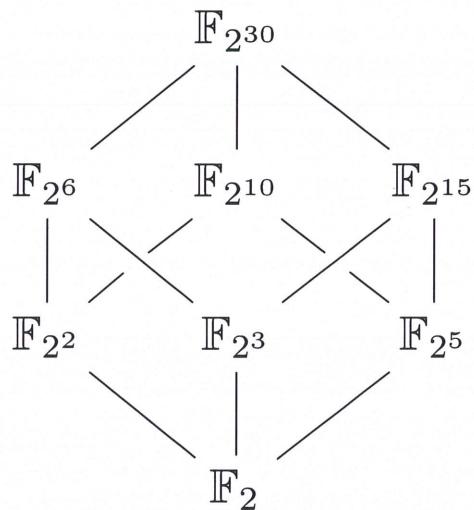


Chapitre 11

Anneaux et corps



Petits corps en treillis.

Les anneaux et les corps, structures algébriques fondamentales, formalisent la notion de nombre et d'opération.

*L'anneau par excellence est \mathbb{Z} .
Le corps par excellence est \mathbb{R} .*



Annexe 7

Bcp + gen^{dl}: Si R anneau, $M_n(R)$ anneau

Ex: $M_2(M_2(\mathbb{Z}))$ est un anneau

(AC)

(1) $M_2(M_2(\mathbb{Z}))$

Soit $A := \begin{pmatrix} (10) & (01) \\ (01) & (10) \\ (11) & (11) \\ (00) & (00) \end{pmatrix}$

Calculons A^2

$$A^2 = \begin{pmatrix} (10) & (01) \\ (11) & (11) \end{pmatrix} \begin{pmatrix} (10) & (01) \\ (01) & (10) \end{pmatrix}$$

$$\begin{pmatrix} (10) & (01) \\ (01) & (10) \\ (11) & (11) \\ (00) & (00) \end{pmatrix} \begin{pmatrix} (10) & (01) \\ (01) & (10) \end{pmatrix} = \begin{pmatrix} (22) & (23) \\ (00) & (01) \end{pmatrix}$$

On a : $\begin{pmatrix} ab \\ cd \end{pmatrix} \begin{pmatrix} 01 \\ 10 \end{pmatrix} = \begin{pmatrix} b \\ d \end{pmatrix} \begin{pmatrix} a \\ c \end{pmatrix}$

(2) Newton particulisé

Soit R un anneau

Soit $x \in R$, on a $x \cdot \gamma = \gamma \cdot x$

i.e. x et γ commutent

Donc $(x + \gamma)^n = \sum_{k=0}^n \binom{n}{k} x^k$

(3) Exemples de sous-anneaux

• L'anneau nul est-il un sous-anneau de $(\mathbb{Z}, +, 0, 1)$?

Notons N l'anneau nul $\{0\}$

Alors, on a $0_N = 1_N$

C'est $1_{\mathbb{Z}} \neq 1_N$, on a $\forall z \in N$ donc : Non

Très joli !

$\mathcal{C}(R, R)$ sous anneau $\mathcal{T}(R, R)$

D/ • Deja $\tilde{0}$ est \mathcal{C}^0

• si f et g \mathcal{C}^0 , alors $f+g$ est \mathcal{C}^0

• Ainsi $\mathcal{C}(R, R)$ sous-groupe de $(\mathcal{T}(R, R), +, \tilde{0})$

De plus si f et g sont \mathcal{C}^0 , fg est \mathcal{C}^0

enfin $\tilde{1}$ est \mathcal{C}^0

$\mathcal{E}^\infty(R, R)$ sous anneau de $\mathcal{C}(R, R)$

$\mathcal{D}(R, R)$ sous anneau de $\mathcal{E}(R, R)$

De plus, $\mathcal{E}^k(R, R)$, $\mathcal{D}^k(I, R)$

On note $\mathbb{Q}[\sqrt{2}] := \{a + b\sqrt{2}; (a, b) \in \mathbb{Q}^2\}$
et $\mathbb{Z}[\sqrt{2}] := \{a + b\sqrt{2}; (a, b) \in \mathbb{Z}^2\}$

$$\text{Ex: } 1 + \sqrt{2} \in \mathbb{Z}[\sqrt{2}]$$

$$\frac{1 - \sqrt{2}}{2} \in \mathbb{Q}[\sqrt{2}]$$

On a : $\mathbb{Z}[\sqrt{2}]$ est le \oplus petit sous-anneau
de \mathbb{R} contenant \mathbb{Z} et $\sqrt{2}$

