16 GROUPE DES REELS MODULO UN

$\forall n \in \omega \setminus \{0,1\}$

RADICAL de n = rad n = produit de l'ensemble des diviseurs premiers de n

n PRIMAIRE ssi rad n premier

si n est puissance (à exposant NON nul) d'un premier

n SEMI-PREMIER ssi rad n = n

rad 2 = 2 — 2 primaire, semi-premier

rad 3 = 3 — 3 primaire, semi-premier

rad 4 = 2 — 4 primaire, non semi-premier

rad 5 = 5 — 5 primaire, semi-premier

rad 6 = 6 — 6 semi-premier, NON primaire

rad 7 = 7 — 7 primaire, semi premier

Si p est premier

Alors rad $p = p$

p est primaire, semi-premier

Si p^i est primaire

Alors rad $p^i = p$

<u>les premiers sont les seuls primaires, semi-premiers</u>

6 est le "plus petit" semi-premier non primaire
10, 14, 15, 21, 22, 26, 30, 33, 34, 35, ...
sont semi-premiers NON primaires

$\forall A, B \subset \mathbf{R}$ $\quad A + B = \{a + b \mid a \in A \wedge b \in B\}$

$\forall a \in \mathbf{R}$ $\forall B \subset \mathbf{R}$ $\quad a + B = \{a + b \mid b \in B\}$

$\forall A \subset \mathbf{R}$ $\forall b \in \mathbf{R}$ $\quad A + b = \{a + b \mid a \in A\}$

$\forall a \in \mathbf{R}$ $\forall B \subset \mathbf{R}$ $\quad aB = \{a b \mid b \in B\}$

$\forall s \in \mathbf{R}_0$

GROUPE des RÉELS MODULO s

Groupe $\mathbf{R}/s\mathbf{Z}, +$

Ensemble $\{r + s\mathbf{Z} \mid r \in \mathbf{R}\}$ muni de l'addition définie dans l'encadré précédent et que rappelle courtoisement la formule

$\forall a, b \in \mathbf{R}$ $\quad (a + s\mathbf{Z}) + (b + s\mathbf{Z}) = (a + b) + s\mathbf{Z}$

EPIMORPHISME CANONIQUE $\mathbf{R},+ \longrightarrow \mathbf{R}/_s\mathbf{Z},+$

$$\varphi : \mathbf{R},+ \longrightarrow \mathbf{R}/_s\mathbf{Z},+ \; : \; r \longmapsto r + {}_s\mathbf{Z}$$

Pour tout réel modulo un

$r+\mathbf{Z}$ RATIONNEL	$r+\mathbf{Z}$ IRRATIONNEL
ssi	ssi
$r \in \mathbf{Q}$	$r \notin \mathbf{Q}$
ssi	ssi
$r+\mathbf{Z} \subset \mathbf{Q}$	$r+\mathbf{Z} \subset \mathbf{R}\setminus\mathbf{Q}$

dans $\mathbf{R}/\mathbf{Z}$

$1+\mathbf{Z}$, $\frac{1}{2}+\mathbf{Z}$, $\frac{1}{3}+\mathbf{Z}$, $\frac{2}{3}+\mathbf{Z}$,
$\frac{1}{4}+\mathbf{Z}$, $\frac{3}{4}+\mathbf{Z}$, $\frac{1}{5}+\mathbf{Z}$, $\frac{2}{5}+\mathbf{Z}$, $\frac{3}{5}+\mathbf{Z}$, $\frac{4}{5}+\mathbf{Z}$, ...

sont rationnels

$(\sqrt{2})-1+\mathbf{Z}$, $\frac{\sqrt{2}}{2}+\mathbf{Z}$, $\frac{\sqrt{3}}{2}+\mathbf{Z}$, ...

sont irrationnels

$\forall n \in \omega_0$

Dans un groupe additif	Dans un groupe multiplicatif
a est UN n-ième de b	a est une RACINE n-ième de b
ssi	ssi
$b = na = a + \cdots + a$ (n termes)	$b = a^n = a \cdot \ldots \cdot a$ (n facteurs)

Soit un groupe additif M, +.

Sa loi scalaire nous permet de « multiplier » scalairement tout élément $m \in$ M par tout entier rationnel $z \in$ Z. Le résultat de cette opération est le multiple entier zm de m.

