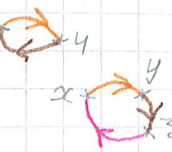
Structures algébriques

I Relation d'équivalence

1. E ensemble, R relation binaire sur E $\quad R : \begin{cases} E\times E \longrightarrow \{0,1\} \\ (x,y) \longmapsto R(x,y) = \begin{cases} 1 & \text{si } xRy \\ 0 & \text{si } x \not R y \end{cases} \end{cases}$

R relation d'équivalence si :

R est $\begin{cases} \text{réflexive} : \forall x \in E, & xRx \\ \text{symétrique} : \forall (x,y) \in E^2 & xRy \Rightarrow yRx \\ \text{transitive} : \forall (x,y,z) \in E^3 & xRy \text{ et } yRz \Rightarrow xRz \end{cases}$



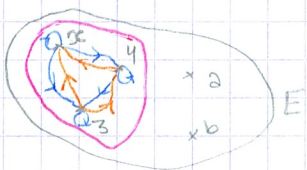
ex : $f : E \longrightarrow F$

$\forall (x,y) \in E^2, \quad xRy \Leftrightarrow f(x) = f(y)$

classe d'équivalence de x : $Cl(x) = \{y \in E / xRy\}$

x est un représentant de $Cl(x)$

(tous les éléments d'une classe sont en relation les uns avec les autres)
(tout élément d'une classe la représente)



Pp 1) $\forall x \in E, \quad x \in Cl(x)$

Pp 2) $\forall x \in E, \quad Cl(x) \neq \emptyset$

Pp 3) $\forall (x,y) \in E^2, \quad Cl(x) = Cl(y)$ ou $Cl(x) \cap Cl(y) = \emptyset$

On suppose $Cl(x) \cap Cl(y) \neq \emptyset$

$\exists z \in E / z \in Cl(x) \cap Cl(y)$: xRz et yRz

$\forall u \in E, \quad u \in Cl(x) \Rightarrow xRu$

donc $yRz, zRx, xRu \Rightarrow yRu \Rightarrow u \in Cl(y)$

donc $Cl(x) \subset Cl(y)$

de même, $Cl(y) \subset Cl(x)$

Pp 4) $\forall (x,y) \in E^2, \quad xRy \Leftrightarrow Cl(x) = Cl(y)$

- $xRy \Rightarrow y \in Cl(x) \Rightarrow y \in Cl(x) \cap Cl(y)$
  $\Rightarrow Cl(x) \cap Cl(y) \neq \emptyset \Rightarrow Cl(x) = Cl(y)$
- $Cl(x) = Cl(y)$ or $y \in Cl(y) = Cl(x) \Rightarrow y \in Cl(x) \Rightarrow xRy$

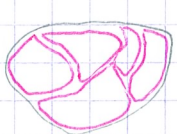
Pp 5) $\forall y \in Cl(x)$, y est un représentant de $Cl(x)$

Pp 6) $E = \bigcup_{x \in E} Cl(x)$

- $\forall x \in E, \quad Cl(x) \subset E$ donc $\bigcup_{x \in E} Cl(x) \subset E$
- $\forall y \in E, \quad y \in Cl(y)$
  $y \in \bigcup_{x \in E} Cl(x)$ donc $E \subset \bigcup_{x \in E} Cl(x)$

"y appartient à 1 classe, donc à l'ensemble de toutes les classes"

Pp 7) des classes d'équivalence réalisent une partition de E



$\forall x \in E, \quad Cl(x) \neq \emptyset$

$\forall (x,y) \in E^2, \quad Cl(x) \cap Cl(y) \neq 0$ ou $Cl(x) = Cl(y)$

$\bigcup_{x \in E} Cl(x) = E$

Pp 8) soit E un ensemble : p classes d'équivalence ayant chacune un représentant $x_1, x_2, \dots, x_p$: $E = \bigcup_{1 \leq k \leq p} Cl(x_k)$

$$\text{Card } E = \sum_{k=1}^{p} \text{card } Cl(x_k)$$

en particulier, si : $\exists q \in \mathbb{N}^* / \forall k \in \{1, \dots, p\}$, $\text{card } Cl(x_k) = q$

alors, $\text{card } E = pq$

E/R : ensemble des classes d'équivalence

$\forall x \in E, \quad Cl(x) \in E/R \qquad Cl(x) \subset E$

II Groupes

1. $(\mathbb{Z}, +)$, $(\mathbb{Q}, +)$, $(\mathbb{R}, +)$, $(\mathbb{C}, +)$
   $(\mathbb{Q}^*, \times)$, $(\mathbb{R}^*, \times)$, $(\mathbb{C}^*, \times)$
   $(E, +)$ avec E ev
   $(GL(E), \circ)$ $(GL_n(\mathbb{R}), \times)$
   $(SL(E), \circ)$ $(SL_n(\mathbb{R}), \times)$

$\varphi : G \longrightarrow G'$ morphisme de groupes

$\text{Ker } \varphi = \varphi^{-1}(e')$

φ injective $\Leftrightarrow \text{Ker } \varphi = \{e\}$

2- **groupe produit** : $n \in \mathbb{N}^*$, $G_1, \dots, G_n$ n groupes de neutres $e_1, \dots, e_n$

$G = G_1 \times \dots \times G_n = \{(x_1, \dots, x_n),\ x_1 \in G_1, \dots, x_n \in G_n\}$

$\forall (x_1, \dots, x_n), (y_1, \dots, y_n) \in G^2$, $(x_1, \dots, x_n) \cdot (y_1, \dots, y_n) = (x_1 \cdot_{G_1} y_1, x_2 \cdot_{G_2} y_2, \dots, x_n \cdot_{G_n} y_n)$

$(G, \cdot)$ est un groupe de neutre $(e_1, \dots, e_n)$

$i_0 \in \{1, \dots, n\}$ $p_{i_0} : \begin{cases} G \longrightarrow G_{i_0} \\ (x_1, \dots, x_{i_0}, \dots x_n) \longmapsto x_{i_0} \end{cases}$ p_{i_0} est un morphisme

$\ker p_{i_0} = G_1 \times G_2 \times \dots \times G_{i_0-1} \times e_{i_0} \times G_{i_0+1} \times \dots \times G_n$ $\quad y \in \ker p_{i_0} \iff x_{i_0} = e_{i_0}$

3- **partie génératrice**

a- **sous-groupe engendré par une partie**

$\forall$ partie non vide du groupe G

$H = \{a_1^{k_1} a_2^{k_2} \dots a_n^{k_n} \mid n \in \mathbb{N}^*, (k_1, \dots, k_n) \in \mathbb{Z}^n, \forall i \in \{1, \dots, n\}, a_i \in A\}$

Pp 1) H est un ss-groupe de G

- $A \subset H$ donc $H \neq \emptyset$
- $H \subset G$
- $\forall (x, y) \in H$,
  $\exists n \in \mathbb{N}^*, \exists (k_1, \dots, k_n) \in \mathbb{Z}^n, \exists (a_1, \dots, a_n) \in A^n$ / $x = a_1^{k_1} \dots a_n^{k_n}$
  $\exists m \in \mathbb{N}^*, \exists (\ell_1, \dots, \ell_m) \in \mathbb{Z}^m, \exists (b_1, \dots, b_m) \in A^m$ / $y = b_1^{\ell_1} \dots b_m^{\ell_m}$
  donc $y^{-1} = b_1^{-\ell_1} \dots b_m^{-\ell_m}$
  donc $xy^{-1} = a_1^{k_1} \dots a_n^{k_n} b_1^{-\ell_1} \dots b_m^{-\ell_m} \in H$

Pp 2) $A \subset H \subset G$

Pp 3) si $\begin{cases} K \text{ ss-groupe de } G \\ A \subset K \end{cases}$ alors $H \subset K$ $\quad (A \subset H \subset K \subset G)$

si $A \subset K$, alors $\forall n \in \mathbb{N}^*, \forall (k_1, \dots, k_n) \in \mathbb{Z}^n, \forall (a_1, \dots, a_n) \in A^n \subset K^n$
$a_1^{k_1} \dots a_n^{k_n} \in K$ donc $H \subset K$

Pp 4) H est le **plus petit** ss-groupe de G qui **contient** A

Pp 5) $\bigcap_{\substack{A \subset K \\ K \text{ ss.gr. de } G}} K = H$

$\bigcap_{\substack{A \subset K \\ K \text{ ss.gr}}} K$ $\begin{cases} \text{est un ss-groupe} \\ \text{contient } A \\ \text{contient } H \end{cases}$ donc $H \subset \bigcap_{\substack{A \subset K \\ K \text{ ss.gr de } G}} K$

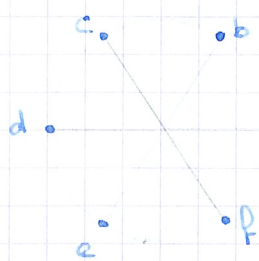
or, $\begin{cases} H \text{ ss.gr. de } G \\ A \subset H \end{cases}$ donc H est un des ss.gr de G $\bigcap_{\substack{A \subset K \\ K \text{ ss.gr de } G}} K \subset H$ (contient H)

H est le ss.gr de G **engendré par** A.

b- **partie génératrice**

$S \subset G$ S **partie génératrice de** G si le **ss.gr engendré par** S est G

ex: $U_6 = \{z \in \mathbb{C} / z^6 = 1\} = \{\underset{a}{1}, \underset{b}{e^{i\pi/3}}, \underset{c}{e^{2i\pi/3}}, \underset{d}{e^{i\pi}}, \underset{e}{e^{4i\pi/3}}, \underset{f}{e^{5i\pi/3}}\}$



ss-gr. engendré par $\{a\}$: $\{a\}$
$\{b\}$: U_6
$\{c\}$: $\{e, c, a\} = U_3$
$\{d\}$: $\{a, d\} = U_2$
$\{e, d\}$: $\{c, d, \underbrace{c^{-1} d}_{b}\} = U_6$

4- **groupe monogène, groupe cyclique**

G est un gr. **monogène** s'il possède 1 **singleton générateur**
G est un gr. **cyclique** s'il est **monogène** et **fini**.

