ALGEBRE
Chapitre 1

Algèbre générale
Groupes, Anneaux, Polynômes

§0 Revoir le cours de sup
- ensemble, application

ex : f surjection de A sur B $\quad f : A \to B$

$\forall b \in B \quad \exists a \in A \quad f(a) = b$

f injection de A dans B

$\forall (x,y) \in A^2 \quad f(x) = f(y) \Rightarrow x = y$

- image

$f(A) = \{ f(a) \,/\, a \in A \} \subset B$

image réciproque $B' \subset B$

"$f^{-1}(B')$" $= \{ a \in A \,/\, f(a) \in B' \}$

- arithmétique, dnb

$\mathbb{N}, \mathbb{Z}$ ensembles finis, infinis, cardinal

ex : E ens fini à n elts

$\mathcal{P}_p(E)$ ens des parties de E à $p \leq n$ elts

$\mathrm{card}\left(\mathcal{P}_p(E)\right) = C_n^p = \binom{n}{p} = \frac{n!}{p!(n-p)!}$

ex : formule du triangle de Pascal

$\binom{n+1}{p+1} = \binom{n}{p+1} + \binom{n}{p}$

méthodes de démo

→ formule du binôme de Newton $\quad u, v \in A \quad u \times v = v \times u, n \in \mathbb{N}$

$(u+v)^n = \sum_{k=0}^{n} \binom{n}{k} u^k \times v^{n-k}$

$(1+X)^{n+1} = (1+X)(1+X)^n$, terme en X^{p+1} ?

$= (1+X) \sum \binom{n}{k} x^k \quad$ coeff $\binom{n}{p+1} + \binom{n}{p}$

→ dnb par ...

- Structures alg

Groupes, Anneaux, Corps

structures de ref

ex groupes : $(\mathbb{R},+)$; $(\mathbb{Z},+)$; $(\mathbb{C},+)$; $(\mathbb{Q},+)$; $(\mathbb{R}^*,\times)$

; ... ; $(\mathbb{Z}/n\mathbb{Z},+)$; $(M_n(\mathbb{R}),+)$; $(\mathbb{R}^{\mathbb{N}},+)$

$\mathbb{U}_n = \{z \in \mathbb{C} / z^n = 1\}$ $\quad (\mathbb{U}_n, \times)$; $(\mathcal{S}_n = \mathrm{Bij}([\![1,n]\!],[\![1,n]\!]), \circ)$

card $\mathcal{S}_n = n!$ $\quad$ ex corps : quaternions $\mathbb{H}$

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

$\mathbb{K}(X)$ $\mathbb{K}$ corps commutatif

$= \left\{ \frac{P}{Q} / P, Q \in \mathbb{K}[X] \; Q \neq 0 \right\}$

- PN, FR

$(\mathbb{K}[X], +, \times, \cdot)$ $\mathbb{K}$-algèbre $\mathbb{K}$ corps commutatif

$\longrightarrow$ base, ...

$\longrightarrow$ division euclidienne

$\forall (A,B) \in \mathbb{K}[X]^2, B \neq 0 \; \exists! (Q,R) \in \mathbb{K}[X]^2 \begin{cases} A = BQ + R \\ d^\circ R < d^\circ B \end{cases}$

$\mathbb{K}(X)$ décompo en elts simples

I INTRO $\longrightarrow$ qq exos

1) $\mathbb{H} = \left\{ \begin{pmatrix} a & -\bar{b} \\ b & \bar{a} \end{pmatrix} ; a, b \in \mathbb{C} \right\}$

mq $(\mathbb{H}, +, \times)$ corps non commutatif

$\mathbb{H} \subset M_2(\mathbb{C})$ $\quad (M_2(\mathbb{C}), +, \times)$ anneau

$(GL_2(\mathbb{C})$ sous ens des elts inversibles de $M_2(\mathbb{C}))$

mq $\mathbb{H}$ sous anneau de $M_2(\mathbb{C})$

SA (SG (- $\mathbb{H} \neq \emptyset$: $0 \in \mathbb{H}$

- $\mathbb{H} \subset M_2(\mathbb{C})$ ✓

- stable pour + : $\forall (A,B) \in \mathbb{H}$, $A - B \in \mathbb{H}$

- $AB \in \mathbb{H}$

non commutatif : $a = d = 0$, $b = c = i$

$A = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}$ $B = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}$