Tout naturellement se pose la question de « *la division scalaire* » par z. Autrement dit, étant donné $w \in$ M, existe-t-il toujours un élément $v \in$ M tel que $zv = w$?

L'exemple du groupe Z, + des entiers rationnels suffit à prouver que la « division scalaire » par z n'est pas toujours possible.

L'exemple du groupe R/Z, + montre que quand cette opération est possible, elle n'est pas toujours unique.

Exemple : $3 \cdot (,000\ldots) = 0$
$3 \cdot (,333\ldots) = 0$
$3 \cdot (,666\ldots) = 0$

Il est facile de voir que la division sera possible par z si et seulement si elle est possible par valeur absolue de z.

On appellera *divisible* un groupe dans lequel la division est possible par tout entier naturel non nul (et donc aussi par tout entier rationnel non nul). Le vocable « divisible » sera utilisé de manière générale quelle que soit la manière de noter la loi interne et la loi scalaire du groupe considéré.

Définition. — Le groupe G, $*$ *est dit divisible* si et seulement si pour tout $g \in$ G et tout $n \in \omega_0$, il existe (au moins) un $h \in$ G tel que

$$g = n \quad h$$

Exemples

a) Le groupe Z, + n'est pas divisible.
b) Les groupes Q, + et R, + sont divisibles.

c) Le groupe R_0^+, $\cdot$ est divisible.
« La division scalaire par n » est ici l'« extraction » de la racine n-ième arithmétique. Dans ce cas, le résultat est unique.
d) Le groupe R_0, $\cdot$ n'est pas divisible.
e) Le groupe R/Z, + est divisible.
Le résultat de la division scalaire n'est pas toujours unique.
f) Le groupe des rotations planes autour d'un point est divisible. Le résultat de la division scalaire n'est pas toujours unique.

Un groupe additif est DIVISIBLE ssi chacun de ses éléments admet au moins un n-ième, pour tout naturel non nul n.	Un groupe multiplicatif est DIVISIBLE ssi chacun de ses éléments admet au moins une racine n-ième, pour tout naturel non nul n.

$\forall a \in \omega \setminus \{0,1\}$

$$\mathbf{L}_a, + = \{ b/a^n \mid b \in \mathbf{Z} \wedge n \in \omega \}, +$$

= Groupe des nombres a-naires limités

$\forall a \in \omega \setminus \{0,1\}$

$\mathbf{L}_a / \mathbf{Z}, +$ = Groupe des a-naires limités modulo un

= Groupe des a-naires limités décapités

$\forall a \in \omega \setminus \{0,1\}$

a-groupe de PRÜFER

Groupe (de type) a^{∞} = Groupe isomorphe à $\mathbf{L}_a / \mathbf{Z}, +$

L_2/Z groupe des binaires limités

quelques éléments :

0 ; ,5 ; ,25 ; ,75 ; ,125 ; ,625 ;

,0625 ; ,1875 ;

,03125

,015625

,0078125

,00390625

,001953125

,0009765625

L_3/Z groupe des Ternaires limités

quelques éléments :

0

,33333333 ....

,66666666 ....

,11111111 ....

,22222222 ...

,44444444 ...

,55555555 ...

,77777777 ...

,88888888 ...

L_4/Z

0; ,25 ; ,0625 ; ,015625 ; ,00390625...

L_5/Z

0; ,2 ; ,4 ; ,6 ; ,8 ;

,04 ; ,08 ; ,12 ; ,16 ; ,24 ; ,28 ; ,32 ; ,36

,44 ; ,48 ; ,52 ; ,56 ; ,64 ; ,68 ; ,72 ;

