ENSEMBLES & LOGIQUE

X est l'ensemble vide $\longmapsto X = \emptyset$ — aucun elt

disjoints $A \cap B = \emptyset$

~~[illegible]~~ $\neg(p \wedge q) \longmapsto (\neg p) \vee (\neg q)$

fini $X = \{a, b, c, d\}$

$x \in X$

Et resumé notions fondamentales sauf Ev et EA NB!

① LCI & GROUPES

② ANNEAUX & CORPS

(3)

④ MORPHISMES

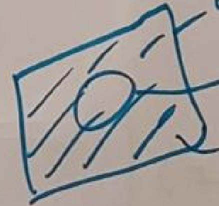
BAILLY

STR ALG

$\ldots, \ldots\}$ exprime qu'il existe ∞é

$\emptyset \in \mathcal{P}(E)$

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



$E \setminus A \begin{cases} A \\ E \end{cases}$

$X^c = \emptyset$ $X \cup X^c = E$

deux à la fois

Soit l'un soit l'autre soit les deux à la fois

$= X \cap Y^c$

$\mathrm{card}(A \cup B) = \mathrm{card}\, A + \mathrm{card}\, B - \mathrm{card}(A \cap B)$

$X = \text{—} \times \text{—}$

$\mathrm{card}\, \emptyset = 0$

ENSEMBLES & LOGIQUE

X est l'ensemble vide $\longmapsto X = \emptyset$ — aucun elt

disjoints $A \cap B = \emptyset$

~~Faux~~ $\neg(p \wedge q) \longmapsto (\neg p) \vee (\neg q)$

fini $X = \{a, b, c, d\}$

$x \in X$

$f \notin X$

$\{a, b\} \subset X$

infini $\mathbb{N} = \{0, 1, 2, 3, \dots, n, n+1, \dots\}$ exprime qu'il existe ∞é

$\emptyset \in \mathcal{P}(E)$

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

$X \subset E \longmapsto X \in \mathcal{P}(E) = 2^E$

$E \setminus A \begin{cases} A \\ E \end{cases}$

$X \subset E \quad X^c = \{x \in E \mid x \notin X\}$ $\quad X \cap X^c = \emptyset \quad X \cup X^c = E$

$= E \setminus X$

les deux à la fois

$X \subset E, Y \subset E$

$X \cap Y = \{x \in E \mid x \in X$ et $x \in Y\}$

$\cup$ — — ou — Soit l'un soit l'autre soit les deux à la fois

$X \setminus Y =$ — — et $x \notin Y\} = X \cap Y^c$

DEMORGAN $(X \cap Y)^c = X^c \cup Y^c$

$\cup \quad \cap$

$E \times F = \{(x, y) \mid x \in E$ et $y \in F\}$

$\mathrm{card}(A \cup B) = \mathrm{card}\, A + \mathrm{card}\, B - \mathrm{card}(A \cap B)$

$\times \quad = \quad — \times —$

$\mathrm{card}\, \emptyset = 0$

$X = \{x \in E \mid p\} \longmapsto$

X est la partie de E pour les elts de laquelle la p est vraie

$X^c = \{x \in E \mid \neg p\}$

$Y = \{x \in E \mid q\}$

$\underset{\cup}{X \cap Y} = \{x \in E \mid \underset{\vee}{p \wedge q}\}$

DE MORGAN (négation d'une conjonction, disjonction)

$\neg (p \underset{\vee}{\wedge} q) \longmapsto (\neg p) \underset{\wedge}{\vee} (\neg q)$

$X = E \longmapsto \forall x \in X, p$ "p ∀ elt de X p est vraie"

$X \neq \emptyset \quad \exists x$ ——— il existe au moins —

Nég° 1 p quantifiée

$\neg (\underset{\exists}{\forall} x, p) \longmapsto \underset{\forall}{\exists} x, \neg p$

i $p \Rightarrow q \vdash (\neg p) \vee q$

Conjuguées

$(p \Rightarrow q) \vdash (\neg q \Rightarrow \neg p)$

directe   contraposée

$q \quad p$ $p \quad q$

réciproque   inverse
= converse

double i

$(p \Rightarrow q) \wedge (q \Rightarrow p) \vdash p \vdash q$

ssi $\vdash \Leftrightarrow$

Déduction $p \wedge (p \Rightarrow q) \vdash (p \vdash q)$

si p je déduis q

FONCTIONS

$f : E \longrightarrow F$

$x \longmapsto f(x)$

Pr argument il existe 1 valeur au plus

$\mathcal{D}_f$ SE de E pr lesquels il existe une val de f

application $\mathcal{D}_f \to F$

$\mathrm{Im}\, f = \{y \in F \,/\, \exists x \in E,\ y = f(x)\}$

SE des elts de F qui ont des ant par f

i ssi $(f(x) = f(x') \Rightarrow x = x')$

s $\quad \forall y \in F, \exists x \in \mathcal{D}_f\ y = f(x) \mapsto \mathrm{Im} f = F$

b

$\mathcal{R} = (E, F, G)$

D A graphe

$(x,y) \in G \longmapsto x \mathcal{R} y$

$a : E \times F \to \{\text{vrai}, \text{faux}\}$

$(x,y) \longmapsto 1 \longmapsto x\mathcal{R}y$

$0 \quad \neg(\ )$

D ds E ssi $E = F$

R binaire propriété caractéristique que peuvent vérifier (ou non) les élts de $E \times E$

ss R bin Ens de couples sur lesquels R est vérifié

PRÉORDRE

(R) $\forall x \in E \quad x\mathcal{R}x$

(T) $\forall x, \forall y, \forall z \quad x\mathcal{R}y$ et $y\mathcal{R}z \Rightarrow x\mathcal{R}z$