Rq : gr. monogène non cyclique : $(\mathbb{Z},+)$ de partie génératrice $\{1\}$ ou $\{-1\}$ C
gr. cyclique : $U_6 = \{z \in \mathbb{C} / z^6 = 1\} = \{e^{i\pi/3}\}$ ..... $\{e^{2i\pi/6}\}$
$U_n = \{z \in \mathbb{C} / z^n = 1\}$ ..... $\{e^{2i\pi/n}\}$
$n \in \mathbb{N}^*$

5. ordre d'un élément dans un groupe

* $a \in G$, $\varphi_a : \begin{cases} \mathbb{Z} \to G \\ k \mapsto a^k \end{cases}$ $\varphi_a(k+k') = \varphi_a(k)\,\varphi_a(k')$

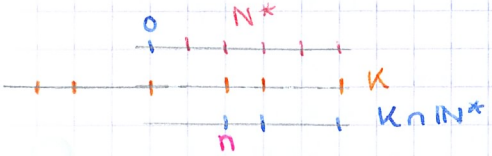
donc φ_a est un morphisme de groupes

$\operatorname{Im}\varphi_a$ est un ss-gr. de G $\operatorname{Im}\varphi_a = \{a^k / k \in \mathbb{Z}\}$
ss-gr engendré par a

notat° multi : $a_1^{k_1} \dots a_n^{k_n}$
addilive : $k_1 a_1 + \dots + k_n a_n$

$\operatorname{Ker}\varphi_a$ est un ss-gr de $(\mathbb{Z},+)$

Rappel : soit K un ss-gr de $(\mathbb{Z},+)$:
1er cas : $K = \{0\}$
2ème cas : • $K \neq \{0\}$ donc $K \cap \mathbb{N}^* \neq \emptyset$
soit $n = \min\{K \cap \mathbb{N}^*\}$
$n \in K$ donc $n\mathbb{Z} \subset K$ (ss-gr engendré par n)
• $\forall m \in K$, $\exists q \in \mathbb{Z} / \exists r \in \{0, \dots, n-1\} / m = qn + r$
donc $r = \underbrace{m}_{\in K} - \underbrace{qn}_{\in K}$ ($qn \in n\mathbb{Z} \subset K$)
$r \in K \cap \{0, \dots, n-1\} = \emptyset$
donc $r = 0$ donc $m = qn \in n\mathbb{Z}$ car n est le plus petit
donc $m \in n\mathbb{Z}$ donc $K \subset n\mathbb{Z}$



Ainsi, les ss-gr de $(\mathbb{Z},+)$ sont $\{0\}$ et $n\mathbb{Z}$ ($n \in \mathbb{N}$)

si $\operatorname{Ker}\varphi_a = \{0\}$, on dit que a est d'ordre infini
si $\operatorname{Ker}\varphi_a \neq \{0\}$ a est d'ordre fini.

* si a est d'ordre infini : $\operatorname{Ker}\varphi_a = \{0\}$, φ_a est injective, donc réalise un isomorphisme du gr. $(\mathbb{Z},+)$ sur $\operatorname{Im}\varphi_a$
$\operatorname{Im}\varphi_a$ est isomorphe à $(\mathbb{Z},+)$
en particulier, $\operatorname{Im}\varphi_a = \{a^k, k \in \mathbb{Z}\}$ est infini
(tous les gr. monogènes non cycliques sont isomorphes à $(\mathbb{Z},+)$)

* si a est d'ordre fini, $a \neq e$:
$\exists n_a \in \mathbb{N}^* / \operatorname{Ker}\varphi_a = n_a\mathbb{Z}$ $n_a = \min\{n \in \mathbb{N}^* / a^n = e\}$: $a^{n_a} = e$
$a^1 \neq e$ donc $n_a > 1$
• si $k \in \{1, \dots, n_a - 1\}$, $a^k \neq e$
• $(r_1, r_2) \in \{0, \dots, n_a - 1\}^2$, $a^{r_1} = a^{r_2} \iff a^{r_1 - r_2} = e \iff r_1 - r_2 \in \operatorname{Ker}\varphi_a$
$\iff r_1 - r_2 \in n_a\mathbb{Z}$
$a^{r_1} = a^{r_2} \iff r_1 = r_2$
or, $r_1 - r_2 \in \{-n_a + 1, n_a - 1\}$
donc $r_1 - r_2 \in \{-n_a + 1, n_a - 1\} \cap n_a\mathbb{Z}$
donc $r_1 - r_2 = 0$ d'où $r_1 = r_2$
• $\{a^0, \dots, a^{n_a - 1}\}$ a exactement n éléments
$\forall k \in \mathbb{Z}$, $\exists q \in \mathbb{Z}$, $\exists r \in \{0, \dots, n_a - 1\} / k = qn_a + r$
$\varphi_a(k) = a^{qn_a + r} = (a^{n_a})^q a^r = a^r$
donc $\operatorname{Im}\varphi_a = \{e, a^1, \dots, a^{n_a - 1}\}$
groupe cyclique de générateur a de cardinal (ordre) n_a
• $\forall m \in \mathbb{Z}$, $a^m \in \operatorname{Im}\varphi_a$,
a^m générateur de $\operatorname{Im}\varphi_a \iff m$ premier avec n_a

• On suppose a^m générateur de $\operatorname{Im}\varphi_a$
$\exists u \in \mathbb{Z} / (a^m)^u = a^1 \to a^{mu} = a^1 \to a^{mu - 1} = e$
$\to mu - 1 \in \operatorname{Ker}\varphi_a = n_a\mathbb{Z}$
$\exists v \in \mathbb{Z} / mu - 1 = n_a v$
$\exists (u,v) \in \mathbb{Z}^2 / mu - n_a v = 1 \to \operatorname{pgcd}(m, n_a) = 1$
• On suppose m et n_a premiers entre eux (Bezout)

$\exists (u,v) \in \mathbb{Z}^2$ / $mu + n_a v = 1$ $\rightarrow$ $a^{mu} = a$ $\rightarrow (a^m)^u (a^{n_a})^v = a$

$\forall k \in \mathbb{Z}$, $a^k = (a^m)^{uk}$ donc a^m est un générateur de $\mathrm{Im}\,\varphi_a$ $\Rightarrow (a^m)^u = a$

* si $a = e$:

$\begin{cases} \mathrm{Ker}\,\varphi_a = \mathbb{Z} \\ \mathrm{Im}\,\varphi_a = \{e\} \end{cases}$ a est d'ordre 1

Pp 1) si G est un gr. fini, alors tous les éléments de G sont d'ordre fini

Pp 2) l'ordre d'un élément divise l'ordre du groupe :

$\begin{cases} G \text{ groupe fini d'ordre } n \ (\mathrm{Card}\, G = n) \\ a \in G, \ a \text{ d'ordre } n_a \end{cases} \rightarrow n_a \mid n$

on définit $\mathcal{R}$:

$H = \mathrm{Im}\,\varphi_a = \{e, a, a^2, \dots, a^{n_a - 1}\}$

- $\mathcal{R}$ relation binaire dans G :

$x \mathcal{R} y \Leftrightarrow xy^{-1} \in H \Leftrightarrow \exists h \in H \ / \ xy^{-1} = h$

$\Leftrightarrow x = hy$

donc $\exists \ h \in H \ / \ y = hx$ $(x \leftrightarrow y)$

- $\mathcal{R}$ réflexive : $\forall x \in G$, $x = ex$: $x \mathcal{R} x$

symétrique : $\forall (x,y) \in G^2$, $x \mathcal{R} y \Leftrightarrow \exists h \in H \ / \ y = xh$

$\Rightarrow \exists h^{-1} \in H \ / \ yh^{-1} = x$ donc $y \mathcal{R} x$

transitive, $\forall (x,y,z) \in G^3$,

$x \mathcal{R} y$ et $y \mathcal{R} z \rightarrow \exists (h_1, h_2) \in H^2 / \begin{cases} y = xh_1 \\ z = yh_2 \end{cases}$

donc $z = x(h_1 h_2)$ donc $x \mathcal{R} z$

donc $\mathcal{R}$ est une relation d'équivalence

- $\forall x \in G$, $Cl(x) = \{y \ / \ x \mathcal{R} y\} = \{hx \ / \ h \in H\}$

$\varphi : \begin{vmatrix} H \rightarrow \\ h \mapsto hx \end{vmatrix}$

φ est surjective (par construction)

injective. $\forall (h_1, h_2) \in H^2$, $\varphi(h_1) = \varphi(h_2)$

$\rightarrow h_1 x = h_2 x \rightarrow h_1 = h_2$

donc φ est bijective

$\mathrm{Card}(Cl(x)) = \mathrm{Card}\, H = n_a$: toutes les classes ont le même ordre n_a

s'il y a q classes : $q \cdot n_a = n$ d'où $n_a \mid n$

Pp 3) si $\begin{cases} G \text{ groupe fini d'ordre } n \\ a \in G \end{cases}$ alors $a^n = e$