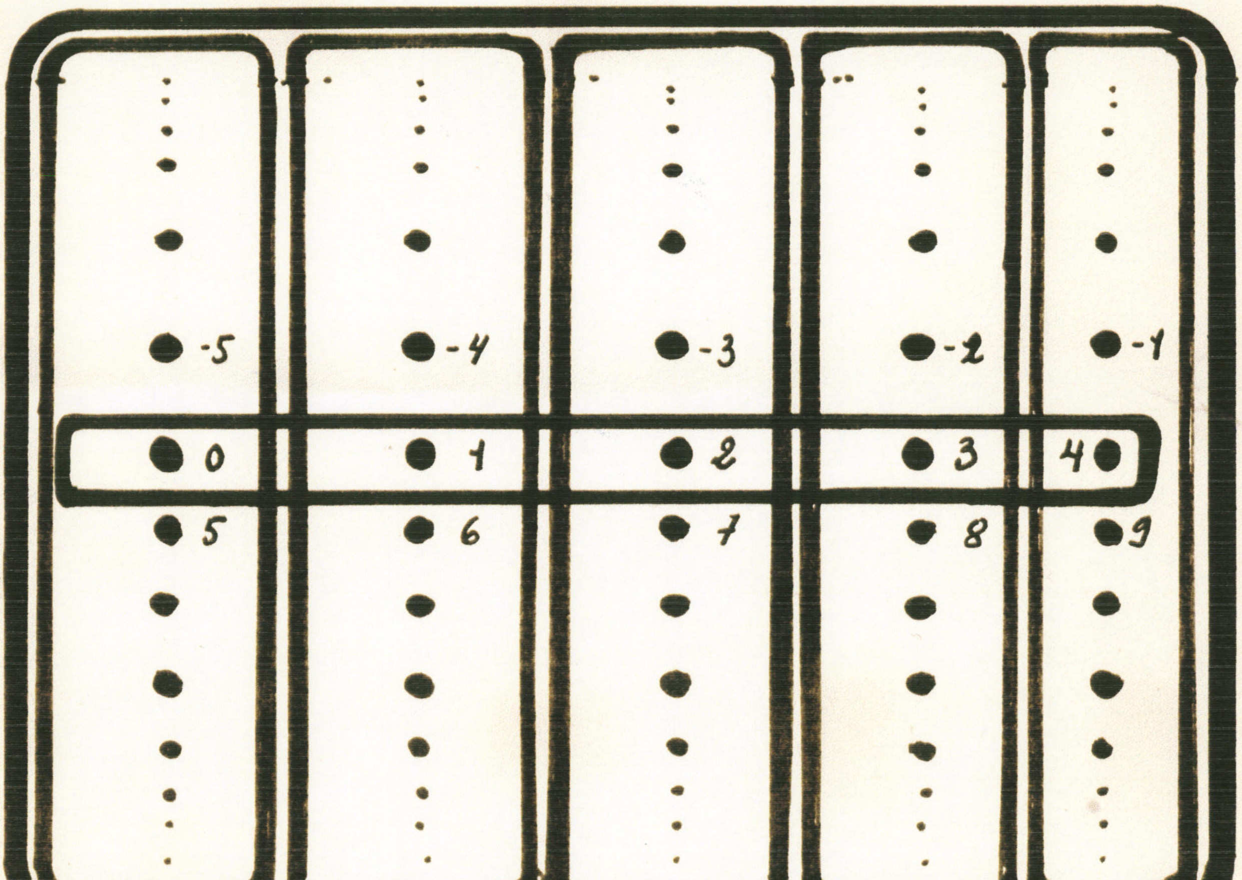
,76 ; ,84 ; ,88 ; ,92 ; ,96

DELEGATION de la partition P de l'ensemble E

||

Partie de E qui trace un singleton sur toute pièce de P

Exemple



D est une délégation de Z_5 sur Z

$\forall s \in \mathbb{R}_0$

Le groupe des réels modulo s est isomorphe à celui des réels modulo un

$$\mathbb{R}/s\mathbb{Z},+ \quad \cong \quad \mathbb{R}/\mathbb{Z},+$$

* L'automorphisme $x \mapsto sx$ de $\mathbb{R},+$ applique $\mathbb{Z}$ sur $s\mathbb{Z}$

■

$\forall s \in \mathbb{R}$

Toute délégation des réels modulo s s'érige naturellement en un groupe isomorphe à celui des réels modulo un.

* Dans la délégation, la somme des délégués x, y est le délégué du réel modulo s

$$x + y + s\mathbb{Z} = (x + s\mathbb{Z}) + (y + s\mathbb{Z})$$

$\forall s \in \mathbb{R}$

$[0, s[$ est une délégation des réels modulo s, et s'érige naturellement en un groupe isomorphe à $\mathbb{R}/\mathbb{Z},+$

$\forall a \in \omega \setminus \{0,1\}$

SI $\mathcal{D}$ est une délégation des réels modulo un (et donc naturellement un groupe isomorphe $\mathbf{R}/\mathbf{Z}$)

ALORS $\mathcal{D} \cap \mathbf{L}_a$ est une délégation de $\mathbf{L}_a/\mathbf{Z}$ et un sous-groupe de $\mathcal{D}$ isomorphe à $\mathbf{L}_a/\mathbf{Z}$