ORAT

(A) $x\mathcal{R}y$ et $y\mathcal{R}x \Rightarrow x = y$

"ds les 2 sens" $a\mathcal{R}b \Leftrightarrow b\mathcal{R}a$

ERST

(S) $x\mathcal{R}y \Rightarrow y\mathcal{R}x$

ssi définit une partition de E

parties ou classes X_i de E $(X_1, X_2, \dots)$ vérifiant

$X_1 \cup X_2 \cup X_n = E$

$X_i \cap X_j = \emptyset$ ssi $i \neq j$

et pour tt $i \in X_i \quad X_i \cap X_i \neq \emptyset$

$x\mathcal{R}y$ ssi $\exists X_i$ tq $x \in X_i$ et $y \in X_i$

• ERST

$\mathbb{Z}$ $a\mathcal{R}b$ signifie $a-b$ multiple de

Classe d'équivalence de a modulo $\mathcal{R}$ (ds E)

L'ensemble de ts les élts x de E qui vérifient $x\mathcal{R}a$ pour a fixé

Ens des CEs (modulo $\mathcal{R}$)

forme SE de parties de E, disjointes 2 à 2

$E/\mathcal{R} \quad \frac{E}{\mathcal{R}}$ Ens quotient de E par $\mathcal{R}$ *

• ORAT

$\mathbb{R} \leq$

total Pr tt couple (a,b) de E^2, l'on a $a\mathcal{R}b$ ou $b\mathcal{R}a$

$(\mathbb{R}, \leq)$

Partiel on peut trouver au moins un couple (a,b) de E^2 ne vérifiant pas $\mathcal{R}$

$\mathbb{N}^*$ a divise b

3 divise 7 n'est pas vérifiée

• LC

$E\ F\ G$

a $E \times F \longrightarrow G$

• LCI

$E \times E \longrightarrow E$

opération

• LCE déf sur E à aide de $\mathbb{K}$

$\mathbb{K} \times E \longrightarrow E$

opération externe de E, déf avec $\mathbb{K}$

$\mathbb{N} \times \mathbb{N} \longrightarrow \mathbb{N}$

$(p,q) \longmapsto p^q$ somme de p est exposant à q

Produit des vecteurs de $\mathbb{R}^2$ par scalaires $\mathbb{R}$

$\mathbb{R} \times \mathbb{R}^2 \longrightarrow \mathbb{R}^2$

$(\lambda, \vec{v}) \longmapsto \lambda \vec{v}$ obtenu en $\times$ composants de $\vec{v}$ par le réel λ

P^{tés} POSSIBLES ASSOCIÉES À UNE loi INT

$E \times E \longrightarrow E$ $\quad$ $(E,*)$

$(a,b) \longmapsto a*b$

I signifie $\forall (a,b) \in E \times E : a*b \in E$

A Lq $(a*b)*c = a*(b*c)$ $\forall (a,b,c) \in E^3$

C Lq $a*b = b*a$ $\forall (a,b) \in E^2$

N elt neutre ds $(E,*)$

Lq qu'il existe e ds E

$\forall a \in E$ $\quad a*e = e*a = a$

Si e existe, il est unique

S'il existe e tq on ait seulement

$e*a = a$

N à gauche (idem à D)

S elts sym ds $(E,*)$

Lq e existe sym de $a \in E$ est Lq qu'il existe

a' ds E $\quad a*a' = a'*a = e$

· Si e' existe, il est unique

· S'il existe e' tq on ait seulement

$e' * e = e$

sym à G

· Cas usuels

$+$ N O O_E

S opposé $-a$

$\times$ ( ) N 1_E S inverse a^{-1} $1/a$

P 2 LCi

$*$ T

· Dé de T par rapport à $*$

1 $aT(b*c) = (aTb)*(aTc)$ G

2 $(b*c)Ta = (bTa)*(cTa)$ D

G A C

Li $*$ T $(E,*)$ (E,T) $(E,*,T)$

G $(E,*)$

I A N S

C abélien si on suit $*$ C, suffit d'avoir un N à D ou sym à D ... "tout court"

A $(E,*,T)$

G C: A N S C (C)