$a^n = a^{q n_a} = (a^{n_a})^q = e$

6- groupes cycliques

Pp 1) Tout groupe cyclique d'ordre n est isomorphe à U_n

$U_n = \{1, e^{2i\pi/n}, e^{4i\pi/n}, \dots, e^{2(n-1)i\pi/n}\}$, G groupe cyclique de générateur a

$G = \{e, a, a^2, \dots, a^{n-1}\}$

soit $\varphi : G \rightarrow U_n$

- φ est bijective
- $\forall (k,k') \in \{0, \dots, n-1\}^2$ (avec $r = k + k'$)

$\varphi(a^k a^{k'}) = \varphi(a^{k+k'}) = \varphi(a^r) = e^{2ir\pi/n}$

$= e^{2i(k+k')\pi/n} = e^{2ik\pi/n} e^{2ik'\pi/n} = \varphi(a^k)\varphi(a^{k'})$

conséquence : Tout groupe cyclique est commutatif

car isomorphe à un gr. commutatif U_n

Pp 2) Tout sous-groupe d'un groupe cyclique est cyclique

$n \in \mathbb{N}^*$ H ss-gr. d'ordre d de U_n

$\forall s \in H$, $s^d = 1$ donc $s \in U_d$ donc $H \subset U_d$

$\varphi_\omega : \mathbb{Z} \to U_n$, $k \mapsto \omega^k$, $\varphi_\omega(n) = \omega^n = 1$

or $\text{card } H = d = \text{card } U_d$ d'où $H = U_d$

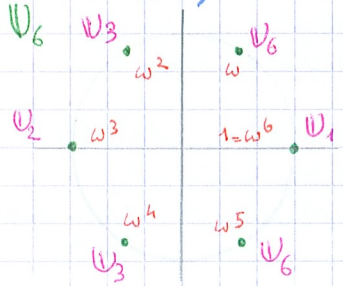
soit ω un générateur de $U_d \subset U_n$: $\omega^d = 1$

$n \in \text{Ker } \varphi_\omega$ l'ordre de ω divise n : $d \mid n$ $\quad n \in d\mathbb{Z} = \text{Ker } \varphi_\omega$

Pp 3) soit G un gr. cyclique d'ordre n, de générateur a,

$\forall r \in \mathbb{Z}$, a^r générateur de $G \iff n \wedge r = 1$

ex : U_6



U_6 a 2 générateurs, ω^1 et ω^5

entiers 1ers avec 6 dans $\{0,1,\dots,5\}$: 1 et 5

groupe engendré

puissance

$\Rightarrow$ a^r générateur de G : $\exists u \in \mathbb{Z} / (a^r)^u = a^1 \iff a^{ru-1} = e$

$\exists v \in \mathbb{Z} / ru - 1 = nv \iff ru - nv = 1 \iff r \wedge n = 1$

$\Leftarrow$ si $r \wedge n = 1$, alors $\exists (u,v) \in \mathbb{Z}^2 / ru - nv = 1$

alors, $(a^r)^u = a^{nv+1} = (a^n)^v a = a$

$\forall k \in \mathbb{Z}$, $a^{ruk} = a^k$

Pp 4) si $\begin{cases} p \text{ est un nombre premier} \\ G \text{ est un groupe d'ordre } p \end{cases}$ alors G est un groupe cyclique

soit $a \in G$, $a \neq e$, l'ordre de a divise p

or p est premier, donc l'ordre de a est 1 ou p

ce n'est pas 1 (au moins 2 éléments dans le ss-groupe : a, e)

l'ordre est donc p

donc le ss. gr engendré par a est G

III. Anneaux

A ensemble muni de 2 l.c.i. $+, \times$,

$(A, +, \times)$ anneau $\iff$ $\begin{cases} (A,+) \text{ groupe commutatif} \\ \times \text{ associative} \\ \times \text{ distributive / } + \text{ (à droite et à gauche)} \\ \times \text{ possède un neutre} \end{cases}$

$(A,+,\times)$ commutatif si $\times$ commutative

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

$\mathbb{Z}[X]$ $\mathbb{Q}[X]$ $\mathbb{R}[X]$ $\mathbb{C}[X]$

$\mathbb{R}^{\mathbb{N}}$, $\mathbb{R}^I$ $\mathbb{C}^{\mathbb{N}}$ I intervalle

A^X A anneau, X ensemble non vide

non commutatifs : $(\mathcal{L}(E), +, \circ)$, $(\mathcal{M}_n(K), +, \times)$

1. morphismes d'anneaux

$\varphi : A \to A'$ morphisme d'anneaux $\iff$ $\forall (x,x') \in A^2$, $\begin{cases} \varphi(x+x') = \varphi(x) + \varphi(x') \\ \varphi(x \times x') = \varphi(x) \times \varphi(x') \\ \varphi(1_A) = 1_{A'} \end{cases}$

2. sous-anneaux

B sous-anneau de A $\iff$ $\begin{cases} \bullet\ B \subset A \\ \bullet\ \forall (x,x') \in B^2, \begin{cases} x - x' \in B \\ x x' \in B \end{cases} \\ \bullet\ 1_A \in B \quad (\text{donc } B \neq \emptyset) \end{cases}$

alors B est un anneau

3. éléments inversibles

$x \in A$, x inversible $\iff$ $\exists (x,x') \in A^2 / \ x x' = x'' x = 1_A$

rem : dans ce cas, $(x'' x) x' = x''(x x')$

$\iff 1_A x' = x'' 1_A$ d'où $x' = x''$

U_A : ensemble des éléments inversibles de A

Pp) $(U_A, \times)$ est un groupe

- $1_A \in U_A$
- si $(x,y) \in U_A^2$, $\exists (x',y') \in A^2$ / $xx' = x'x = 1_A$, $yy' = y'y = 1_A$
  donc $(xy)(y'x') = x(yy')x' = xx' = 1_A$
  $(y'x')(xy) = y'(x'x)y = y'y = 1_A$
  donc $xy \in U_A$
  $\times$ est une l.c.i associative dans U_A
- si $x \in U_A$, $\exists x' \in A$ / $xx' = x'x = 1_A$
  donc $x' \in U_A$: x possède un inverse dans U_A

$U_{\mathbb{Z}} = \{-1, 1\}$ $U_{\mathbb{R}} = \mathbb{R}^*$ $U_{\mathbb{R}[X]}$ = ensemble des polynômes de degré 0 $= \mathbb{R}^*$

$U_{\mathcal{L}(E)} = GL(E)$ $U_{M_n(\mathbb{R})} = GL(n, \mathbb{R})$

4- diviseurs de zéro

$x \in A$, x diviseur de zéro à droite :
si $x \neq 0$, $\exists y \in A$, $y \neq 0$ / $yx = 0$

rem : Les éléments inversibles ne sont pas diviseur de zéro

x inversible, d'inverse x',
$\forall y \in A$, $yx = 0 \Rightarrow yxx' = 0 \Rightarrow y = 0$
$xy = 0 \Rightarrow x'xy = 0 \Rightarrow y = 0$

ex * pas de diviseur de zéro dans $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$

* $\mathbb{R}^{[-1,1]}$, $f : [-1,1] \to \mathbb{R}$, $x \mapsto \frac{1}{2}(x + |x|)$

$g : [-1,1] \to \mathbb{R}$, $x \mapsto \frac{1}{2}(x - |x|)$

$\forall x \in [-1,1]$,
$f(x)g(x) = \frac{1}{4}(x + |x|)(x - |x|)$
$= \frac{1}{4}(x^2 - |x|^2) = 0$

5- anneaux intègres

$(A, +, \times)$ intègre $\Leftrightarrow$ A commutatif et sans diviseur de zéro

ex : $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, $\mathbb{R}[X]$, $\mathbb{Q}[X]$

IV Idéaux dans un anneau commutatif

1-

$(A, +, \times)$ anneau commutatif, $I \subset A$,
I idéal de A $\Leftrightarrow$ $\begin{cases} (I, +) \text{ ss-groupe de } (A, +) \\ \forall x \in I, \forall a \in A, \quad xa \in I \end{cases}$

ex : $\{0\}$, A

$A = \mathbb{R}^{[-1,1]}$, $I = \{f \in A / f(0) = 0\}$

* $I \subset A$
- $0_A \in I$ donc $I \neq \emptyset$
- $\forall (f,g) \in I^2$, $(f-g)(0) = f(0) - g(0) = 0$ donc $f - g \in I$
* $\forall f \in I$, $\forall h \in A$, $(fh)(0) = f(0)h(0) = 0$ donc $fh \in I$

$\Big\}$ $(I, +)$ ss-gr. de $(A, +)$

Pp) φ morphisme de A dans A' $\Rightarrow$ $\ker \varphi$ idéal de A

le noyau d'un morphisme est un idéal

- φ morphisme du groupe $(A, +)$ dans $(A', +)$
  donc $\ker \varphi$ est un ss-gr. de $(A, +)$
- $\forall x \in \ker \varphi$, $\forall a \in A$, $\varphi(ax) = \varphi(a)\varphi(x) = \varphi(a) \times 0 = 0$: $ax \in \ker \varphi$

2- critère

I idéal de A $\Leftrightarrow$ $\begin{cases} I \subset A \\ I \neq \emptyset \\ \forall (x,y) \in I^2, \forall (a,b) \in A^2, \quad ax + by \in I \end{cases}$

on peut prendre $b' = -b$

Pp 1) A anneau, I idéal de A, $1_A \in I \Rightarrow I = A$

$1_A \in I$, $\forall a \in A$, $1_A \times a = a \in I$: $A \subset I$ or $I \subset A$