$\forall a \in \omega \setminus \{0,1\}$

$[0,1[$ est une délégation des réels modulo un et donc naturellement un groupe isomorphe à $\mathbf{R}/\mathbf{Z}$

$[0,1[\cap \mathbf{L}_a$ est une délégation de $\mathbf{L}_a/\mathbf{Z}$ et un sous groupe de $[0,1[$ isomorphe à $\mathbf{L}_a/\mathbf{Z}$

Situation pédagogique

Dans la base a, tout réel de $[0,1[$ s'écrit d'au moins une manière

$$0, a_1 a_2 \ldots\ldots$$

On peut indiquer que l'on se place dans le groupe de la délégation $[0,1[$ des réels modulo un en remplaçant 0 par ,

En base dix

$$,3 + ,4 = ,7$$

$$,7 + ,8 = ,5$$

$$- ,3 = ,7$$

$$,8 + ,2 = 0$$

Pour tout réel modulo un RATIONNEL = D'ORDRE FINI dans le groupe $\mathbf{R}/\mathbf{Z}, +$

□ Tout rationnel modulo un est d'ordre fini

* le rationnel modulo un nul $\mathbf{Z}$ est d'ordre 1...

Tout rationnel modulo un non nul s'écrit de manière unique $p/q + \mathbf{Z}$

avec $p \in \omega \wedge q \in \omega_0 \wedge p \wedge q = 1 \wedge p < q$

... et q est l'ordre de $p/q + \mathbf{Z}$, dans le groupe $\mathbf{R}/\mathbf{Z}, +$

■

□ Tout réel modulo un d'ordre fini est rationnel

* ▲ $r + \mathbf{Z}$ réel modulo un d'ordre n.

$n(r + \mathbf{Z}) = \mathbf{Z}$

$n r \in \mathbf{Z}$

$r \in \mathbf{Q}$

■

■

$\forall s \in \mathbf{R}_0$ — $\forall r \in \mathbf{R}$

Tout groupe des réels modulo s est divisible

$$\frac{r}{n}+\mathbf{Z},\quad \frac{r+1}{n}+\mathbf{Z},\ \dots,\ \frac{r+(n-1)}{n}+\mathbf{Z}$$

sont les n n-ièmes du réel modulo un
$r+\mathbf{Z}$

tandis que

$$\frac{sr}{n}+s\mathbf{Z},\quad \frac{s(r+1)}{n}+s\mathbf{Z},\ \dots,\ s\left(\frac{r+n-1}{n}\right)+s\mathbf{Z}$$

sont les n-nièmes de $r+s\mathbf{Z}$ réel
modulo s.

$$\mathbf{Z},\quad \frac{1}{n}+\mathbf{Z},\ \dots,\ \frac{n-1}{n}+\mathbf{Z}$$

sont les n nièmes du zéro de $\mathbf{R}/\mathbf{Z}$

$$s\mathbf{Z},\quad \frac{s}{n}+s\mathbf{Z},\ \dots,\ \frac{n-1}{n}s+s\mathbf{Z}$$

sont les n n-ièmes du zéro de $\mathbf{R}/s\mathbf{Z}$

En $\mathbb{R}/\mathbb{Z}$, +

$\frac{1}{2}+\mathbb{Z}$, $\mathbb{Z}$ 2-ièmes de $\mathbb{Z}$

$\mathbb{Z}$, $\frac{1}{3}+\mathbb{Z}$, $\frac{2}{3}+\mathbb{Z}$ sont les 3-ièmes de $\mathbb{Z}$

$\mathbb{Z}$, $\frac{1}{4}+\mathbb{Z}$, $\frac{2}{4}+\mathbb{Z}$, $\frac{3}{4}+\mathbb{Z}$ sont les 4-ièmes de $\mathbb{Z}$

$0{,}25+\mathbb{Z} = {,}25$
$0{,}75+\mathbb{Z} = {,}75$
sont les 2-ièmes de $0{,}5+\mathbb{Z} = {,}5$