Fait : $\mathbb{Z}[\sqrt{2}]$ sous-anneau de \mathbb{R}

D/ Deja $\mathbb{Z}[\sqrt{2}] \subset \mathbb{R}$

06 $\mathbb{Z}[\sqrt{2}]$ car $0 = 0 + 0\sqrt{2}$

Sont $a, b \in \mathbb{Z}$ $-(a + b\sqrt{2}) = -a - b\sqrt{2} \in \mathbb{Z}[\sqrt{2}]$

$\mathbb{Z}[\sqrt{2}]$

si $a', b' \in \mathbb{Z}$, alors

$$(a + b\sqrt{2}) + (a' + b'\sqrt{2}) = (a + a') + (b + b')\sqrt{2}$$

$$\begin{aligned} \text{enfin } & (a + b\sqrt{2})(a' + b'\sqrt{2}) \\ &= (aa' + 2bb') + (ab' + b'a)\sqrt{2} \end{aligned}$$

$$\text{et } 1 = 1 + 0\sqrt{2} \in \mathbb{Z}[\sqrt{2}]$$

De m⁺ $\mathbb{Q}[\sqrt{2}]$ ss-anneau de \mathbb{R}

De m⁺ $\mathbb{Z}[\sqrt{2}]$ ss-anneau de \mathbb{C}

Notons

$$T_n^+(\mathbb{R}) := \left\{ \begin{pmatrix} * & * & * \\ 0 & * & * \\ 0 & 0 & * \end{pmatrix} \right\}$$

C'est l'ensemble des matrices triangulaires supérieures

Ex :

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 0 & 5 & 6 & 7 \\ 0 & 0 & 8 & 9 \\ 0 & 0 & 0 & 10 \end{pmatrix} \in T_4^+(\mathbb{R})$$

On a : $\bullet M, N \in T_n^+(\mathbb{R}) \Rightarrow M+N \in T_n^+(\mathbb{R})$

$\bullet M \in T_n^+(\mathbb{R}) \Rightarrow -M \in T_n^+(\mathbb{R})$

$\bullet O_n \in T_n^+(\mathbb{R})$

$\bullet I_n \in T_n^+(\mathbb{R})$

$\bullet M, N \in T_n^+(\mathbb{R}) \Rightarrow M \times N \in T_n^+(\mathbb{R})$

(AF) : $\begin{pmatrix} 1 & 2 & 3 \\ 0 & 2 & 4 \\ 0 & 0 & 3 \end{pmatrix} \times \begin{pmatrix} 1 & 0 & 5 \\ 0 & 1 & 0 \\ 0 & 0 & -1 \end{pmatrix}$

Ainsi, $T_n^+(\mathbb{R})$ sous-anneau de $M_n(\mathbb{R})$

(b) Exemples de morphismes

On considère $\bar{ev}_0 : \mathcal{F}(\mathbb{R}, \mathbb{R}) \rightarrow \mathbb{R}$

$$f \mapsto f(0)$$

On a $\begin{cases} \bar{ev}_0(f+g) = \bar{ev}_0(f) + \bar{ev}_0(g) \\ \bar{ev}_0(fg) = \bar{ev}_0(f)\bar{ev}_0(g) \\ \bar{ev}_0(1) = 1 \end{cases}$

On a $\overline{z+z'} = \overline{z} + \overline{z'}$

et $\overline{zz'} = \overline{z} \cdot \overline{z'}$

$\overline{1} = 1$

$$\begin{aligned} D^{\oplus}(\psi \circ \varphi)(x+y) &= \psi(\varphi(x+y)) = \psi(\varphi(x) \underset{T}{\oplus} \varphi(y)) \\ &= \psi(\varphi(x)) \underset{T}{\oplus} \psi(\varphi(y)) = \psi \circ \varphi(x) \underset{T}{\oplus} \psi \circ \varphi(y) \end{aligned}$$

De même $(\psi \circ \varphi)(xy) = (\psi \circ \varphi(x)) \cdot (\psi \circ \varphi(y))$

$$(\psi \circ \varphi)(1_R) = \psi(\varphi(1_R)) = \psi(\gamma_s) = 1_T$$

⑤ La conjugaison complexe

Notons $c: \mathbb{C} \rightarrow \mathbb{C}$
 $z \mapsto \bar{z}$

- Déjà', $c \in \text{Hom}_{(\text{Ann})}(\mathbb{C}, \mathbb{C})$

- $I_e \subset \text{End}_{(\text{Ann})}(\mathbb{C})$

- Ensuite : c est bijectif. En effet : $c \circ c = I_{\mathbb{C}}$
 donc c est bij et $c^{-1} = c$