Pp 2) I, J idéaux de A, $I \cap J$ est un idéal de A
$I + J = \{x+y / x \in I, y \in J\}$

- $I \cap J$ est un gr
  $\forall x \in I \cap J, \forall a \in A, \begin{cases} ax \in I \text{ donc } ax \in I \cap J \\ ax \in J \end{cases}$
- s-gr de $(A,+)$
  - $I + J \subset A$
  - $I + J \neq \emptyset$
  - $\forall (z,z') \in (I+J)^2, \exists (x,x',y,y') \in I^2 \times J^2 \;/\; z = x+y,\ z' = x'+y'$
    $z - z' = x + y - x' - y' = (x - x') + (y - y') \in I + J$
  - $\forall z \in I+J, \forall a \in A, az = a(x+y) = ax + ay \in I + J$

3. Idéal principal

Pp) $\begin{cases} A \text{ anneau commutatif} \\ x \in A \\ I = \{ax / a \in A\} \end{cases}$ alors $\begin{cases} I \text{ idéal} \\ x \in I \\ I \text{ est le plus petit idéal de } A \text{ contenant } x \end{cases}$

- $I \subset A$
- $I \neq \emptyset$ $(x \in I)$
- $\forall (z,z') \in I^2, \exists (a,a') \in A^2 \;/\; z = ax,\ z' = a'x$
  $z - z' = ax - a'x = (a - a')x \in I$
- $\forall z \in I, \forall b \in A, bz = bax \in I$

x générateur de I : $I = xA$
I idéal principal $\iff \exists x \in A \;/\; I = xA$ (il doit y avoir un unique générateur)

rem: $\forall (x,y) \in A^2, J = \{ax + by / (a,b) \in A^2\} = xA + yA$
J est un idéal, pas forcément principal.

4. Divisibilité

A anneau intègre

Pp 1) $\forall (x,y) \in A^2$, $(\exists a \in A \;/\; y = ax) \iff$ (multiple de ya / de xa) $yA \subset xA$
alors $x \mid y$

- $\Rightarrow$ $\forall z \in yA, \exists b \in A \;/\; z = yb = axb = x \underbrace{ab}_{\in A} \in xA$
- $\Leftarrow$ $y \in yA$ $(y = y1_A)$
  donc $y \in xA$
  donc $\exists a \in A \;/\; y = xa = ax$

Pp 2) $\forall (x,y,z,a,b) \in A^5$, $\begin{cases} x \mid y \\ x \mid z \end{cases} \Rightarrow x \mid ay + bz$

$\begin{cases} yA \subset xA \\ zA \subset xA \end{cases} \Rightarrow \begin{cases} ayA \subset yA \subset xA \\ bzA \subset zA \subset xA \end{cases} \Rightarrow ayA + bzA \subset xA$
$(ay + bz)A \subset ayA + bzA \subset xA$
donc $x \mid ay + bz$

La relation binaire "divise" est réflexive, transitive, en général ni symétrique, ni antisymétrique

Pp 3) $\forall (x,y) \in A^2$, les propositions suivantes sont équivalentes :
(1) $x \mid y$ et $y \mid x$
(2) $\exists u \in U_A \;/\; y = ux$
(3) $xA = yA$ (x, y engendrent le même idéal principal)

dans ce cas, x et y sont associés

- si $x = y = 0$, vrai
- on suppose $x \neq 0$, $y \neq 0$

(1) $\Rightarrow$ (2) : si $x \mid y$ et $y \mid x$ $\exists (a,b) \in A^2 \;/\; y = ax,\ x = by$
donc $y = aby \iff y(1 - ab) = 0$
or $y \neq 0$ donc $1 = ab$ donc a est inversible
d'où $a \in U_A$, $y = ax$

(2) $\Rightarrow$ (3) : on suppose $y = ux$ avec $u \in U_A$,
$\forall z \in yA, \exists a \in A \;/\; z = ya$

donc $z = ux a = ua\,x \in x\mathbb{A}$ d'où $u\mathbb{A} \subset x\mathbb{A}$

soit $u' \in \mathbb{A}$ / $uu' = 1_{\mathbb{A}}$, $y = ux \Rightarrow u'y = x$ avec $u' \in \mathbb{A}$ d'où $x\mathbb{A} \subset y\mathbb{A}$

• (3) $\Rightarrow$ (1) : $x\mathbb{A} = y\mathbb{A} \Rightarrow \begin{cases} y \in x\mathbb{A} \\ x \in y\mathbb{A} \end{cases} \Rightarrow \begin{cases} y \mid x \\ x \mid y \end{cases}$

I $\mathbb{Z}$

• élts inversible de $\mathbb{Z}$: $U_{\mathbb{Z}} = \{-1, 1\}$

• soit I un idéal de $\mathbb{Z}$, $\exists ! n \in \mathbb{N}$ / $I = n\mathbb{Z}$

I est un ss-gr. donc $\exists ! n \in \mathbb{N}$ / $I = n\mathbb{Z}$

$n\mathbb{Z}$ est un idéal principal

n est le générateur positif de I

si $n \neq 0$, $-n$ est l'autre générateur

• I est l'ensemble des multiples de n

• Tous les idéaux de $\mathbb{Z}$ sont principaux : $\mathbb{Z}$ est un anneau principal

PGCD

• soit $(n, m) \in \mathbb{Z}^2$,

→ $n\mathbb{Z} + m\mathbb{Z}$ est un idéal de $\mathbb{Z}$, de générateur positif d

$\begin{cases} n\mathbb{Z} \subset d\mathbb{Z} \\ m\mathbb{Z} \subset d\mathbb{Z} \end{cases} \Rightarrow \begin{cases} d \mid n \\ d \mid m \end{cases}$ d est un diviseur commun de m et n

→ soit δ un diviseur de d

$d\mathbb{Z} \subset \delta\mathbb{Z} \Rightarrow \begin{cases} n\mathbb{Z} \subset \delta\mathbb{Z} \\ m\mathbb{Z} \subset \delta\mathbb{Z} \end{cases}$ δ est un diviseur commun de m et n

→ soit δ un diviseur commun de m et n

$\begin{cases} n\mathbb{Z} \subset \delta\mathbb{Z} \\ m\mathbb{Z} \subset \delta\mathbb{Z} \end{cases} \Rightarrow n\mathbb{Z} + m\mathbb{Z} \subset \delta\mathbb{Z} \Rightarrow d\mathbb{Z} \subset \delta\mathbb{Z} \Rightarrow \delta \mid d$

l'ensemble des diviseurs communs de m et n est l'ensemble des diviseurs de d :

$d = pgcd(n, m) = n \wedge m$

PPCM

• → $n\mathbb{Z} \cap m\mathbb{Z}$ est un idéal de $\mathbb{Z}$, de générateur positif μ

$\begin{cases} \mu \in n\mathbb{Z} \\ \mu \in m\mathbb{Z} \end{cases}$ μ : multiple commun de m et n

→ soit ν un multiple de μ

$\nu \in \mu\mathbb{Z} \Rightarrow \begin{cases} \nu \in n\mathbb{Z} \\ \nu \in m\mathbb{Z} \end{cases}$ ν : multiple commun de m et n

→ soit ν un multiple commun de m et n

$\begin{cases} \nu \in n\mathbb{Z} \\ \nu \in m\mathbb{Z} \end{cases} \Rightarrow \nu \in n\mathbb{Z} \cap m\mathbb{Z} \Rightarrow \nu \in \mu\mathbb{Z}$: ν multiple de μ

$\mu\mathbb{Z}$: ensemble des multiples communs de m et n

$\mu = ppcm(n, m) = n \vee m$

corollaires : <u>relation de Bezout</u>

$\forall (n, m) \in \mathbb{Z}^2$, $d = n \wedge m$, $\exists (u, v) \in \mathbb{Z}^2$ / $d = nu + mv$

$(d \in d\mathbb{Z} = n\mathbb{Z} + m\mathbb{Z})$

<u>Th de Bezout</u>

$\forall (n, m) \in \mathbb{Z}^2$, <u>n, m premiers entre eux</u> $\Leftrightarrow \exists (u, v) \in \mathbb{Z}^2$ / $nu + mv = 1$

<u>th de Gauss</u>

soit $(n, m, x) \in \mathbb{Z}^3$ $\begin{cases} x \wedge n = 1 \\ x \mid nm \end{cases} \Rightarrow x \mid m$

$x \mid nm \Rightarrow \exists a \in \mathbb{Z}$ / $ax = nm$

$x \wedge n = 1 \Rightarrow \exists (b, c) \in \mathbb{Z}^2$ / $xb + nc = 1$

donc $cax = cnm \Rightarrow cax = (1 - bx)m$

$\Leftrightarrow$ <u>$(ca + bm)x = m$</u>

VI $\mathbb{K}[X]$

- él/mts inversibles $\mathbb{K}[X]$: $U_{\mathbb{K}[X]} = \mathbb{K}^*$
- soit I un idéal de $\mathbb{K}[X]$, avec $I \neq \{0\}$,
  $\exists !$ polynôme unitaire P / $I = P\mathbb{K}[X]$ (anneau principal)