A: A D — UNITAIRE

(C) — COMMUTATIF

D

C

A N S C

A N → SAUF N de $(E,*)$

ZERO ; UNITÉ

$E * T$

0_E 1_E

DIVISEURS DE ZERO

Si 2 elts distincts on a

$a \neq 0_E$, $b \neq 0_E$

$a T b = 0_E$

diviseurs de 0

INTÉGRITÉ

Si il y a des $(E,*,T)$ n'est pas intègre

UN GROUPE est nécessairement

$(E,*,T)$:

$a T b = 0$

$\Rightarrow [a = 0$ ou $b = 0]$

4 Axiomes vérifiés

I $\neq \emptyset$

II i $*: E \times E \to E$ $(x,y) \mapsto x * y$

III A

IV élément neutre e

V inverse

fini

ordre n

Ex Rotations carré de Klein

$x * y = y * x$

$(E, *, \perp)$

I $(E,*)$ Groupe Com

II $\perp$ A

III $\perp$ D/$*$

$(\mathbb{Z},+,\times)$ Com et unitaire Polynômes à coef réels

Anneau unitaire dont tt elt $\neq e$ pour $*$ a un inverse pour $\perp$

$(\mathbb{Q},+,\times)$ $(\mathbb{R},+,\times)$ Com

$\exists$ ~~Com~~ quaternions

MORPHISMES

HOMOM

$f : (E, *) \longrightarrow (F, T)$

$x \longmapsto f(x)$

$\forall (x, x') \in E^2 : \quad f(\underbrace{x * x'}_{\text{ds } E}) = \underbrace{f(x)\, T\, f(x')}_{\text{ds } F}$

"transporte"

la loi $*$ de E en la loi T de f

ex $(\mathbb{Z}, +) \longrightarrow (F, \times)$

$n \longmapsto f(n) = 5^{n} \in \mathbb{R}$

$f(n+n') = 5^{n+n'}$ de $f(n+n') = 5^{n} \times 5^{n'}$

or $5^{n} = f(n)$
$5^{n'} = f(n')$ Donc $f(n+n') = f(n) \times f(n')$

ENDO $F = E$ et event T et $*$ identiques

f peut ê "plus fois" homo en ensb si il y a plus opé ds E et F

ISO bij AUTO $F = E$ ~~mais~~ et $* = T$

+ mvt entre 2 G, A,
doit faire correspondre lois nom "chacune à chacune"

STR ALG 1/6 LCI + Groupes

- G c'est un E muni d'une "opération" vérifiant certaines p^tés

$+$ 2 nbs f^ns suits mut

$-$

$\times$

$\div$

quelque chose qui à partir de 2 élts de E

– Soit ne donne pas de résultat $(3 \div 0)$ * NB !

– Soit ___ " ___ qui est un élt de E

pas forcément une application !

Résumé $E \times E \xrightarrow[\text{élts}]{f} E$

- LCI * image (x, y) $x * y$

$\uparrow$ puis sur $\mathbb{N}$ $\underline{a \uparrow b} = a^b$

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

$\cup$ ___

$\oplus$ directe de 2 SEV

$\circ$ composition des ap^ns

. A Comment lire $x * y * z$ de manière ~~antique~~

$(x * y) * z$ $\qquad$ $x * (y * z)$

$3 - 2 - 1 = $ 0 ? / 2 ?

ssi $\forall (x, y, z) \in E^3$, $(x * y) * z = x * (y * z)$

EX

$+ \; - \; \times \; \div \; \uparrow \; \cap \; \cup \; \circ$?

$3 + 2 + 1 = 6$

$3 - (2 - 1) = 3 - 1 = 2$

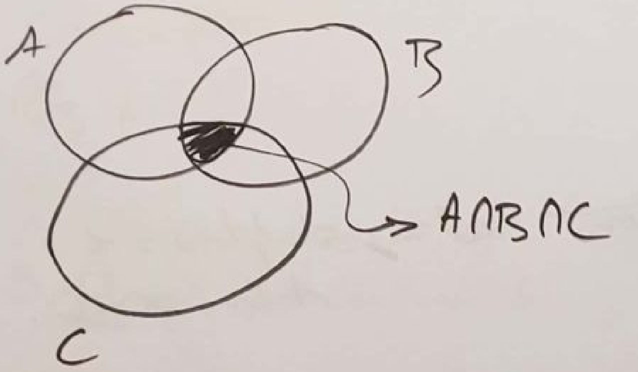
$(3 - 2) - 1 = 1 - 1 = 0$

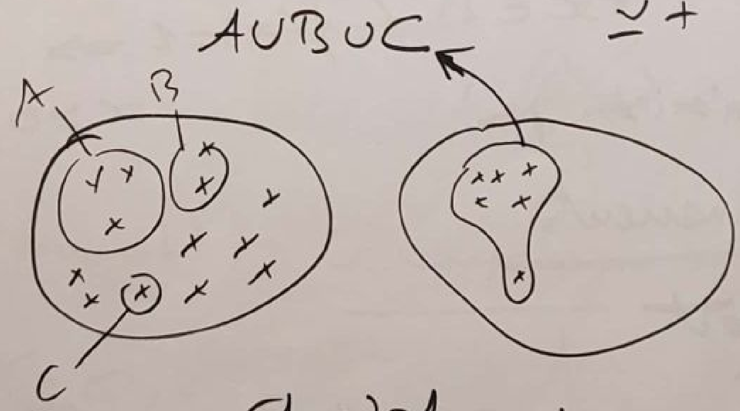
$3 - 2 - 1 = \underline{3 + (-2) + (-1)}$ convention *