,16666...
,5
,83333...
sont les 3-ièmes de ,5

,15
,375
,625
,875
sont les 4-ièmes de ,5

,1
,3
,5
,7
,9
sont les 5-ièmes de ,5

,833333 ...
,25
,416666 ...
,586666 ...
,75
,916666 ...
sont les 6-ièmes de ,5

Si $\mathbf{L}_a \subset \mathbf{L}_b$

$\forall x \in \mathbf{L}_a$

$$x = z/a^n = z'/b^m$$

$$z/a^n = z'/b^m$$

$$b^m\mathbf{Z} \subset a^n\mathbf{Z}$$

$$a^n \mid b^m$$

$$a \mid a^n \mid b^m$$

$$a \mid b^m$$

Tout premier divisant a divise b^m

Tout premier divisant a doit diviser b

$p_1 \cdot \ldots \cdot p_m = \text{rad } a$

Alors $p_1, \ldots, p_m$ sont des premiers divisant b

et $$b = [p_1 \cdot \ldots \cdot p_m] \cdot p_1^{\alpha_1} \cdot \ldots \cdot p_m^{\alpha_m} \cdot q_1^{\beta_1} \cdot \ldots \cdot q_m^{\beta_m}$$

$$= \underbrace{[p_1 \cdot \ldots \cdot p_m] \cdot q_1 \cdot \ldots \cdot q_m} \cdot p_1^{\alpha_1} \cdot \ldots \cdot p_m^{\alpha_m} \cdot q_1^{\beta_1 - 1} \cdot \ldots \cdot q_m^{\beta_m - 1}$$

$$= \text{rad } b \cdot p_1^{\alpha_1} \cdot \ldots \cdot p_m^{\alpha_m} \cdot q_1^{\beta_1 - 1} \cdot \ldots \cdot q_m^{\beta_m - 1}$$

et $\text{rad } a \mid \text{rad } b$

$$a = p_1^{\alpha_1} \cdot \ldots \cdot p_m^{\alpha_m}$$

$$b = p_1^{\beta_1} \cdot \ldots \cdot p_m^{\beta_m} \cdot q_1^{\gamma_1} \cdot \ldots \cdot q_\ell^{\gamma_\ell}$$

$$b = p_1^{\alpha_1} \cdot \ldots \cdot p_m^{\alpha_m} \cdot p_1^{\beta_1 - \alpha_1} \cdot \ldots \cdot p_m^{\beta_m - \alpha_m} \cdot q_1^{\gamma_1} \cdot \ldots \cdot q_\ell^{\gamma_\ell}$$

$$a^i = (p_1^{\alpha_1} \cdot \ldots \cdot p_m^{\alpha_m})^i = p_1^{\alpha_1 i} \cdot \ldots \cdot p_m^{\alpha_m i}$$

$$a^i \cdot p_1^{(\beta_1-\alpha_1)i} \cdot \ldots \cdot p_m^{(\beta_m-\alpha_m)i} \cdot q_1^{\gamma_1 i} \cdot \ldots \cdot q_\ell^{\gamma_\ell i} = b^i$$

$$3/a^i = \frac{3 \cdot p_1^{(\beta_1-\alpha_1)i} \cdot \ldots \cdot p_m^{(\beta_m-\alpha_m)i} \cdot q_1^{\gamma_1 i} \cdot \ldots \cdot q_\ell^{\gamma_\ell i}}{b^i}$$

$$= 3'/b^i$$

et... $\mathbf{L}_a \subset \mathbf{L}_b$

D'où le théorème :

$$\forall a, b \in \omega \setminus \{0,1\}$$

$$\boxed{\mathbf{L}_a \subset \mathbf{L}_b \iff \exists n \in \omega \quad a \mid b^n \iff \operatorname{rad} a \mid \operatorname{rad} b}$$

Ex. $3/8^2 \in \mathbf{L}_8$

$\operatorname{rad} 8 = 2$

$8^2 = (2^3)^2 = 2^6 = 2^2 \cdot 2^2 \cdot 2^2$

$a = 8 \qquad b = 4 \qquad \operatorname{rad} b = 2 = \operatorname{rad} a$

$$3/64 = 3/8^2 = 3 \cdot 2^2 / 2^2 \cdot 2^2 \cdot 2^2 \cdot 2^2$$

$$= 3 \cdot 2^2 / 4^4 = 12/4^4$$

$$3/8^2 = 12/4^4$$

et bien sûr découle le théorème

$$\forall a, b \in \omega \setminus \{0,1\}$$

$$\boxed{\mathbf{L}_a = \mathbf{L}_b \iff \text{rad}\, a = \text{rad}\, b \iff \mathbf{L}_a/\mathbf{Z} = \mathbf{L}_b/\mathbf{Z}}$$