  - soit $A = \{n \in \mathbb{N} / \exists Q \in I$ avec $\deg Q = n\}$
    $A \subset \mathbb{N}$
    $A \neq \emptyset$ ($I \neq \{0\}$, $\exists Q \in I$ avec $\deg Q \in \mathbb{N}$, $\deg Q \in A$)
    une partie non vide de $\mathbb{N}$ a un plus petit élément : n_0
    $\exists Q \in I$ avec $\deg Q = n_0$ et $\forall P \in I$, $P \neq 0 \Rightarrow \deg P \geq n_0$
    soit $H \in I$ unitaire,
    $\exists (S,R) \in \mathbb{K}[X]^2$, $H = SQ + R$ avec $\deg R < \deg Q = n_0$
    $R = \underbrace{H - SQ}_{\in I}$
    donc $\begin{cases} R \in I \\ \deg R < n_0 \end{cases}$ donc $R = 0$ d'où $H = SQ \in Q\mathbb{K}[X]$
    d'où $I \subset Q\mathbb{K}[X]$
    or, $Q \in I$ donc $Q\mathbb{K}[X] \subset I$
    Ainsi, $I = Q\mathbb{K}[X]$: Q est un générateur de I
  - Les générateurs de I sont tous les él/mts associés :
    λQ avec $\lambda \in \mathbb{K}^*$
    $P = \underbrace{\frac{1}{\text{coeff. dominant}}}\, Q$ P est le seul générateur unitaire de I

rem : si $I = \{0\}$, $P = 0$

soit $(P,Q) \in \mathbb{K}[X]^2$,

PGCD • $P\mathbb{K}[X] + Q\mathbb{K}[X]$ est un idéal de $\mathbb{K}[X]$, de générateur unitaire D
D est l'ensemble des diviseurs de D est l'ensemble des diviseurs communs de P et Q. $D = P \wedge Q$

PPCM • $P\mathbb{K}[X] \cap Q\mathbb{K}[X]$ est un idéal de $\mathbb{K}[X]$, de générateur unitaire M
l'ensemble des multiples de M est l'ensemble des multiples communs de P et Q. $M = P \vee Q$

corollaires : P, Q 2 polynômes premiers entre eux
$\exists ! (U,V) \in \mathbb{K}[X]^2$ / $\begin{cases} UP + VQ = 1 \\ \deg U < \deg Q \\ \deg V < \deg P \end{cases}$

unicité soit $((U,V),(U_1,V_1)) \in (\mathbb{K}[X]^2)^2$ / $UP + VQ = 1$, $U_1P + V_1Q = 1$
$\begin{cases} \deg U < \deg Q \\ \deg V < \deg P \end{cases}$ $\begin{cases} \deg U_1 < \deg Q \\ \deg V_1 < \deg P \end{cases}$

$(U - U_1)P = (V_1 - V)Q$
Th de Gauss : $\begin{cases} P \mid (V_1 - V)Q \\ P \wedge Q = 1 \end{cases}$ donc $P \mid V_1 - V$
or, $\deg(V_1 - V) < \max\{\deg V_1, \deg V\} < \deg P$ donc $V_1 - V = 0$
d'où $V_1 = V$ d'où $U_1 = U$

existence Bezout : $\exists (U_1,V_1) \in \mathbb{K}[X]^2$ / $U_1P + V_1Q = 1$
*division euclidienne
$\begin{cases} U_1 = AQ + U \\ V_1 = BP + V \end{cases}$ $\Leftrightarrow$ $1 = (AQ+U)P + (BP+V)Q = (A+B)PQ + UP + VQ$
si $A + B \neq 0$, $\deg(A+B)PQ = \deg(A+B) + \deg P + \deg Q \geq \deg P + \deg Q$
or $\deg(\underbrace{UP + VQ}_{1}) < \deg P + \deg Q$ $\Leftrightarrow$ $\deg P + \deg Q > 0$
et $\deg 1 = \deg[(A+B)PQ + UP + VQ] \geq \deg P + \deg Q$
d'où $\deg P + \deg Q \leq 0$ impossible

VII $\mathbb{Z}/n\mathbb{Z}$ $n \in \mathbb{N}^*$

1.- congruence

$(p,q) \in \mathbb{Z}^2$ p congru à q modulo n $\Leftrightarrow$ $p - q \in n\mathbb{Z}$
$p \equiv q\ [n]$ $\Leftrightarrow$ $\exists k \in \mathbb{Z}$ / $p - q = nk$

La congruence est une relation d'équivalence

2- classe d'équivalence

$\mathbb{Z}$ est partitionné en classes d'équivalence

p et q appartiennent à la **même classe** $\Leftrightarrow$ $p \equiv q\ [n]$

notation : $\bar{p}$: classe de p

$$\bar{p} = \{ q \in \mathbb{Z} / p \equiv q\ [n] \} = \{ p + nk / k \in \mathbb{Z} \}$$

$\bar{p} \in \mathbb{Z}$

p est un représentant de $\bar{p}$

$\forall (p,q) \in \mathbb{Z}^2$, $(\bar{p} = \bar{q}$ ou $\bar{p} \cap \bar{q} = \emptyset)$

$(p \equiv q\ [n])$ $(p \not\equiv q\ [n])$

3- représentants

soit $p \in \mathbb{Z}$, $\exists k \in \mathbb{Z}$, $\exists r \in \{0, \dots, n-1\}$ / $p = nk + r$ alors $p \equiv r\ [n]$

$\Leftrightarrow$ $\bar{p} = \bar{r}$

donc il y a au plus n classes (r prend n valeurs)

$\forall (r_1, r_2) \in \{0, \dots, n-1\}^2$, $\bar{r_1} = \bar{r_2} \Leftrightarrow r_1 \equiv r_2\ [n] \Leftrightarrow r_1 - r_2 \in n\mathbb{Z}$

$\in \{-n+1, -n+2, \dots 0, 1, \dots n-1\}$

$\Leftrightarrow r_1 - r_2 = 0 \Leftrightarrow r_1 = r_2$

donc il y a au moins n classes

Ainsi, il y a **n classes** et chacune a un représentant dans $\{0, \dots, n-1\}$

4- notations

a- $\mathbb{Z}/n\mathbb{Z}$: ensemble des classes d'équivalence

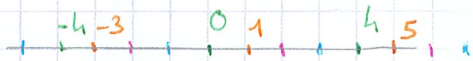
$= \{ \bar{0}, \bar{1}, \bar{2}, \dots, \overline{n-1} \}$

$\mathbb{Z}/2\mathbb{Z} = \{ \bar{0}, \bar{1} \}$

ensemble des nombres pairs

impairs

$\mathbb{Z}/4\mathbb{Z} = \{ \bar{0}, \bar{1}, \bar{2}, \bar{3} \}$



$\bar{0} = 4\mathbb{Z}$

$\bar{1} = \{4k+1 / k \in \mathbb{Z}\}$

b- opérations

* addition : $\begin{cases} p' \equiv p\ [n] \\ q' \equiv q\ [n] \end{cases} \Rightarrow \exists (k_1, k_2) \in \mathbb{Z}^2 / \begin{cases} p' = p + k_1 n \\ q' = q + k_2 n \end{cases}$

$\Rightarrow \exists k \in \mathbb{Z} / p' + q' = p + q + kn \Rightarrow p' + q' \equiv p + q\ [n]$

autrement dit : $\begin{cases} \bar{p} = \bar{p'} \\ \bar{q} = \bar{q'} \end{cases} \Rightarrow \overline{p+q} = \overline{p'+q'}$

l'addition est compatible avec la relation d'équivalence

on pose $\bar{p} + \bar{q} = \overline{p+q}$ (indépendant du représentant)

On munit $\mathbb{Z}/n\mathbb{Z}$ d'une l.c.i $+$.

$(\mathbb{Z}/n\mathbb{Z}, +)$ est un groupe abélien

- $+$ l.c.i
- $+$ associative :

$(\bar{p} + \bar{q}) + \bar{r} = \overline{p+q} + \bar{r} = \overline{(p+q)+r} = \overline{p+(q+r)} = \bar{p} + \overline{q+r}$

$= \bar{p} + (\bar{q} + \bar{r})$

- $+$ commutative :

$\bar{p} + \bar{q} = \overline{p+q} = \overline{q+p} = \bar{q} + \bar{p}$

- neutre : $\bar{0}$
- symétrique : $-\bar{p}$

* multiplication : ... $\exists (k_1, k_2) \in \mathbb{Z}^2 / p'q' = pq + pk_2 n + qk_1 n + k_1 k_2 n^2$

$p'q' = pq + [pk_2 + qk_1 + k_1 k_2 n]n$

donc $p'q' \equiv pq\ [n]$

autrement dit : $\overline{pq} = \overline{p'q'}$ donc $\bar{p}\,\bar{q} = \overline{pq}$

la multiplication est compatible avec la relation d'équivalence.

On munit $\mathbb{Z}/n\mathbb{Z}$ d'une l.c.i $\cdot$.