- $3 \times 2 \times 5 = 30$

$(6 \div 2) \div 3 = 1$ $\qquad$ $6 \div (2 \div 3) = 6 \times (3 \times 1/2) = 9$

$2 \uparrow (2 \uparrow 3) = 2 \uparrow 8 = 256$ $\qquad$ $(2 \uparrow 2) \uparrow 3 = 4 \uparrow 3 = 64$





$$\begin{tikzcd}
E \arrow[r, "h"] \arrow[rr, bend right, "g\circ h"'] \arrow[rrr, bend left=50, "(f\circ g)\circ h"] \arrow[rrr, bend right=50, "f\circ(g\circ h)"'] & E \arrow[r, "g"] \arrow[rr, bend left, "f\circ g"] & E \arrow[r, "f"] & E
\end{tikzcd}$$

- C ou Abélienne

ssi $\forall (x,y)\in E^2,\ x*y=y*x$

$\cancel{+ \times \cap \cup}$

$+ - \times \div \uparrow \cap \cup \circ$

- N | $*$

$n\in E$

un elt N pour $*$ ds E ? | $*$ sens !

ssi $\forall x\in E,\ x*n=n*x=x$ — m̂ si c'est pas Commutatif

$+ - \times \div \uparrow \cap \cup \circ$

$0 \quad 1 \quad E \quad \emptyset \quad id_E$ — unic si m

- S on suppose qu'il existe un elt n

n m $*$

| $x\in E$ symétrique de x x' tq $x*x'=x'*x=n$

$+$ $-x$ opposé

$\times$ x^{-1} inverse

$\frac{a}{b}=a\times b^{-1}$ ou $b^{-1}\times a$

2 interprétations

Si $\times$ commutative noté $\frac{1}{x}$ ★

GROUPE

(G, LCI)

A

N il existe un elt N

S tt elt possède un S

$(\mathbb{Z},+)$ mais pas $(\mathbb{N},+)$ $(\mathbb{Q},+)$ $(\mathbb{R},+)$ $(\mathbb{C},+)$

$\cancel{(\mathbb{Q},\times)}$

0

(Commutatif) Groupe sym *

$\mathbb{K} = \mathbb{Q}, \mathbb{R}, \mathbb{C}$

$(\mathbb{K}^n,+)$ $(M_{n,p}(\mathbb{K}),+)$ $(\mathbb{K}[X],+)$

$(\mathbb{K}^*,\times)$ $(GL_n(\mathbb{K}),\times)$

mat inversible

$(\mathbb{Z}/n\mathbb{Z},+)$ $((\mathbb{Z}/n\mathbb{Z})^*,\times)$ $(S_n,\circ)$

cependant

2/6 Anneaux & Corps

- EX

D

A nul?

A_x de pol

elts inversibles

Corps

EXO $\mathbb{Q}(\sqrt{2})$

EQ 1er degré

A intègre

Corps fractions

- EX

Anneaux: "+" "×"

$\mathbb{Z}$ $\mathbb{R}[X]$ $\mathbb{Z}[i]$ $\mathbb{Z}/n\mathbb{Z}$ $M_n(\mathbb{C})$

$\mathcal{F}(E,A)$: f à val ds 1 anneau

$(f+g)(x) = f(x)+g(x)$

$(f\times g)(x) = f(x)\times g(x)$

Corps

tous les elts ont peut ÷ par eux
sauf 0

$\mathbb{Q}, \mathbb{R}, \mathbb{C}$

$\mathbb{R}(X)$
fractions rationnelles

$\mathbb{Z}/p\mathbb{Z}$ ex

D A $+ \times$ vérifiant

- $(A,+)$ GC dont elt N 0_A

- A $\forall a,b,c \in A,\ (a\times b)\times c = a\times(b\times c)$
→ ordre!
≠ Commutatif

- D $\times / +$ par rapport à
↑2

$(a+b)c = ac+bc$
ds cet ordre là (et)
$c(a+b) = ca+cb$

inverse n'est pas V

pas forcément C!

- il existe un elt N pr $\times$ 1_A
~~Sym~~

$\times$ C GC Anneau Commutatif ~~=~~ ~~abélien~~

+ ×
A A
N N
S ×
C ()

0_A 1_A

$x + 0_A = x$
~~$x \times 0 = x$~~
$x \times 1_A = x$

Et si jamais $0_A = 1_A$?

$\forall x \in A,\ x \times 1_A = x$
(et)
on sait que $x \times 0_A = 0_A$
le prouver

Lorsqu'il ≠ 2 elts au moins ⇒ 1 Anneau

vieilles habitudes

Car $x \times (0_A + 0_A) = x \times 0_A + x \times 0_A = x \times 0_A$

$A = \{0_A\}$ c'est l'anneau nul

Et si $A = \{0_A, 1_A\}$ c'est un anneau?