- CC1 : $c \in \text{Aut}_{(\text{Ann})}(\mathbb{C})$

$$\ker \varphi = \{z \in \mathbb{R} \mid \varphi(z) = 0_s\}$$

⑥ Exemples d'anneaux intègres

- $\mathbb{R}, \mathbb{Z}, \mathbb{C}, \mathbb{Q}, \mathbb{Z}_1, \mathbb{Z}[\Sigma], \mathbb{Q}[\Sigma]$, ...
 sont tous intègres

Ex : $\begin{pmatrix} 0 & 2 \\ 0 & -8 \end{pmatrix} \cdot \begin{pmatrix} 4 & 1 \\ 0 & 0 \end{pmatrix} = 0_2$

5.5 Rq: si $f: G \rightarrow H$ est un iso, on note

$$G \xrightarrow[f]{\sim} H$$

On considère d'un côté $(\mathbb{Z}, +, 0)$ et on définit un ensemble $\widetilde{\mathbb{Z}} :=$

$$\left\{ \dots, \overline{-3}, \overline{-2}, \overline{-1}, \overline{0}, \overline{1}, \overline{2}, \overline{3}, \dots \right\}$$

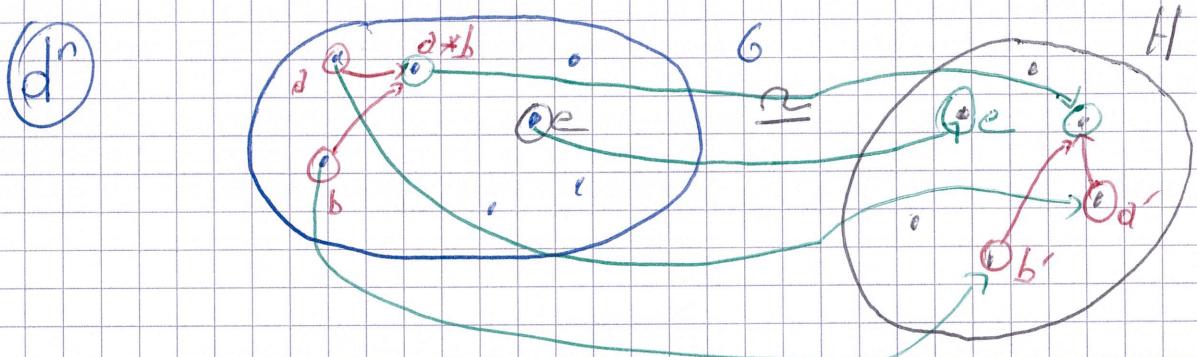
où \overline{m} est l'entier m avec un tilde au dessus.

On munit $\widetilde{\mathbb{Z}}$ d'une loi $\widetilde{+}$ définie par

$$\overline{n} \widetilde{+} \overline{m} = \overline{n+m}$$

Ex: $\overline{8} \widetilde{+} \overline{3} = \overline{11}$

Alors $(\mathbb{Z}, +, 0) \cong (\widetilde{\mathbb{Z}}, \widetilde{+}, \widetilde{0})$



Exemple surprenant

$$(\mathbb{R}_+^*, \times) \cong (\mathbb{R}, +)$$

D/T: $\ln: \mathbb{R}_+^* \rightarrow \mathbb{R}$ est un iso de groupes

En effet: $\ln(\cdot)$ est bijective ($\ln: \mathbb{C}^\times, \mathbb{R}^*$ et

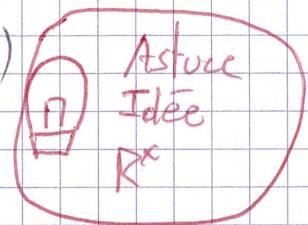
$\ln(x) \rightarrow -\infty$ $x \rightarrow 0^+$ $\ln(x) \rightarrow +\infty$ $x \rightarrow +\infty$