$(\mathbb{Z}/n\mathbb{Z}, +, \cdot)$ est un anneau commutatif

tables : $\mathbb{Z}/2\mathbb{Z}$

+	$\bar{0}$	$\bar{1}$
$\bar{0}$	$\bar{0}$	$\bar{1}$
$\bar{1}$	$\bar{1}$	$\bar{0}$

·	$\bar{0}$	$\bar{1}$
$\bar{0}$	$\bar{0}$	$\bar{0}$
$\bar{1}$	$\bar{0}$	$\bar{1}$

$\mathbb{Z}/4\mathbb{Z}$

+	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$
$\bar{0}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$
$\bar{1}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{0}$
$\bar{2}$	$\bar{2}$	$\bar{3}$	$\bar{0}$	$\bar{1}$
$\bar{3}$	$\bar{3}$	$\bar{0}$	$\bar{1}$	$\bar{2}$

·	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$
$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$
$\bar{1}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$
$\bar{2}$	$\bar{0}$	$\bar{2}$	$\bar{0}$	$\bar{2}$
$\bar{3}$	$\bar{0}$	$\bar{3}$	$\bar{2}$	$\bar{1}$

$\bar{2}$ est diviseur de zéro

c. projection canonique

$\pi_n : \mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$, $p \mapsto \bar{p}$

$\forall (p,q) \in \mathbb{Z}^2$, $\begin{cases} \pi_n(p+q) = \bar{p+q} = \bar{p}+\bar{q} = \pi_n(p)+\pi_n(q) \\ \pi_n(pq) = \bar{pq} = \bar{p}\,\bar{q} = \pi_n(p)\,\pi_n(q) \\ \pi_n(1) = \bar{1} \end{cases}$

π_n est un morphisme d'anneaux

- π_n est surjectif : chaque classe a au moins 1 représentant
- non injectif : $\mathbb{Z}/n\mathbb{Z}$ est fini alors que $\mathbb{Z}$ est infini
- $\operatorname{Ker}\pi_n = \{nk / k \in \mathbb{Z}\} = \bar{0} = n\mathbb{Z}$ ($\bar{0} \in \mathbb{Z}$)

d. factorisation des morphismes d'anneaux (de $\mathbb{Z}$ dans A)

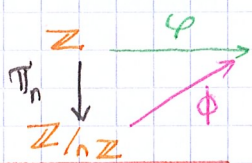
$\bar{x} \in \pi_n(A) \Leftrightarrow x \in A$

th

A un anneau

$\varphi : \mathbb{Z} \to A$ morphisme d'anneaux

on suppose $n\mathbb{Z} \subset \operatorname{Ker}\varphi$



alors, $\exists ! \Phi : \mathbb{Z}/n\mathbb{Z} \to A$ avec $\begin{cases} \Phi \text{ morphisme d'anneaux} \\ \varphi = \Phi \circ \pi_n \end{cases}$

- $\forall x \in \mathbb{Z}/n\mathbb{Z}$, $\forall (a,b) \in \mathbb{Z}^2$, $\bar{a-b} = x \to a = b\ [n]$ (2 représentants)
  $\to a-b \in n\mathbb{Z} \subset \operatorname{Ker}\varphi$
  $\to \varphi(a-b) = 0$ (φ morphisme)
  $\to \varphi(a) = \varphi(b)$ ne dépend que de la classe de même image

On pose : $\Phi(x) = \varphi(a)$

On définit : $\Phi : \mathbb{Z}/n\mathbb{Z} \to A$

$\Phi(x) = \Phi(\bar{a}) = \Phi(\pi_n(a))$

$\varphi(a) = (\Phi \circ \pi_n)(a) = \Phi(x)$ Φ est unique

et $\varphi = \Phi \circ \pi_n$

- $\forall (x,y) \in (\mathbb{Z}/n\mathbb{Z})^2$, $\exists a \in x$, $\exists b \in y$! ($a+b \in x+y$, $ab \in xy$)

$\begin{cases} \Phi(x+y) = \varphi(a+b) = \varphi(a)+\varphi(b) = \Phi(x)+\Phi(y) \\ \Phi(xy) = \varphi(ab) = \varphi(a)\varphi(b) = \Phi(x)\Phi(y) \\ \Phi(1) = \varphi(1) = 1_A \end{cases}$

donc Φ est un morphisme d'anneaux

Pp 1) $\operatorname{Ker}\Phi = \pi_n(\operatorname{Ker}\varphi)$

$\forall x \in \mathbb{Z}/n\mathbb{Z}$, $x \in \operatorname{Ker}\Phi \Leftrightarrow \Phi(x) = 0_A \Leftrightarrow (\forall a \in x,\ \varphi(a) = 0)^* \Leftrightarrow x \subset \operatorname{Ker}\varphi \Leftrightarrow x \in \pi_n(\operatorname{Ker}\varphi)$

$\therefore \operatorname{Ker}\Phi \subset \pi_n(\operatorname{Ker}\varphi)$

et $\pi_n(\operatorname{Ker}\varphi) \subset \operatorname{Ker}\Phi$: $\bar{x} \in \pi_n(\operatorname{Ker}\varphi) \Leftrightarrow x \in \operatorname{Ker}\varphi \Leftrightarrow \varphi(x) = 0 = \Phi(x) \Leftrightarrow x \in \operatorname{Ker}\Phi$

* pr $\forall a \in x$, on doit avoir $a \in \operatorname{Ker}\varphi$ donc si $x \subset \operatorname{Ker}\varphi$, $a \in x \subset \operatorname{Ker}\varphi$

Pp 2) Φ injective $\Leftrightarrow$ $n\mathbb{Z} = \operatorname{Ker}\varphi$

Φ injective $\Leftrightarrow \operatorname{Ker}\Phi = \{\bar{0}\} \Leftrightarrow \pi_n(\operatorname{Ker}\varphi) = \{\bar{0}\}$

$\Leftrightarrow \operatorname{Ker}\varphi \subset n\mathbb{Z}$

par hyp., $n\mathbb{Z} \subset \operatorname{Ker}\varphi$ d'où $\operatorname{Ker}\varphi = n\mathbb{Z}$

Pp 3) $\operatorname{Im}\Phi = \operatorname{Im}\varphi$

$\pi_n(\mathbb{Z}) = \mathbb{Z}/n\mathbb{Z}$ (surjectivité de π_n)

$\Phi(\pi_n(\mathbb{Z})) = \Phi(\mathbb{Z}/n\mathbb{Z})$

$\varphi(\mathbb{Z}) = \Phi(\mathbb{Z}/n\mathbb{Z})$

$\operatorname{Im}\varphi = \operatorname{Im}\Phi$

($\varphi : \mathbb{Z} \to \varphi(\mathbb{Z})$, $\Phi : \mathbb{Z}/n\mathbb{Z} \to \Phi(\mathbb{Z}/n\mathbb{Z})$)

e. factorisation des morphismes de groupes (de $(\mathbb{Z},+)$ dans G)

idem avec $\Phi : \mathbb{Z}/n\mathbb{Z} \to G$ morphisme de groupes

f- $(\mathbb{Z}/n\mathbb{Z}, +)$

- $(\mathbb{Z}/n\mathbb{Z}, +)$ est un groupe abélien
- $\forall (a,b) \in \mathbb{Z}^2$,

$a\bar{b} = \begin{cases} \bar{b} + \bar{b} + \dots + \bar{b} & \text{si } a \geq 0 \\ -\bar{b} - \bar{b} - \dots - \bar{b} & \text{si } a < 0 \end{cases}$ (a fois)

$b\bar{a} = \begin{cases} \bar{a} + \bar{a} + \dots + \bar{a} & \text{si } b \geq 0 \\ -\bar{a} - \bar{a} - \dots - \bar{a} & \text{si } b < 0 \end{cases}$ (b fois)

$\bar{ab}$

3 classes ... ... égales

$\begin{cases} ab \in \bar{ab} \\ ab \in a\bar{b} \\ ab \in b\bar{a} \end{cases}$ donc $\bar{ab} = a\bar{b} = b\bar{a}$

$\mathbb{Z}/n\mathbb{Z} = \{\bar{1}, \bar{2}, \dots, \bar{n}\} = \{1\bar{1}, 2\bar{1}, 3\bar{1}, \dots, n\bar{1}\}$

donc $(\mathbb{Z}/n\mathbb{Z}, +)$ est un groupe cyclique, dont $\bar{1}$ est un générateur

Pp) $\varphi : \begin{cases} \mathbb{Z} \longrightarrow \mathbb{U}_n \\ k \longmapsto e^{2ik\pi/n} = (e^{2i\pi/n})^k \end{cases}$ alors, φ morphisme de groupes $(\mathbb{Z}, +)$ dans $(\mathbb{U}_n, \cdot)$

et $\ker \varphi = n\mathbb{Z}$ donc $\exists ! \Phi : \mathbb{Z}/n\mathbb{Z} \longrightarrow \mathbb{U}_n$ morphisme de groupes /

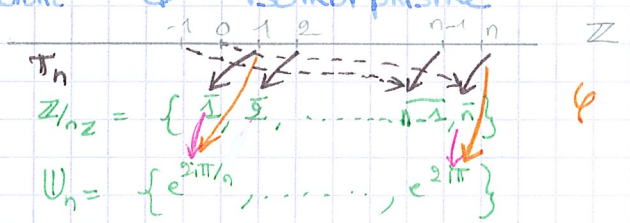
$\varphi = \Phi \circ \pi_n$

et $\ker \varphi = n\mathbb{Z} \Rightarrow \Phi$ injectif

or, $\text{Card}(\mathbb{Z}/n\mathbb{Z}) = \text{Card}(\mathbb{U}_n) = n$ donc Φ isomorphisme

$\mathbb{Z}/n\mathbb{Z} = \{\bar{1}, \bar{2}, \dots, \overline{n-1}, \bar{n}\}$

$\mathbb{U}_n = \{e^{2i\pi/n}, e^{4i\pi/n}, \dots, e^{2i\pi}\}$ Φ



application : $x \in \mathbb{Z}/n\mathbb{Z}$, r un représentant de x ($r = x$)

x générateur de $(\mathbb{Z}/n\mathbb{Z}, +)$ $\iff$ $\Phi(x)$ générateur de $\mathbb{U}_n$