$0_A \times 0_A = \quad 1_A \times 1_A = 1_A \quad 1_A \times 0_A = 0_A =$
$0_A \times 1_A = 0_A$

$0_A + 0_A = 0_A \quad 1_A + 0_A = 1_A \quad 1_A + 1_A = ?$

$1_A + 1_A = 1_A \Rightarrow 1_A = 0_A$

Donc $1_A + 1_A = 0_A$ et $A = \mathbb{Z}/2\mathbb{Z}$

$\mathbb{R}[X] \to \mathbb{C}$

$\to 0_{\mathbb{R}[X]} = 0 + 0X + 0X^2 + \cdots$

$\to 1_{\mathbb{R}[X]} = \underline{\underline{1 + 0X + 0X^2 + \cdots}}$

+ gen ⊤ Subtil

| A Commutatif

$A[X] = \{ a_0 + a_1 X + a_2 X + \cdots$ où $(a_n)_{n\in\mathbb{N}} \in A^{(\mathbb{N})} \}$

sur un AC suite presque nulle

Ainsi de suite

$A[X, Y] = A[X][Y]$
est l'anneau des pol de 2 var
$A[X_1, X_2, \ldots, X_n)$ des pol de n var

$P = \sum_{i=0}^{n} p_i X^i$

$Q = \sum_{j=0}^{n} q_j X^j$

$R = \sum_{l=0}^{n} r_l X^l$

$PQ = \sum_{k=0}^{2n} a_k X^k \quad a_k = \sum_{\substack{i\geq 0,\, j\geq 0 \\ i+j=k}} p_i q_j$

$(PQ)R = \sum_{k=0}^{3n} b_k X^k$ avec $b_k = \sum_{\substack{i\geq 0,\, j\geq 0,\, l\geq 0 \\ i+j+l=k}} p_i q_j r_l$

$(PQ)R = P(QR)$

X^n pol sur A

| $(A, +, \times)$
elts inversibles pour 2ème loi

Un elt a de A est dit <u>inversible</u> ssi
il existe un elt b de A tq $a\times b = b\times a = 1_A$
b est l'inverse de a
Ens elts inversibles de $A = \underline{A^{\times}}$ DefG

Ex

$\mathbb{Z}^{\times} = \{-1, +1\} \quad \mathbb{Q}^{\times} = \mathbb{Q}^{*} = \mathbb{Q}\setminus\{0\}$

$\mathbb{R}[X]^{\times} = \{$ pol constants non nuls "

$M_n(\mathbb{C})^{\times} = GL_n(\mathbb{C}) \quad (\mathbb{Z}/n\mathbb{Z})^{\times} = \{ \dot{k} \mid \mathrm{pgcd}(k, n) = 1\}$

Un anneau A est un corps lorsque tous ses ~~elt~~ éléments non nuls sont inversibles

c'est lorsque $\boxed{A^\times = A \setminus \{0\}}$

$\mathbb{Q}$ $\mathbb{R}$ $\mathbb{C}$ $\quad \mathbb{Z}/p\mathbb{Z}$ $\quad \mathbb{R}(X)$

premier

Si $a \in A^\times$, son inverse ~~est~~ est noté a^{-1}

Si A est C, on peut remplacer a^{-1} par $\frac{1}{a}$

$\frac{b}{a} = \begin{cases} ba^{-1} \\ a^{-1}b \end{cases}$? ~~égal~~

~~ex~~

EXO M que $\mathbb{Q}(\sqrt{2}) = \{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\}$ est un Corps

Comme $\mathbb{Q}(\sqrt{2}) \subset \mathbb{R}$, nous savons que :

- $+$ et $\times$ A et C
- $\times$ D / $+$

Or ~~€~~ 1 sont ds $\mathbb{Q}(\sqrt{2})$

stable par $+$ et $\times$

reste M   opposé

$x = a + b\sqrt{2}$ et $y = c + d\sqrt{2}$ ds $\mathbb{Q}(\sqrt{2})$

on a $x - y = (a-c) + (b-d)\sqrt{2} \in \mathbb{Q}(\sqrt{2})$

Dc $(\mathbb{Q}(\sqrt{2}), +)$ GC

$x \times y = (ac ~~\ldots~~ + 2bd) + (bc + ad)\sqrt{2} \in \mathbb{Q}(\sqrt{2})$

Donc $(\mathbb{Q}(\sqrt{2}), +, \times)$ est un AC

reste à M que pr ~~tt~~ tt $x = a + b\sqrt{2}$ ds $\mathbb{Q}(\sqrt{2})$

on a : $x \neq 0 \Rightarrow 1/x \in \mathbb{Q}(\sqrt{2})$

$$\frac{1}{a + b\sqrt{2}} = \frac{a - b\sqrt{2}}{(a + b\sqrt{2})(a - b\sqrt{2})}$$ × expr conjuguée

$$= \frac{a - b\sqrt{2}}{a^2 - 2b^2} \quad ? \overset{?}{=} 0$$ ($\sqrt{2}$ serait une fraction)

$$= \frac{a}{a^2 - 2b^2} - \frac{b}{a^2 - 2b^2}\sqrt{2} \in \mathbb{Q}(\sqrt{2})$$

piège

1 $(A,+,\times)$

Pr $a,b \in A$, Considérons l'Eq

$ax = b$

Si $\in A^\times$, $x = a^{-1}b$ est l'unique sol

~~et~~ et sinon, il n'y a pas de sols ?