(7)

$$3) \text{ On a } \overline{0} + z = \overline{0} + \overline{a} = \overline{0+a} = \overline{a} = z$$

$$\text{et de m } z + \overline{0} = z$$

b)



$$\text{Posons } z' := \overline{-a}$$

$$\text{On a } z - z' = \overline{0} + \overline{-a} = \overline{0-a} = \overline{a} = z$$

$$\text{et de m } z - z' = \overline{0} \blacksquare$$

Ex : Dans $\mathbb{Z}/3\mathbb{Z}$, on a 3 éléments

$$\text{"}\{3k\}\text{"} = \overline{0} = \{\dots, -3, 0, 3, 6, \dots\}$$

$$\text{"}\{3k+1\}\text{"} = \overline{1} = \{\dots, -3+1, 1, 3+1, 6+1, \dots\}$$

$$\text{"}\{3k+2\}\text{"} = \overline{2} = \{\dots, -3+2, 2, 3+2, \dots\}$$

$$\text{On a } \mathbb{Z}/3\mathbb{Z} = \{\overline{0}, \overline{1}, \overline{2}\}$$

Calculons

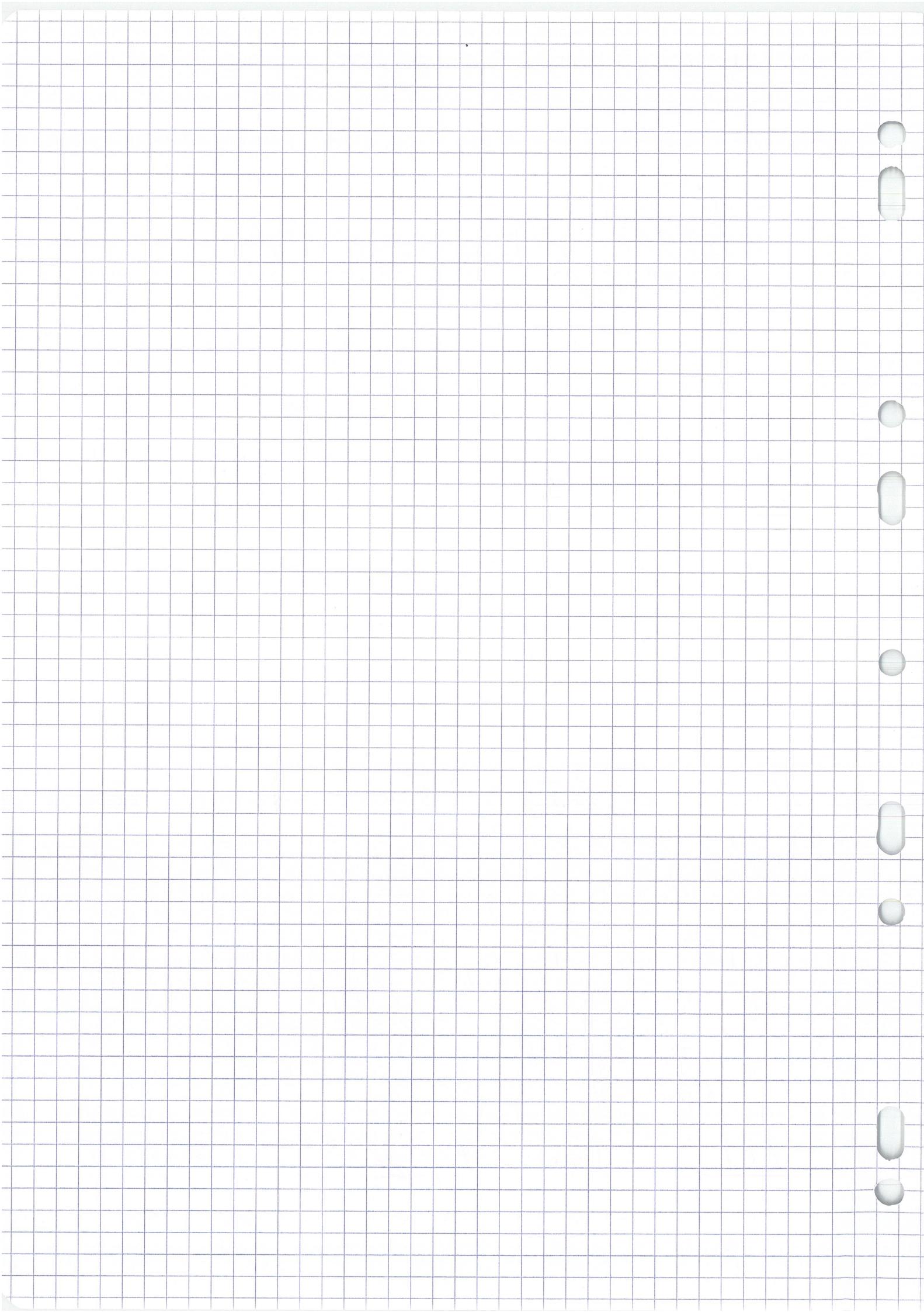
$$\overline{1} + \overline{2} = \{1, 4, 7, \dots\} + \{2, 5, 7, \dots\}$$