Lemme : 1. si p est un premier ne divisant pas b
Alors $b^\infty = \mathbf{L}_b/\mathbf{Z}$ ne comprend
aucun p-ième de zéro non nul

$*$ x/b^m un p-ième de zéro

$$p \cdot x/b^m = \frac{px}{b^m} \in \mathbf{Z}$$

$$\exists z \in \mathbf{Z} \quad px = b^m z$$

$$p \nmid b \Rightarrow p \mid z \quad \text{et} \quad b^m \mid x$$

$$x/b^m + \mathbf{Z} = \alpha b^m/b^m + \mathbf{Z}$$

$$= \alpha + \mathbf{Z} = \mathbf{Z}$$

et… $x/b^m + \mathbf{Z}$ est nul

2. Si p est un premier divisant a
Alors $a^\infty = \mathbf{L}_a/\mathbf{Z}$ comprend le
p-ième $1/p + \mathbf{Z}$ NON nul de zéro

$*$ $1/p + \mathbf{Z} \neq \mathbf{Z}$

$$p(1/p + \mathbf{Z}) = \mathbf{Z}$$

- 3^∞ contient des images isomorphes aux groupes cycliques FINIS d'ordre puissance naturelle de 3.
  à un iso près,
  $\mathbb{Z}_3, \mathbb{Z}_9, \mathbb{Z}_{27}, \dots, \mathbb{Z}_{3^i}$
  sont sous-groupes de 3^∞

$4^\infty = 2^\infty$

- 5^∞ contient des images isomorphes aux groupes cycliques FINIS d'ordre puissance naturelle de 5
  à un iso près,
  $\mathbb{Z}_5, \mathbb{Z}_{25}, \mathbb{Z}_{125}, \dots, \mathbb{Z}_{5^i}$
  sont sous-groupes de 5^∞

- $6^\infty =$
  rad $6 = 6 = 2 \cdot 3$
  rad $2 = 2 \mid 6 =$ rad 6
  rad $3 = 3 \mid 6 =$ rad 6

$$2^\infty = \{ z/2^i \mid z \in \mathbb{Z} \ i \in \mathbb{N}_0 \} = \{ z \cdot 3^i/6^i \mid z \in \mathbb{Z} \ i \in \mathbb{N}_0 \}$$

2^∞ est un sous-groupe PROPRE INFINI de 6^∞

$$3^\infty = \{ z/3^j \mid z \in \mathbb{Z} \ j \in \mathbb{N}_0 \} = \{ z \cdot 2^j/6^j \mid z \in \mathbb{Z} \ j \in \mathbb{N}_0 \}$$

3^∞ est un sous-groupe PROPRE INFINI de 6^∞

Si p est un premier divisant a
ne divisant pas b

Alors

$\mathbf{L}_a/\mathbf{Z}$ comprend UN p-ième NON nul de zéro
$\mathbf{L}_b/\mathbf{Z}$ NE comprend AUCUN p-ième NON nul de zéro

et $\mathbf{L}_a/\mathbf{Z}$ $\mathbf{L}_b/\mathbf{Z}$ sont NON isos.

$\forall a, b \in \omega \setminus \{0, 1\}$

a^∞ iso b^∞ ssi $\mathbf{L}_a/\mathbf{Z}$ iso $\mathbf{L}_b/\mathbf{Z}$ ssi $\operatorname{rad} a = \operatorname{rad} b$

Tout a-groupe de PRÜFER $a^\infty = \mathbf{L}_a/\mathbf{Z}$
est commutatif, dénombrable et divisible

des sous-groupes des **a**-groupes de PRÜFER

a) en $\mathbf{2}^\infty$

$\operatorname{grp}(0{,}5) = \{0{,}5 \ ; \ 0\}$ iso $\mathbf{Z}_2$
$\operatorname{grp}(0{,}25) = \{0{,}25 \ ; \ 0{,}5 \ ; \ 0{,}75 \ ; \ 0\}$ iso $\mathbf{Z}_4$
$\vdots$
$\operatorname{grp}(1/2^i) =$ iso $\mathbf{Z}_{2^i}$

Tout élément NON nul de 2^∞
engendre un sous-groupe cyclique FINI
d'ordre puissance naturelle de 2

<u>Si</u> a <u>est NON primaire</u>

<u>Alors</u> <u>rad a est non premier</u>

soit p un premier divisant rad a

On a rad $p = p$

d'où rad $p \mid$ rad a

et... $\mathbf{L}_p \subsetneq \mathbf{L}_a$

Si **a** est NON primaire,

alors le a-groupe de PRÜFER

$$a^\infty = \mathbf{L}_a / \mathbf{Z}$$

contient des sous-groupes propres INFINIS

Il en est ainsi des a-groupes de PRÜFER

6^∞ ; 10^∞ ; 14^∞ ; 15^∞ ; 22^∞ ; 26^∞ ; 30^∞, ...