$AB = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$ $BA = \begin{pmatrix} 0 & \vdots \\ 1 & \vdots \end{pmatrix}$ ✓

corps ? $A = \begin{pmatrix} a & -\bar{b} \\ b & \bar{a} \end{pmatrix}$ non nul A inversible pour X

$\det A = |a|^2 + |b|^2 > 0$ car $(a, b) \neq (0, 0)$ ✓

$\left(A^{-1} = \frac{1}{|a|^2+|b|^2} \begin{pmatrix} \bar{a} & \bar{b} \\ -b & a \end{pmatrix} \in \mathbb{H} \right)$

Un corps fini est commutatif.

2) $n \in \mathbb{N}^*$, $n \geq 2$ Calculer $P_n = \prod_{k=1}^{n-1} \sin\left(\frac{k\pi}{n}\right)$

NB relations coeff racine d'1 PN scindé

$P \in \mathbb{C}[X]$; $d^\circ P = p \geq 1$; $P = \sum_{k=0}^{p} a_k X^k = a_p \times \prod_{k=1}^{p} (X - z_k)$

racines $z_1, \dots, z_p$

produit des racines

$z_1 \times \dots \times z_p = \sigma_p = (-1)^p \frac{a_0}{a_p}$ ← valeur du PN en 0

somme des racines

$z_1 + \dots + z_p = \sigma_1 = -\frac{a_{p-1}}{a_p}$

Rem $\sigma_j = \sum_{1 \leq i_1 < i_2 < \dots < i_j \leq p} z_{i_1} \times \dots \times z_{i_j} = (-1)^j \frac{a_{p-j}}{a_p}$

sommes de Newton : $\sum_{j=1}^{p} z_j^p = S_p$

ex : $\sum_{j=1}^{p} z_j^2 = S_2$ $(\sigma_1)^2 = (z_1 + \dots + z_p)^2 = S_2 + 2\sigma_2$

...

→ trouver 1 PN dont les racines sont liés à P_n

Formules d'Euler $\cos\theta = \frac{e^{i\theta} + e^{-i\theta}}{2}$; $\sin\theta = \frac{e^{i\theta} - e^{-i\theta}}{2i}$

$\Rightarrow \sin\frac{k\pi}{n} = \frac{e^{\frac{ik\pi}{n}} - e^{-\frac{ik\pi}{n}}}{2i} = \frac{e^{-\frac{ik\pi}{n}}}{2i}\left(e^{\frac{2ik\pi}{n}} - 1\right)$

$e^{\frac{2ik\pi}{n}} - 1$ $1 \leq k \leq n-1$ racines de $Q_n = (X+1)^n - 1$

$k = 0$? $\Rightarrow Q_n = \frac{(X+1)^n - 1}{X} = \prod_{k=1}^{n-1} \left(X - \left(e^{\frac{2ik\pi}{n}} - 1\right)\right)$

$$P_n = \prod_{k=1}^{n-1} \sin\left(\frac{k\pi}{n}\right) = \left(\prod_{k=1}^{n-1} \frac{e^{-\frac{ik\pi}{n}}}{2i}\right)\left(\prod_{k=1}^{n-1}\left(e^{\frac{2ik\pi}{n}}-1\right)\right)$$

$$= \left(\frac{1}{(2i)^{n-1}} e^{-\frac{i\pi}{n}\left(\frac{n(n-1)}{2}\right)}\right)$$