$\iff$ $\varphi(r)$ ----------

$\iff$ $(e^{2i\pi/n})^r$ ----------

$\iff$ r, n 1ers entre eux

ex : $\mathbb{Z}/8\mathbb{Z} = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}, \bar{5}, \bar{6}, \bar{7}\}$

ss-gr. engendré par

$\bar{0}$: $\{\bar{0}\} \neq \mathbb{Z}/8\mathbb{Z}$

$\bar{1}$: $\{\bar{1}, \bar{2}, \bar{3}, \bar{4}, \bar{5}, \bar{6}, \bar{7}, \bar{8}\} = \mathbb{Z}/8\mathbb{Z}$

$\bar{2}$: $\{\bar{2}, \bar{4}, \bar{6}, \bar{8}\} \neq \mathbb{Z}/8\mathbb{Z}$

$\bar{3}$: $\{\bar{3}, \bar{6}, \bar{1}, \bar{4}, \bar{7}, \bar{2}, \bar{5}, \bar{8}\} = \mathbb{Z}/8\mathbb{Z}$ (1ers avec 8)

$\bar{4}$: $\{\bar{4}, \bar{8}\} \neq \mathbb{Z}/8\mathbb{Z}$

$\bar{5}$: $\{\bar{5}, \bar{2}, \bar{7}, \bar{4}, \bar{1}, \bar{6}, \bar{3}, \bar{8}\} = \mathbb{Z}/8\mathbb{Z}$

$\bar{6}$: $\{\bar{6}, \bar{4}, \bar{2}, \bar{8}\} \neq \mathbb{Z}/8\mathbb{Z}$

$\bar{7}$: $\{\bar{7}, \bar{6}, \bar{5}, \bar{4}, \bar{3}, \bar{2}, \bar{1}, \bar{8}\} = \mathbb{Z}/8\mathbb{Z}$

g- éléments inversibles

Pp) $\forall m \in \mathbb{Z}$, $\bar{m}$ inversible dans $\mathbb{Z}/n\mathbb{Z}$ (pour $\times$) $\iff$ $m \wedge n = 1$ (indépendant du représentant)

$\Leftarrow$ $m \wedge n = 1 \iff \exists (u,v) \in \mathbb{Z}^2$, $mu + nv = 1$

$\iff \bar{mu} + \bar{nv} = \bar{1} = \bar{m}\bar{u} + \bar{n}\bar{v} = \bar{m}\bar{u} + \bar{0}$

donc $\bar{m}\bar{u} = \bar{1}$ (inverse : $\bar{u} = \frac{\bar{1}}{\bar{m}}$)

$\Rightarrow$ $\bar{m}$ inversible : $\exists u \in \mathbb{Z}$ / $\bar{m}\bar{u} = \bar{1}$

$\bar{m}$ générateur de $(\mathbb{Z}/n\mathbb{Z}, +)$

donc $m \wedge n = 1$

dans $\mathbb{Z}/n\mathbb{Z}$, $\bar{u}\bar{v} \in n\mathbb{Z}$: $uv \equiv 0 [n]$, $\bar{u}\bar{v} = \bar{0}$

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

$\varphi : \begin{cases} \mathbb{N} \setminus \{0,1\} \longrightarrow \mathbb{N} \\ n \longmapsto \varphi(n) = \text{nb d'éléments inversibles de } \mathbb{Z}/n\mathbb{Z} : \text{1ers avec } n \end{cases}$

↑ indicatrice d'Euler

n	2	3	4	5	6	7
$\varphi(n)$	1	2	2	4	2	6

$\varphi(n)$: nb d'él^{ts} de $\{0,1,2,\dots,n-1\}$ premiers avec n

C

Pp 1) p premier $\iff \varphi(p) = p-1$

2) $\begin{cases} p \text{ premier} \\ \alpha \in \mathbb{N}^* \end{cases}$ $\varphi(p^\alpha) = p^\alpha - p^{\alpha-1} = p^{\alpha-1}(p-1)$

$\varphi(p^\alpha)$: nb d'él^{ts} 1ers avec p^α nb de $m \in \mathbb{Z}$ / $m \wedge p^\alpha = 1$

$\forall m \in \mathbb{Z}$, $m \wedge p^\alpha = 1 \iff m \wedge p = 1 \iff p$ ne divise pas m

$1, 2, \dots, p, p+1, \dots, 2p, \dots, 3p, \dots, (p-1)p, \dots (p^{\alpha-1}-1)p, (p^{\alpha-1}-1)p+1, \dots, p^\alpha$

il y a $p^\alpha - p^{\alpha-1}$ él^{ts} non inversibles dans $\mathbb{Z}/n\mathbb{Z}$ $\quad (p^{\alpha-1}-1)p+p$

3 premier, $3^3 = 27$

1 2 ~~3~~ 4 5 ~~6~~ 7 8 ~~9~~ 10 11 ~~12~~ 13 14 ~~15~~ 16 17 ~~18~~ 19 20 ~~21~~ 22 23 ~~24~~ 25 26 ~~27~~

les nombres premiers avec $27 = 3^3$ ne sont pas des multiples de 3 : il faut les retirer : jusqu'à 3^3, il y en a $\frac{3^3}{3} = 3^2$

ainsi, les nb premiers avec 3^3 sont ceux qui restent : $3^3 - 3^2$

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

h- th chinois

th $(m,n) \in \mathbb{N}^2$, $m \wedge n = 1$

$\Psi : \mathbb{Z} \to \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$, $a \mapsto (\overline{a}_n, \overline{a}_m)$

- Ψ est un morphisme d'anneaux.

$\forall (a,b) \in \mathbb{Z}^2$, $\begin{cases} \Psi(a+b) = (\overline{a+b}_n, \overline{a+b}_m) = (\overline{a}_n + \overline{b}_n, \overline{a}_m + \overline{b}_m) = (\overline{a}_n, \overline{a}_m) + (\overline{b}_n, \overline{b}_m) \\ \qquad = \Psi(a) + \Psi(b) \\ \Psi(ab) = (\overline{ab}_n, \overline{ab}_m) = (\overline{a}_n \overline{b}_n, \overline{a}_m \overline{b}_m) = (\overline{a}_n, \overline{a}_m)(\overline{b}_n, \overline{b}_m) = \Psi(a)\Psi(b) \\ \Psi(1) = (\overline{1}_n, \overline{1}_m) = 1_{\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}} \end{cases}$

- $\forall a \in \mathbb{Z}$, $a \in \operatorname{Ker}\Psi \iff \Psi(a) = (\overline{0}_n, \overline{0}_m) \iff \begin{cases} \overline{a}_n = \overline{0}_n \\ \overline{a}_m = \overline{0}_m \end{cases}$ ($a \equiv 0 [n]$: a multiple de n) $\iff \begin{cases} a \in n\mathbb{Z} \\ a \in m\mathbb{Z} \end{cases}$

$\iff a \in n\mathbb{Z} \cap m\mathbb{Z} \iff a \in \mu\mathbb{Z}$ $(\mu = n \vee m)$

$\iff a \in nm\mathbb{Z}^*$

($n=4$, $m=6$: $\mu = 12$, $4\mathbb{Z} \cap 6\mathbb{Z} = 12\mathbb{Z}$)

donc $\operatorname{Ker}\Psi = nm\mathbb{Z}$

- puisque $nm\mathbb{Z} \subset \operatorname{Ker}\Psi$, on peut factoriser :

$\exists\, \Phi : \mathbb{Z}/nm\mathbb{Z} \to \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ morphisme d'anneaux