Lemme

Si p est premier

Si S est un sous-groupe de $\mathbf{L}_p/\mathbf{Z}$

Si $\exists n \in \omega$

$$\bigstar/p + \mathbf{Z},\ \bigstar/p^2 + \mathbf{Z},\ \dots,\ \bigstar/p^n + \mathbf{Z} \ \in S$$

$$\bigstar/p^{n+1} + \mathbf{Z} \notin S$$

les $\bigstar$ désignent des entiers rationnels non divisibles par p

Alors par BACHET-BEZOUT

$$\exists\ p', b \in \mathbf{Z} \qquad p^n \cdot p' + \bigstar\, b = \bigstar \wedge p^n = 1$$

d'où $\exists\ p', b \in \mathbf{Z} \qquad b\,(\bigstar/p^{n} + \mathbf{Z}) = 1/p^n + \mathbf{Z}$

et... $grp\,(1/p^n + \mathbf{Z}) \subset S$

montrons par l'absurde que

$$S \setminus grp\,(1/p^n + \mathbf{Z}) = \emptyset$$

soit $x \in S \setminus grp(1/p^n + \mathbf{Z})$

il existe alors un $m > n$ tel que

$$x \in grp\,(1/p^m + \mathbf{Z}) \setminus grp\,(1/p^{m-1} + \mathbf{Z})$$

mézalor $\quad grp\,(x) = grp\,(1/p^m + \mathbf{Z}) \qquad m > n$

or $\quad m > n \Rightarrow m \geqslant n+1$

et... $\quad 1/p^{n+1} + \mathbf{Z} \in grp(x) \subset S$

ce qui est en contradiction avec l'hypothèse

Ex en $\mathbb{L}_2/\mathbb{Z}$

Si $1/2 + \mathbb{Z} \in S$ $\quad 1/2^2 + \mathbb{Z} \notin S$

Alors $\quad S \cong \mathbb{Z}_2 = \text{grp}\,(,5)$

Si $1/2 + \mathbb{Z},\ 1/2^2 + \mathbb{Z} \in S$

$1/2^3 + \mathbb{Z} \notin S$

Alors $\quad S \cong \mathbb{Z}_4 = \text{grp}\,(,25)$

$\vdots$

Si $\exists n \in \omega$

$1/p + \mathbb{Z},\ 1/p^2 + \mathbb{Z},\ \ldots,\ 1/p^n + \mathbb{Z} \in S$

$1/p^{n+1} + \mathbb{Z} \notin S$

Alors S iso $\mathbb{Z}_{p^n}$

et... S est sous-groupe FINI de $\mathbb{L}_p/\mathbb{Z}, +$

Si p est premier

Si S est un sous-groupe INFINI de $\mathbf{L}_p/\mathbf{Z}, +$

Alors

$\forall n \in \omega$

S doit comprendre au moins un élément

$$b/p^m + \mathbf{Z}$$

avec $b, m \in N$ $\quad m > n \quad p \nmid b$

et par BACHET-BEZOUT et conséquences,

$\forall n \in \omega$

S doit comprendre au moins

$$1/p^m + \mathbf{Z}$$

avec $m > n$

d'où $\quad 1/p + \mathbf{Z} \in S$

$\quad 1/p^2 + \mathbf{Z} \in S$

$\vdots$

$\forall i \in \omega \quad 1/p^i + \mathbf{Z} \in S$

et... $\forall i \in \omega \; \forall b \in \mathbf{N} \quad b(1/p^i + \mathbf{Z})$

$$= b/p^i + \mathbf{Z} \in S$$

et... $\quad S = \mathbf{L}_p/\mathbf{Z}$

En résumé

$$\boxed{\begin{array}{c}\text{Tout sous-groupe propre d'un } a\text{-groupe de PRÜFER} \\ \text{est FINI} \\ \text{ssi} \\ a \text{ est primaire.}\end{array}}$$

Ce sont des groupes quasi-cycliques dont l'importance est considérable en la catégorie des groupes commutatifs.