Formule (identité géom)

$$\sum_{k=0}^{p} z^k = \begin{cases} p+1 & \text{si } z=1 \\ \dfrac{z^{p+1}-1}{z-1} & \text{si } z\neq 1 \end{cases} \quad z\in\mathbb{C}$$

$$\Rightarrow Q_n(X) = \sum_{k=0}^{n-1} (X+1)^k$$

valeur en 0 : n

$$\Rightarrow P_n = \left(\frac{1}{(2i)^{n-1}} e^{-\frac{i\pi}{2}(n-1)}\right)\left(\frac{n}{(-1)^{n-1}}\right)$$

$$= \frac{n(-1)^{n-1}}{(-2i)^{n-1}} = \underline{\frac{n}{2^{n-1}}}$$

II Compléments sur les groupes, $\mathbb{Z}/n\mathbb{Z}$

1°) Propriétés générales

a) Morphismes de groupes

<u>Def</u> $(G,\times)$ et $(H,+)$; $f : G \to H$

f est un morphisme de groupes

si $\forall g, g' \in G$, $f(g\times g') = f(g) + f(g')$

<u>Prop</u> Dans ce cas :

- si G' SG de G, $f(G')$ SG de H
- si H' SG de H, $f^{-1}(H')$ SG de G

<u>dém</u> ② $f^{-1}(H') \subset G$ par def, non vide :

$f(1_G) = 0_H \in H' \Rightarrow 1_G \in f^{-1}(H')$

$a, b \in f^{-1}(H')$

$f(a\times b^{-1}) = \underset{\in H'}{f(a)} - \underset{\in H'}{f(b)} \in H' \Rightarrow a\times b^{-1} \in f^{-1}(H')$

<u>En particulier</u>

- $\operatorname{Im} f = f(G)$ SG de H
- $\operatorname{Ker} f = f^{-1}(\{0_H\})$ SG de G

Rem f injective ?

$$f(x) = f(y) \iff f(x \times y^{-1}) = 0$$

$$f \text{ inj} \iff \operatorname{Ker} f = \{1_G\}$$

Ex • $\ln$ isomorphisme de $(\mathbb{R}_+^*, \times)$ sur $(\mathbb{R}, +)$

$\exp = (\ln)^{-1}$

• $\sigma : S_n \to \{-1, 1\}$

$\sigma(f) = (-1)^{N_f}$

$N_f = \operatorname{Card}\{(i,j) \in [\![1,n]\!]^2 \,/\, i<j \,;\, f(i) > f(j)\}$

(Rem : $A_n = \operatorname{Ker} \sigma$)

• $\det : GL_n(\mathbb{C}) \to \mathbb{C}^*$

(b) groupe engendré par une partie

def $(G, \times)$ groupe, $A \subset G$

$\langle A \rangle = gp(A)$: groupe engendré par A

$=$ plus petit SG de G contenant A

- A est une partie génératrice de G si $\langle A \rangle = G$
- G monogène si il existe $a \in G$ tq $G = \langle a \rangle$
- G cyclique si G est monogène et fini

NB. $(G, \times)$ groupe (resp $(G,+)$), $a \in G$

$\langle a \rangle = \{a^k \,/\, k \in \mathbb{Z}\}$ (resp $\{ka \,/\, k \in \mathbb{Z}\}$)

Rem $\langle A \rangle$ est aussi l'intersection de ts les SG de G contenant A.

$$\langle A \rangle = \bigcap_{\substack{H \text{ SG de } G \\ A \subset H}} H$$

Une intersection de SG de G est un SG de G.