$$= \overline{3} = \overline{0}$$

par déf°

R* prosopagnosique

CCL : Dans $\mathbb{Z}/3\mathbb{Z}$, on a $\overline{1} + \overline{2} = \overline{0}$



(8)

(E)

Osq n premier mq $\mathbb{Z}/n\mathbb{Z}$ corpsIe, mq $\forall k \in [1, n-1]$, \bar{k} inversible dans $\mathbb{Z}/n\mathbb{Z}$ (B°) \bar{k} inversible ($\Leftrightarrow \bar{k} \cdot \bar{P} = \bar{1}$)

$$\Leftrightarrow kP \equiv 1 \pmod{n}$$

$$kp - 1 \equiv dn$$

$$kp + dn = 1$$

Cⁿ n est premier et $\exists k \in [1, n-1]$, ond

$$\text{pgcd}(n, k) = 1$$

Fixons donc $P, d \in \mathbb{Z}$ tq $kP + dn = 1$ Donc $Pk \equiv 1 \pmod{n}$ i.e. $\bar{k} \cdot \bar{P} = \bar{1}$ Donc $\bar{k} \in U(\mathbb{Z}/n\mathbb{Z})$

ex : Resolvons l'équation $n^3 - hn = 77$ dans \mathbb{Z}
 (éq^o diophantienne)

Fixons une solution $n_0 \in \mathbb{Z}$, ond alors

$$n_0^3 - hn_0 = 77 \quad (*)$$

Reduisons modulo 3 (*): on obtient

$$\bar{n_0}^3 - \bar{h} \cdot \bar{n_0} = \bar{77} \quad \text{dans } \mathbb{Z}/3\mathbb{Z}$$

$$\text{i.e. } \bar{n_0}^3 - \bar{n_0} = \bar{2}$$

$$\text{or } \bar{0}^3 - \bar{0} = \bar{0} \neq \bar{2}$$

$$\frac{\bar{1}^3 - \bar{1}}{\bar{1} - \bar{1}} = \bar{0} \neq \bar{2}$$

$$\frac{\bar{2}^3 - \bar{2}}{\bar{2} - \bar{1}} = \frac{\bar{8} - \bar{2}}{\bar{-1} - \bar{1}} = \bar{6} - \bar{2} = \bar{4} \neq \bar{2}$$

CC1: $\{n \in \mathbb{Z} \mid n^3 - 5n = 77\} = \emptyset$ \blacksquare

Complément de Djemaïl

Soit G un groupe ; soit $g \in G$

• RDC : soit $x \in G$.

On dispose de $gxg^{-1} \in G$

C'est le conjugué de x par g

notation : $\text{conj}(x)$ ou $\text{conj}_g^{[G]}(x)$

• 1^{er} étage

On dispose $\text{conj}_g : G \rightarrow G$
 $x \mapsto gxg^{-1}$

On a $\text{conj}_g \in \text{Tr}(G, G)$

Fait : • $\text{Conj}_g(\cdot)$ est un morphisme

• Ie : $\text{Conj}_g \in \text{End}_{(G_{\text{gp}})}(G)$

2^e étage :

On dispose donc de $\text{conj} : G \rightarrow \text{End}_{(G_{\text{gp}})}(G)$
 $g \mapsto \text{Conj}_g$

Fait : • Conj_g est bijectif

• Ie : $\text{Conj}_g \in \text{Aut}_{(G_{\text{gp}})}(G)$

2^e étage rénové : On sait que $\text{Aut}_{(G_{\text{gp}})}(G)$ est un groupe ?