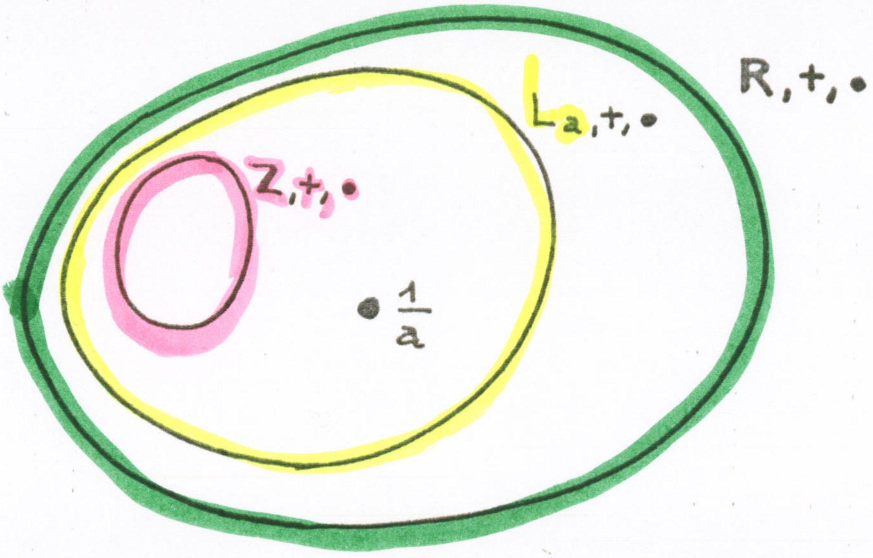
Les groupes INFINIS

$\mathbf{L}_2/\mathbf{Z}$; $\mathbf{L}_3/\mathbf{Z}$; $\mathbf{L}_5/\mathbf{Z}$; ... ; $\mathbf{L}_p/\mathbf{Z}$ p premier

n'ont comme sous-groupes PROPRES que les groupes CYCLIQUES FINIS

EX $\quad L_a, +, \cdot$ est un sous-anneau de $\mathbf{R}, +, \cdot$

EX $\quad L_a, +$ est le groupe additif du sous-anneau de $\mathbf{R}, +, \cdot$ engendré par $\mathbf{Z} \cup \left\{ \frac{1}{a} \right\}$



EX $\quad L_a, +$ est le sous-groupe de $\mathbf{R}, +$

engendré par $\mathbf{Z} \cup \{ 1/a^n \mid n \in \omega \}$

engendré par $\{1\} \cup \{ 1/a^n \mid n \in \omega \}$

engendré par $\{ 1/a^n \mid n \in \omega \}$

engendré par $\{ 1/a^n \mid n \in \omega \text{ et } n > m \}$

(où m, naturel, est fixé)

engendré par une partie infinie quelconque de $\{ 1/a^n \mid n \in \omega \}$

EX La fonction rad : $\omega \setminus \{0,1\} \to \omega \setminus \{0,1\} : n \mapsto \text{rad}\, n$

est croissante

EX G est groupe divisible ssi $\forall n \in \omega_0 : nG = G$

EX $\forall s \in R_0^+$

$[0,s[$ est un ensemble de choix des réels modulo s et

s'érige naturellement en groupe

$[0,s[\,, \oplus$ isomorphe à $R/Z\,, +$

EX Dans $R/Z\,, +$

tout élément a exactement deux demis.

EX Dans $[0,1[\,, \oplus$

tout élément a exactement deux demis

Les deux **demis** de r

Dans $[0,1[\,, \oplus$

EX Dans $[0,1[\,, \oplus\,, \leqslant$

tout élément a exactement un demi *plus petit que lui* .

EX Dans $[0,1[\,, \oplus$, pour tout $n \in \omega_0$:

$$\left(\tfrac{1}{2}\right)^{n+1} \text{ et } \frac{\left(\tfrac{1}{2}\right)^{n}+1}{2} \text{ sont les deux } \textbf{demis} \text{ de } \left(\tfrac{1}{2}\right)^{n}$$

$$0 < \left(\tfrac{1}{2}\right)^{n+1} < \left(\tfrac{1}{2}\right)^{n} < \frac{\left(\tfrac{1}{2}\right)^{n}+1}{2} < 1$$