Des fois non

Ds $\mathbb{Z}$ $3x=5$ n'admet pas de sol

mais $3x=6$ admet ~~...~~ comme sol $x=2$

Ah oui ! si $b = ac$, $ax = ac \Rightarrow x = c$!

plus compliqué que ça

Ds $\mathbb{Z}/10\mathbb{Z}$ $\dot{4}\dot{x} = \dot{8}$

admet comme sol $x = \dot{2}$ et $x = \dot{7}$

~~crypto~~ crypto

- quels sont les A_s $(A,+,\times)$ vérifiant $\forall (a,b,c) \in A$,

$ab = ac \Rightarrow b = c$?

$\forall a \in A \setminus \{0_A\}$, $\forall b, c \in A$

$ab = ac \Rightarrow b = c$?

Cond Suf A est inclus ds un corps.

CN :

$\forall a \in A \setminus \{0_A\}$

$\forall b \in A$,

$ab = 0_A \Rightarrow b = 0_A$

Un A sans diviseurs de zéros ssi

$\forall a,b \in A$, $a \times b = 0_A \Rightarrow (a = 0_A$ ou $b = 0_A)$

Si de plus, A est C, on dit que A est intègre

$\mathbb{Z}$ $\mathbb{R}[X]$ $\mathbb{Z}[i]$ sont int

$M_n(\mathbb{C})$ et $\mathbb{Z}/n\mathbb{Z}$ ~~int~~

n non premier

$$\begin{pmatrix} -2 & 3 \\ -4 & 6 \end{pmatrix}\begin{pmatrix} 3 & -3 \\ 2 & -2 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$$

- Corps des fractions

$|(A, +, \times)$ intègre

il existe un corps $\subset \mathbb{K}$ dont un sous Anneau est isomorphe à A

de A Frac(A)

$$\mathbb{Z} \simeq \left\{ \frac{n}{1}, n \in \mathbb{Z} \right\} \subset \mathbb{Q}$$

$$\mathbb{R}[X] \simeq \left\{ \frac{P}{1}, P \in \mathbb{R}[X] \right\} \subset \mathbb{R}(X)$$

habituel → bizarre

corps comm — anneaux intègres — anneaux avec diviseurs de zero et/ou non commutatifs

~~NB je saute pour l'ins~~

NB je saute pour l'instant "le corps des fractions ! d'un anneau intègre"

3/5 Morphismes &

iso

SOM

f^s 1 opera^{ns}

mor de G

A_x

isom

m i

Noyau d'un m

Fonctions 1 operations

$E \xrightarrow{f} F$

$(\mathbb{R},+) \xrightarrow{f} (\mathbb{R},+)$

$\forall x,y \in \mathbb{R}, f(x+y) = f(x)+f(y)$

f est compatible avec o^{ns} +

$f(x) = 3x$

$(\mathbb{R},+) \xrightarrow{f} (\mathbb{R}^*,\times)$

$\forall x,y \in \mathbb{R}, f(x+y) = f(x)\times f(y)$

$f(x) = e^{2x}$

Morphisme de Groupe

$(G,*)$ $(H,\circledast)$

f $E \longrightarrow H$

est un / entre G et H

ssi $\forall (x,y) \in G, \boxed{f(x*y) = f(x) \circledast f(y)}$

$\circledast$
"+ et x"

• $(\mathbb{Z},+) \longrightarrow (\mathbb{C}^*,\times)$

$n \longrightarrow e^{in}$

• $(\mathbb{R}[X],+) \longrightarrow (\mathbb{R},+)$

$P \longrightarrow P(0)$

• $(GL_n(\mathbb{R}),\times) \longrightarrow (\mathbb{R}^*,\times)$

$M \longrightarrow \det(M)$

• f morph entre $(G,*)$ et $(H,\circledast)$

n_G n_H

on a $\boxed{f(n_G) = n_H}$

1 et 1

$e^0 = 1$ $\det I_n = 1$

Preuve

$\forall g \in G,\ f(g) = f(g * n_G)$
$\qquad = f(g) * f(n_G)$

On as H, il existe un elt h ~~*~~
tq $h * f(g) = n_H$
on en deduit $n_H = n_H * f(n_G)$ or
donc $f(n_G) * = n_H$

PÉ

f morph entre $(G,*)$ et $(H,*)$

$\forall g \in G,\ (f(g))^{-1} = f(g^{-1})$ | -1 inverse | inversi !