1) La composée de 2 autos est une auto

2) L'inverse d'un auto est un auto

3) Id_G auto

⊕ précisément $(\text{aut}_{(\text{corp})}(G), \circ, \text{Id}_G)$

Prop.: $\text{conj}^{[G]}: G \rightarrow \text{Aut}(G)$ est un morphisme

Ie: $\text{conj}^{[G]} \in \text{Hom}_{(G_{\text{grp}})}(G, \text{Aut}_{(\text{corp})}(G))$

(exo) Soit \mathbb{R} ($R, +, \times, 0, 1$) un anneau

Mq $(R, \times, 1)$ n'est pas un groupe !!!
(sauf si R est l'anneau nul)

Rq : Dans un anneau R , je peux faire

$$x^2(1-y) + 5xy^2 + 7zy \in$$

$\underbrace{1+1+\dots+1}_{5\text{ fois}}$

Rq !:

$$(\overline{\mathbb{P}}(\mathbb{R}, R), +, \circ, \tilde{o}, \text{Id}_R)$$

n'est pas un anneau

On a $(\overline{\mathbb{P}}(\mathbb{R}, \mathbb{R}), +, \tilde{o})$ est un groupe commutatif

et $(\overline{\mathbb{P}}(\mathbb{R}, \mathbb{R}), \circ, \text{Id}_{\mathbb{R}})$ est un monoïde

$$\text{On a } ((f+g) \circ h)(x) = (f+g)(h(x))$$

def \circ de \circ

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

Ccl : $(f+g) \circ h = f \circ h + g \circ h$

Mais $f \circ (g+h) \neq fog + foh$

contre exemple

$$f(x) = |x|$$

$$h(x) = x$$

$$g(x) = -x$$

ou encore $f = (\cdot)^2$; $g = \text{Id}_{\mathbb{R}}$; $h = \tilde{\gamma}$
 A-t-on \circledast ? $(x+1)^2 = x^2 + 1^2$ Non

ou $f = (\cdot)^2$; $g = h = \tilde{\gamma}$
Plus simple: $f = g = h = \tilde{\gamma}$

Trailler du chap 5^e: on va se restreindre à
 des fonctions telles que ça marche.

On définira une partie $\mathcal{F} \subset \mathcal{F}(\mathbb{R}, \mathbb{R})$ tq

1°) \mathcal{F} sgr $(\mathcal{F}(\mathbb{R}, \mathbb{R}), +, \circ)$

2°) \mathcal{F} stable par 0

3°) $\text{Id}_{\mathbb{R}} \in \mathcal{F}$

4°) $\forall f, g, h \in \mathcal{F}, f \circ (g+h) = f \circ g + f \circ h$

Exemples : anneaux intègres

• $(\mathcal{F}(\mathbb{R}, \mathbb{R}), +, \times, \circ, \tilde{\gamma})$ n'est pas intègre

D/ $1|_{\mathbb{R}_-} \times 1|_{\mathbb{R}_+^*} = \tilde{0}$ mais

$$\begin{cases} 1|_{\mathbb{R}_-} \neq \tilde{0} \\ 1|_{\mathbb{R}_+^*} \neq \tilde{0} \end{cases} \quad \text{d'après}$$

Bilan

- Plaçons-nous dans $(\mathbb{Z}/n\mathbb{Z}, +, \times, 0_{\mathbb{Z}/n\mathbb{Z}}, 1_{\mathbb{Z}/n\mathbb{Z}})$
- Notons pour simplifier $0 := 0_{\mathbb{Z}/n\mathbb{Z}}$; $1 := 1_{\mathbb{Z}/n\mathbb{Z}}$

On a $O = \{-3_n, -2_n, -n, 0_{\mathbb{Z}}, 1_n, 2_n, \dots\}$

$$1 = \{kn + 1_{\mathbb{Z}}; k \in \mathbb{Z}\}$$

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

- Rappel: Dans un anneau R , si $m \in \mathbb{Z}$, on a défini $m \cdot 1_R$; c'est $\underbrace{1_R + 1_R + \dots + 1_R}_{m \text{ fois}}$

On peut même le noter m tout court

- On a, si $m \in \mathbb{N}$:

$$\overline{m} = \underbrace{\overline{1} + \overline{1} + \dots + \overline{1}}_{m \text{ fois}}$$

$$= m \cdot \overline{1} = m \cdot 1_{\mathbb{Z}/n\mathbb{Z}} = m$$

- On sait que $\overline{0} = \overline{n}$

- Dans $\mathbb{Z}/n\mathbb{Z}$, on a $\overline{0} = \overline{n}$

- Ex: Dans $\mathbb{Z}/3\mathbb{Z}$, on a $\overline{1} + \overline{1} + \overline{1} = \overline{0}$

donc $\overline{1} + \overline{1} = \overline{-1}$ i.e. $2 = -1$

$2 \times 2 = 1$

Ex :

