\star)$ car il se peut que elts de F commutent entre eux sans que ts elts de E commutent

Dc ~~inutile~~ car $F \neq \emptyset \subset E$

dm que loi $\star$ ds F,

que cette loi assoc mN

S'

ça P étant vraies ds E ...

par contre supposé 2 elt. ds F

pouvant ê un elt ou E ... etc

Ex F de $\mathbb{R}^3$ $(a, b, 0)$

Morphisme de Gs

$(G, \perp)$ $(G', \star)$

$(\forall (a,b) \in G^2)$ ~~f(f)~~ $f(a \perp b) = f(a) \star f(b)$

bij isom

Ex

1. ln isom $\overbrace{(\mathbb{R}^*_+, \cdot)\ (\mathbb{R}, +)}^{bis}$

$\forall (x,y) \in \mathbb{R}^{*2}_+$, ~~et~~ $\ln(x \cdot y) = \ln x + \ln y$

2. $\vec{v}$ $\vec{V}$ $\underline{ens}$ $t_{\vec{u}}$ $\mathcal{T}$

$(\vec{V}, +)$ $(\mathcal{T}, \circ)$

$\forall (\vec{u}, \vec{v}) \in \vec{V}^2$ $t_{\vec{u}+\vec{v}} = t_{\vec{u}} \circ t_{\vec{v}}$

bis

4. | |

$(\mathbb{R}, +)$ ~~homom~~ ds $\mathbb{R}$

car $|a+b| \neq |a| + |b|$

$(\mathbb{R}^*, \cdot)$ homom

Rappels

loi quotient déf ds ens quotient $E/\mathcal{R}$

$E \perp$ $\mathcal{R}E$ compat avec $\perp$

$\left[(a \mathcal{R} a' \text{ et } b \mathcal{R} b') \Rightarrow (a \perp b) \mathcal{R} (a' \perp b') \right]$

$E/\mathcal{R} \times E/\mathcal{R} \rightarrow E/\mathcal{R}$

$(\bar{a}, \bar{b}) \longmapsto \overline{a \perp b}$

Loi ds $E/\mathcal{R}$

$\bar{\perp}$ ie $\perp$

$\forall (a,b) \in E^2$ $\bar{a} \mathbin{\bar{\perp}} \bar{b} = \overline{a \perp b}$

↳ ∘ canonique f

$$(G,\perp) \longrightarrow (G/\mathcal{R}, \overline{\perp})$$

Propriétés des morphismes de Groupes

$(G,\perp)(G',\star)$ homor

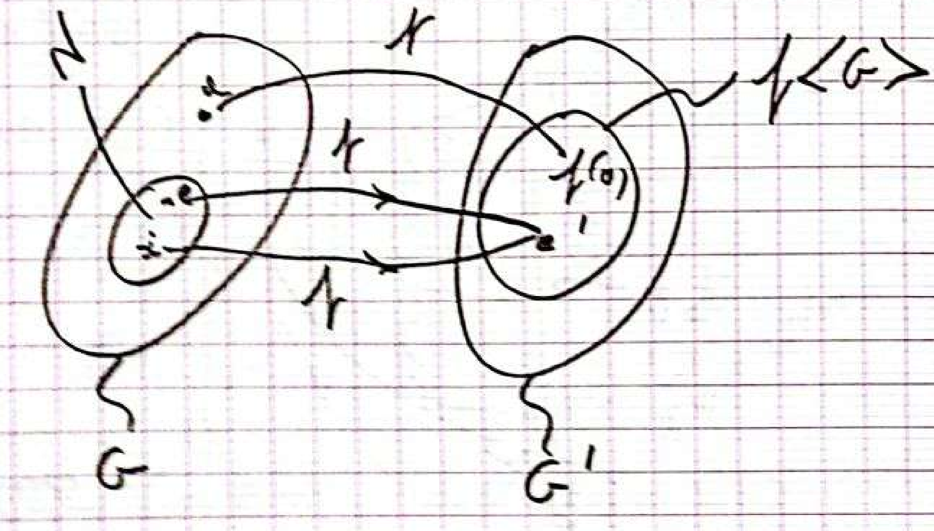
$\exists\, e'$ / $f(e)=e'$

$e \; e^{-1} \quad f(e)\; f(e^{-1})$

$f\langle G\rangle = \{f(x) / x\in G\}$ SG de G' Im de f

$N = \{x\in G / f(x)=e'\}$

Si f inj … $\cancel{\{N\}} = \{e\}$



G quotient modulo un SG

$(G,\perp)$ GC

$(H,\perp)$ SG de G

on définit des G $\mathcal{R}$ par

Si $(x,y)\in G^2$

$x\mathcal{R}y \Leftrightarrow x\perp y^{-1}\in H$

ERST

permet def $(G/\mathcal{R}, \overline{\perp})$

$(G/H, \overline{\perp})$

ds un G, on peut associer à tte $\mathcal{R}$ … sur G compatible avec la sur G le SG H = Noyau

morph canonique $g : (x \longmapsto \bar{x}$

Application à la somme cumique d'un morph de Gs

...

3) Str A & C

1) A

$(E, +, \cdot)$

1 GAINS
0

2 • A

3 • D

Si possède 1 pr. unitaire multiplic

Ex $(\mathbb{Z}, +, \cdot)$ C unifère

D

O

$(\mathbb{R}, +, \cdot)$

$\mathcal{F}(E, \mathbb{R}, +, \cdot)$ CU

P $(A, +, \cdot)$
0

Alors $\forall x \in A \quad \underline{x \cdot 0 = 0 \cdot x = 0}$

A
G G
Z
N
S
C
D

!

A
Z
S
C
A
D

absorbant pr . de A

GNS

Si $(A, +, \cdot)$ ~~n'est~~ $(\{0\}, +, \cdot)$

Si Gi pas nécess. $a \cdot b = 0$

A N de A pr +

n'admet pas de sym

SA $(H, +)$ SG de $(A, +)$

H stable pr x

$\forall (x, y) \in H^2, \; x \cdot y \in H$

$x - y \in H$

$x \cdot y \in H$

Diviseurs de zéro

$A \neq \{0\} \quad (A, +, \cdot)$ C
0

a et b sont des diviseurs de 0

si $a \neq 0$ et $b \neq 0$

et $a \cdot b = 0$

A sans diviseur de 0 est dit intègre

lors

Idéal d'un A C

$(A,+,\cdot)$ C

$H \subset A$

$H \neq 0$

$(H,+,\cdot)$ idéal de A si

i) $(H,+)$ est un SG de $(A,+)$

ii) ~~$\forall x$~~ $\forall a \in A, \forall x \in H \quad a.x \in H$

...

B) Str de Grps

A

i i

A A

N (unitaire intègre)

S

C

D

$+ \quad \cdot$

$(A,+,\cdot)$

$(A^*,\cdot)$ G

P $(K,+,\cdot)$

– tt elt de K est simplifiable pr +

– sauf 0 — X

est absorbant pour .

$\forall (a,b) \in A^2,\ a.b = 0 \Leftrightarrow \begin{cases} a = 0 \\ \text{ou} \\ b = 0 \end{cases}$

pas de diviseur de 0

$a.x = b$