l'inverse de l'im c'est l'im de l'inv

$e^{-x} = 1/e^x \qquad \det A^{-1} = 1/\det A$

Preuve

$\forall g \in G,\ f(g) * f(g^{-1}) = f(g * g^{-1})$
$\qquad = f(n_G)$
$\qquad = n_H$

Dc $f(g^{-1})$ est le sym de $f(g)$ ds H

M d'Anneaux

$(A,+,\times)\ (B,+,\times)$

$f : A \longrightarrow B$

ssi

$\forall x,y \in G\ \ f(x+y) = f(x) + f(y)$

× ×

$f(1_A) = 1_B$

min mor G

$\mathbb{Z} \longrightarrow \mathbb{Z}$

$f(1) = 1,\ f(2) = f(1+1)$
$\qquad = f(1) + f(1)$
$\qquad = 2$

$f(n) = f(n-1+1) = n-1+1 = n$
$f(-n+n) = f(-n) + f(n) = 0,\ f(-n) = n$
$f = id$ seul m de $\mathbb{Z}$

. $\mathbb{R}[X] \longrightarrow \mathbb{R}$

$P \longrightarrow P(0)$

. $\mathbb{Z} \longrightarrow \mathbb{Z}/n\mathbb{Z}$

$a \longrightarrow \dot{a}$

Si $(A,+,\times)$ et ~~B~~ $(B,+,\times)$ 2 Corps,

Si f est un morph d'un anneau de A ds B

on dit que f est un morph de Corps entre A et B

<u>iso M</u>

Si $f : E \to F$ est un morph b, Alors

$f^{-1} : F \to E$ est un morph

$\forall x, y \in F, \exists a, b \in E, x = f(a)$ et $y = f(b)$

$$f^{-1}(x * y) = f^{-1}(f(a) * f(b))$$
$$= f^{-1}(f(a * b))$$
$$= a * b = f^{-1}(x) * f^{-1}(y)$$

Si : $E \to F$ morph bij entre

2 G_s ou 2 A_x

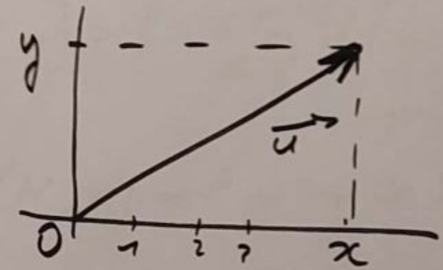
on dit que f est un isom de

G_s d'A_x

E et F sont isomorphes, $E \simeq F$ | "les même"

$\mathbb{R}^2 \longrightarrow P$

$(x, y) \longrightarrow \vec{u}$



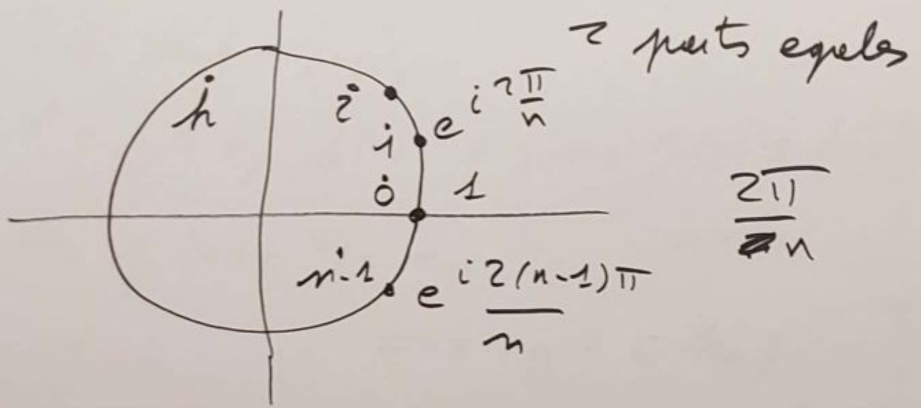
$(\{-1, 1\}, \times) \longrightarrow (\mathbb{Z}/2\mathbb{Z}, +)$

$1 \longrightarrow \dot{0}$

$-1 \longrightarrow \dot{1}$

17:01

~~17:00~~



rac nièmes unité

G cyclique × Y est +

$(\Omega_n, \times) \simeq (\mathbb{Z}/n\mathbb{Z}, +)$

Mor i^{ls}

Si $f : E \to F$ est un m i
Al c'est un isom entre E et Im f

Cela permet de définir une "inclusion" de E ds F

$\mathbb{Z} \to \mathbb{Q}$
$n \to \frac{n}{1}$

$\mathbb{R} \to \mathbb{C}$
$x \to x + 0i$

$\mathbb{R} \to \mathbb{R}[X]$
$x \to x\ (+0X + 0X^2 + \dots)$

On dit $f : E \to F$ est un prolongement de E ds F

et que F est une extension de E

Noyau d'un morphisme

$f : (G, *) \to (H, \circledast)$ m de G

$\ker f = f^{-1}\{n_H\} = \{x \in G,\ f(x) = n_H\}$

T $f : (G, *) \to (H, \circledast)$ est un m de G

- ker f est un SG de G
- f est i $\Leftrightarrow \ker f = \{n_G\}$

utile ça?