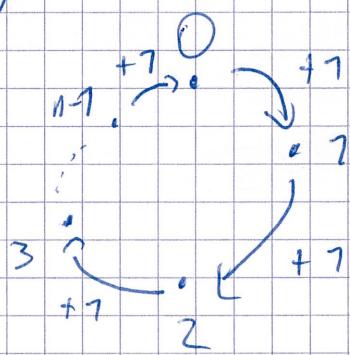
$\mathbb{Z}/n\mathbb{Z}$ n'est pas intègre

D/ Dans $\mathbb{Z}/n\mathbb{Z}$, $2 \times 2 = 0$ mais $2 \neq 0$

(exo) : Montrer que $(\mathbb{Z}/n\mathbb{Z}, +, \bar{0})$ est cyclique

(exo) $M_q (\mathbb{Z}/n\mathbb{Z}, +, \bar{0}) \cong (U_n, \times, 1)$

(dⁿ)



Rq : $\mathbb{Z}/n\mathbb{Z} \cong_{(ann)} \mathbb{F}_2$

(n>2)

Thm : $\mathbb{Z}/n\mathbb{Z}$ corps $\Leftrightarrow n$ premier

D/ \Rightarrow par contraposition

Ie montrer que si n pas premier $\Rightarrow \mathbb{Z}/n\mathbb{Z}$ pas un corps

On écrit $n = a \times b$ avec $a, b \in \mathbb{Z}$
comme $a \in [2, n-1]$, on

$$a \neq \bar{0}$$

De même, $\bar{b} \neq \bar{0}$

$$\text{Mais } \bar{a} \cdot \bar{b} = \overline{a \times b} = \overline{n} = \bar{0}$$

Donc $\mathbb{Z}/n\mathbb{Z}$ n'est pas intègre et n'est donc pas un corps.

S: R, S anneaux, $\hat{\epsilon}$ pour les groupes,
je peux munir $R \times S$ d'une structure
d'anneau

Ex: \mathbb{Z}^2 est non intègre

$$\underline{D/} \quad (1,0) \times (0,1) = (1 \times 0, 0 \times 1) \\ = (0,0) = O_{\mathbb{Z}^2}$$

et $(1,0) \neq O_{\mathbb{Z}^2}$

et $(0,1) \neq O_{\mathbb{Z}^2}$

Rq * $\frac{3}{2}$: $\mathbb{Z}^2 \cong \mathcal{T}_R(\{0,1\}, R)$ AC

b) Simplifiabilité dans un anneau intègre

Prop \textcircled{T} : $\begin{cases} ab = ac \\ a \neq 0 \end{cases} \Rightarrow b = c$

Ctrax si A n'est pas intègre

$$(1,0) \times (0,1) = (1,0) \times (0,0) = (0,0)$$

or $(0,1) \neq (0,0)$

$$a = (0, h_2) \neq 0$$

$$b = (18, 1)$$

$$c = (27, 1)$$

$$\text{mais } \begin{cases} a \times b = (0, 42) \\ a \times c = (0, 42) \end{cases}$$

(Très joli!)

D/ osq $a \neq 0$ et $ab = ac$

On a donc $ab - ac = 0$ ie $a(b-c) = 0$

Or, A intègre donc $a = 0$ ou $b-c = 0$

C/ $a \neq 0$, on a $b-c=0$, ie $b=c$ ■

\mathbb{F}_2 est un corps

D/ Soit A un anneau,

osq A est un corps

Montrons que A est intègre. Déjà A est commutatif et A est non nul

Soient $a, b \in A$ tq $ab = 0$

Mq $a=0$ ou $b=0$

On distingue deux cas

si $a=0$ ok

si $a \neq 0$ alors a est inversible car A corps

C/ $ab = 0$ on a $\frac{1}{a} \cdot ab = \frac{1}{a} \cdot 0$

donc $1 \cdot b = \frac{1}{a} \cdot 0$

donc $b = 0$ ■

Rq: + gennalt: On a

Prop Soit R un anneau

Soit $x \in R$ inversible (soit $x \in U(R)$)

Alors \textcircled{T} : $xy = xz \Rightarrow y = z$