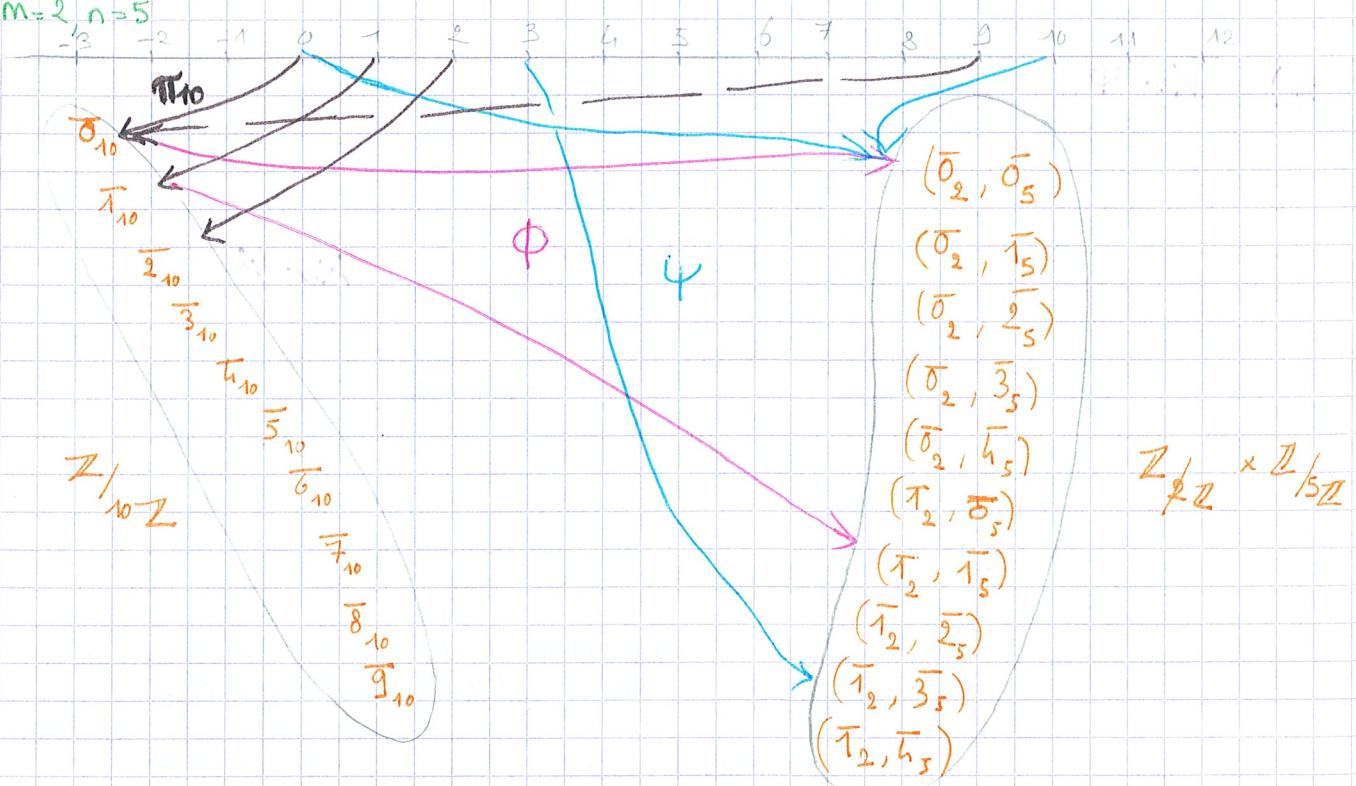
$\Psi = \Phi \circ \pi_{nm}$

$nm\mathbb{Z} = \operatorname{Ker}\Psi$ donc Φ est injectif

or, $\operatorname{card}(\mathbb{Z}/nm\mathbb{Z}) = nm = \operatorname{card}(\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z})$ donc Φ est bijectif

donc Φ est un isomorphisme d'anneaux.

ex : $n=2$, $m=5$



application : $\forall (a,b) \in \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$

(a,b) inversible $\iff \exists (a',b') \in \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z} \ / \ (a,b)(a',b') = (aa', bb') = (\bar{1}_m, \bar{1}_n)$

$\iff \begin{cases} a \text{ inversible dans } \mathbb{Z}/m\mathbb{Z} \\ b \text{ inversible dans } \mathbb{Z}/n\mathbb{Z} \end{cases}$

il y a donc $\varphi(m)\varphi(n)$ éléments inversibles dans $\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$

or, dans $\mathbb{Z}/mn\mathbb{Z}$, il y a $\varphi(mn)$ éléments inversibles

Ainsi, $m \wedge n = 1 \Rightarrow \varphi(mn) = \varphi(m)\varphi(n)$

ex : $\varphi(750) = \varphi(25 \times 3 \times 5^2) = \varphi(5^3 \times 3 \times 2) = \varphi(5^3)\varphi(3)\varphi(2) = 5^2(5-1)(3-1)(2-1)$

$= 200$: il y a 200 e/mts inversibles dans $\mathbb{Z}/750\mathbb{Z}$

exo : Déterminer $p \in \mathbb{Z} \ / \begin{cases} p \equiv 3 \ [5] \\ p \equiv 7 \ [9] \end{cases}$

$\Psi : \mathbb{Z} \longrightarrow \mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/9\mathbb{Z}$ on cherche $\Psi^{-1}(\bar{3}, \bar{7})$

1 solution partic. on cherche $(k,k') \in \mathbb{Z}^2$ / $3 + 5k = 7 + 9k'$

$\iff 5k - 9k' = 4$

or, $5 \wedge 9 = 1$, Bezout : $5(2) - 9(1) = 1$

donc $5(8) - 9(4) = 4$

1 sol: $3 + 5 \times 8 = 43 = 7 + 9 \times 4$ $\quad k = 8, \ k' = 4$

solutions : $\{43 + \underbrace{45}_{5\times 9}k, \ k \in \mathbb{Z}\}$

5 - corps

l'anneau $(\mathbb{K}, +, \times)$ est un corps $\iff \begin{cases} \times \text{ commutative} \\ 1_{\mathbb{K}} \neq 0_{\mathbb{K}} \\ \forall x \in \mathbb{K} \setminus \{0_{\mathbb{K}}\}, \ x \text{ est inversible} \end{cases}$

Pp) $n \in \mathbb{N} \setminus \{0,1\}$,

$(\mathbb{Z}/n\mathbb{Z}, +, \times)$ corps $\iff \begin{cases} \text{tous les éléments sauf } \bar{0} \text{ sont inversibles} \\ \varphi(n) = n-1 \\ n \text{ premier} \end{cases}$

(p premier $\Rightarrow \mathbb{Z}/p\mathbb{Z}$ corps)

* **caractéristique**

$\mathbb{K}$ corps, soit $\Psi : \begin{cases} \mathbb{Z} \longrightarrow \mathbb{K} \\ m \longmapsto m 1_{\mathbb{K}} \end{cases}$ Ψ est un morphisme d'anneaux :

$\begin{cases} \Psi(m+n) = (m+n)1_{\mathbb{K}} = m1_{\mathbb{K}} + n1_{\mathbb{K}} \\ \Psi(mn) = mn1_{\mathbb{K}}1_{\mathbb{K}} = m1_{\mathbb{K}} \, n1_{\mathbb{K}} \\ \Psi(1) = 1.1_{\mathbb{K}} = 1_{\mathbb{K}} \end{cases}$

Pp) $\operatorname{Ker}\Psi$ est un idéal de $\mathbb{Z}$

1er cas : $\operatorname{Ker}\Psi = \{0\}$ on dit que $\mathbb{K}$ est de caractéristique nulle

$\mathbb{K}$ possède un ss-anneau isomorphe à $\mathbb{Z}$

2ème cas : $\operatorname{Ker}\Psi \neq \{0\}$ on dit que le générateur positif de l'idéal principal $\operatorname{Ker}\Psi$ est la caractéristique de $\mathbb{K}$

$\operatorname{Ker}\Psi = n\mathbb{Z}$ idéal de $\mathbb{Z}$, donc principal

dans ce cas, si k est la caractéristique de $\mathbb{K}$

* $k \neq 1$ | supposons $k = 1$, $\operatorname{Ker}\Psi = \mathbb{Z}$, $\Psi(1) = 0_{\mathbb{K}}$, $1_{\mathbb{K}} = 0_{\mathbb{K}}$ or $1_{\mathbb{K}} \neq 0_{\mathbb{K}}$

* k premier | si k non premier, $\exists (a,b) \in \mathbb{N}^2$, $a \neq 1$, $b \neq 1$ / $k = ab$ donc $\Psi(k) = \Psi(a)\Psi(b)$

$\begin{cases} 1 < a < k \\ 1 < b < k \end{cases} \Rightarrow \begin{cases} a \notin k\mathbb{Z} \\ b \notin k\mathbb{Z} \end{cases} \Rightarrow \begin{cases} \Psi(a) \neq 0_{\mathbb{K}} \\ \Psi(b) \neq 0_{\mathbb{K}} \end{cases}$

$\Psi(k) = 0_{\mathbb{K}} \Leftrightarrow \Psi(ab) = \Psi(a)\Psi(b) = 0_{\mathbb{K}}$

diviseur de zéro (non inversible)

impossible ds un corps

* $k 1_{\mathbb{K}} = 0_{\mathbb{K}}$ et $k = \inf\{n \in \mathbb{N}^* / \ n 1_{\mathbb{K}} = 0_{\mathbb{K}}\}$

($\mathbb{Z}/3\mathbb{Z}$: $\bar{1} + \bar{1} + \bar{1} = \bar{3} = \bar{0}$, $3.\bar{1} = \bar{0}$)

* p premier $\Rightarrow$ la caractéristique de $\mathbb{Z}/p\mathbb{Z}$ est p.

6. $\mathbb{Z}/p\mathbb{Z}$, p premier

$\mathbb{Z}/p\mathbb{Z}$ est un corps, $U_{\mathbb{Z}/p\mathbb{Z}} = (\mathbb{Z}/p\mathbb{Z})^* = \mathbb{Z}/p\mathbb{Z} \setminus \{\bar{0}\}$

$(\mathbb{Z}/p\mathbb{Z}^*, \times)$ est un groupe

$\text{card}(\mathbb{Z}/p\mathbb{Z}^*) = p-1$

Petit Th de Fermat : p premier $\Rightarrow$ $\forall x \in (\mathbb{Z}/p\mathbb{Z})^*$, $x^{p-1} = \bar{1}$ (ordre d'un élt dans un groupe)

$x = \bar{n}$ $\forall n \in \mathbb{Z}$, $n \wedge p = 1 \Rightarrow n^{p-1} \equiv 1 \ [p]$

$\forall x \in \mathbb{Z}/p\mathbb{Z}$, $x^p = x$

$\forall n \in \mathbb{Z}$, $n \wedge p = 1 \Rightarrow n^p \equiv n \ [p]$

rem : • soit $X^{p-1} - \bar{1} \in \mathbb{Z}/p\mathbb{Z}[X]$

$X^{p-1} - \bar{1}$ a pour racines les éléments de $(\mathbb{Z}/p\mathbb{Z})^*$

donc $X^{p-1} - \bar{1} = \prod_{x \in (\mathbb{Z}/p\mathbb{Z})^*} (X - x)$

• si $n \in \mathbb{N} \setminus \{0,1\}$ non 1er

$\mathbb{Z}/n\mathbb{Z}$ n'est pas un corps

$U_{\mathbb{Z}/n\mathbb{Z}}$ est un gr. multiplicatif ayant $\varphi(n)$ élts

donc, $\forall x \in U_{\mathbb{Z}/n\mathbb{Z}}$, $x^{\varphi(n)} = \bar{1}$ $\forall n \in \mathbb{Z}$, $m \wedge n = 1 \Rightarrow m^{\varphi(n)} \equiv 1 \ [n]$