Preuve

$n_G \in \ker f$ donc $\ker f \neq \emptyset$

$\forall x, y \in \ker f,\ x * y^{-1} \in \ker f$? à vérif

$\forall x, y \in \ker f,\ f(x * y^{-1}) = f(x) \circledast f(y)^{-1}$
$= n_H \circledast n_H^{-1} = n_H$

f est i $\Rightarrow \ker f = \{n_G\}$

Sur $\ker f = \{n_G\}$

$\forall x, y \in G,\ f(x) = f(y) \Rightarrow f(x) * f(y)^{-1} = n_H$

$\Rightarrow f(x * y^{-1}) = n_H$

$\Rightarrow x * y^{-1} \in \ker f$

$\Rightarrow x * y^{-1} = n_G$

$\Rightarrow x = y$

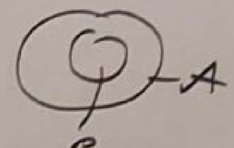
4/5 IDEAUX

Sous A
Noyau 1 m A
D 1 ideal
Ideaux d'un Cnps
Ideal princ 1 Ann princ
Ideaux type fini
Generateurs d'un ideal
Autre ideaux
opera° sur —
Divisibilité
PGCD PPCM

ideaux premiers
Parenthèse
(premier ou maximal)
Ideaux maximaux
$\mathbb{Z}$ est principal

$|$ $(A, +, \times)$ un anneau $P \subset A$
ev

Sous A de A ssi



- $\forall x, y \in P,\ x - y \in P$ $\sim G$
- ______ $x \times y \in P$ stables
- 1_A ~~I_A~~ $\in P$

Le seule SA de $\mathbb{Z}$, c'est $\mathbb{Z}$

Si $f : A \to B$ m d'A

$\ker f = \{a \in A,\ f(a) = 0_B\}$

Or, $f(1_A) = 1_B$

dc $\ker f$ n'est pas un SA

- Si $f : A \to B$ est m d'A
  $\ker f$ est un SG de $(A,+)$ qui ne contient pas I_A

$A_2(\mathbb{R}) = \left\{ \begin{pmatrix} 0 & -a \\ a & 0 \end{pmatrix}, a \in \mathbb{R} \right\}$, SG de $M_2(\mathbb{R})$

$\begin{pmatrix}0 & -a\\ a & 0\end{pmatrix}\times\begin{pmatrix}0 & -b\\ b & 0\end{pmatrix}=\begin{pmatrix}-ab & 0\\ 0 & -ab\end{pmatrix}\notin A_2(\mathbb{R})$

Si $x, y\in \ker f$ alors ~~$f(x)$~~

$$f(xy)=f(x)f(y)$$
Noyau d'un ↗
$$= 0_B\times 0_B = 0_B$$

Si $x\in\ker f$ Alors

$\forall a\in A$, $f(xa)=f(x)f(a)=0_B$

et $f(ax)=f(a)f(x)=0_B$

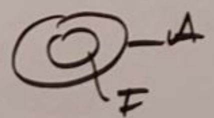
Si $x\in\ker f$ Al $\forall a\in A$, $xa\in\ker f$

et $ax\in\ker f$ $\rfloor$

Idéal

$(A,+,\times)$

idéal I de A



- I SG de $(A,+)$
- $\forall x\in I, \forall a\in A$, $ax\in I$ et $xa\in I$ $\rfloor$

$>$ que SA

$\{0_A\}$ est un I de A

Si I est un I de $\mathbb{Z}$, Al $\exists n\in\mathbb{N}^*$,

$I=n\mathbb{Z}$

pas d'autre!

Si A est Cm, pr $\forall x$ de A

$xA=\{xa, a\in A\}$ est un I de A

$0_A = x0_A\in xA$

idéal à G / D / bilatère

je saute

Idéaux d'un Cps

$(A,+,\times)$ Cm, I idéal de A

Si I contient un elt inversible de A, Alors $I=A$ $\rfloor$

A est un C $\Leftrightarrow$ les seuls idéaux de A sont $\{0_A\}$ et A

Idéal principal et
Anneau ___

$(A,+,\times)$ C

I de A est dit principal
Si il existe x de A tq $I = xA$
$\langle x \rangle$ (x)

$(A,+,\times)$
Si ts idéaux de A sont principaux
= A est un anneau principal

$\mathbb{Z}$ est principal

Idéaux de type fini

"CL"

Générateurs d'un idéal

Autres idéaux

∩ sm idéaux

~~Divi~~ Divisibilités

PGCD PPCM

Idéaux premiers

Parenthèse (premier ou irréductible ?

Idéaux maximaux

$\mathbb{Z}$ est principal

5/5 ANNEAUX QUOTIENTS

Voc
Gen~ de $\mathbb{Z}/n\mathbb{Z}$
RE?
CE
Ann quot def
EX
π
quot par idéal premier
maximal

Preuve qu'un idéal maximal est premier

T iso n app