Ex de groupe cyclique : $n \in \mathbb{N}^*$

$$U_n = \{z \in \mathbb{C} \,/\, z^n = 1\} = \{e^{\frac{2ik\pi}{n}},\ k \in \{0, \dots, n-1\}\}$$

$a = e^{\frac{2i\pi}{n}}$ $\quad U_n = \{a^k,\ k \in \mathbb{Z}\}$ $\quad (a^n = 1)$

$= \{a^k,\ k \in \{0, \dots, n-1\}\} = \langle a \rangle$

Prop (1) $(G, \cdot)$ gpe soit $a \in G$, $\langle a \rangle = \{a^k, k \in \mathbb{Z}\}$

(2) $(G, +)$ ——————— $\langle a \rangle = \{ka, k$ — $\}$

et $\begin{matrix} k \mapsto a^k \\ \mathbb{Z} \to G \end{matrix}$ (resp $\begin{matrix} k \mapsto ka \\ \mathbb{Z} \to G \end{matrix}$) morphisme de gpe.

(c) SG de $(\mathbb{Z}, +)$

Th Tout SG de $(\mathbb{Z}, +)$ est monogène, de la forme $n\mathbb{Z}$ avec $n \in \mathbb{N}$

démo (1) $n \in \mathbb{N}$ $n\mathbb{Z} = \{nk / k \in \mathbb{Z}\} = \langle n \rangle$ SG de $(\mathbb{Z}, +)$

$= \mathrm{Im}\begin{pmatrix} k \mapsto kn \\ \mathbb{Z} \to \mathbb{Z} \end{pmatrix}$

(2) H SG de $(\mathbb{Z}, +)$ .. ?

2 cas 1er : $H = \{0\} = 0\mathbb{Z}$

2e : $H \neq \{0\}$ alors $H \cap \mathbb{N}^* \neq \emptyset$

en ~~effet~~ $\exists x \in H \setminus \{0\}$, x ou $-x$ dans $\mathbb{N}^*$

$H \cap \mathbb{N}^*$ partie de $\mathbb{N}$ non vide possède un minimum n

$n = \min H \cap \mathbb{N}^*$

$n \in H$, $k \in \mathbb{Z}$, $nk \in H$, $n\mathbb{Z} \subset H$

récip : $h \in H$ DE de h par n

$\exists (q, r) \in \mathbb{Z}^2$, $0 \leq r < n$ $h = nq + r$

$r = h - nq \in H$ $r < n$ donc $r = 0$
sinon $r \in H \cap \mathbb{N}^*$

$\Rightarrow h = nq \in n\mathbb{Z} \Rightarrow H \subset n\mathbb{Z} \Rightarrow H = n\mathbb{Z}$ $\square$

Rem $n = 0$ sinon $n = \min(\mathbb{N}^* \cap H)$ lorsque $H \neq \{0\}$

Cy pour les groupes

Soit $(G, \cdot)$ (resp $(G, +)$) groupe

Soit $a \in G$. $f_a : \begin{matrix} k \mapsto a^k \\ \mathbb{Z} \to G \end{matrix}$ (resp $\begin{matrix} k \mapsto ka \\ \mathbb{Z} \to G \end{matrix}$) est un morphisme de groupe.

Ker f_a SG de $\mathbb{Z}$ de la forme $n\mathbb{Z}$ avec $n \in \mathbb{N}$ unique

- soit $n = 0 \Rightarrow f_a$ est injective $\langle a \rangle$ infini
- soit $n \neq 0$ $\langle a \rangle = \{e, a, \dots, a^{n-1}\}$ (resp $\{0, a, 2a, \dots, (n-1)a\}$)

est groupe cyclique de cardinal n

en effet, $\langle a \rangle = \{a^k / k \in \mathbb{Z}\}$; $k = nq + r$ $\quad 0 \leq r < n-1$ $\quad a^n = e$

$a^k = (a^n)^q \times a^r = a^r$

<u>unicité</u> $a^r = a^{r'}$; $a^{r'-r} = e$ $\quad (r, r' \in \{0, \dots, n-1\})$

$(r \leq r')$ $\quad r' - r \in \text{Ker } f_a$ et $n \mid r' - r \Rightarrow r = r'$

<u>Def</u> $(G, \cdot)$ groupe, $a \in G$

a est dit d'ordre fini si $\langle a \rangle$ est fini

alors l'ordre de a est card $\langle a \rangle = n$ caractérisé

par $n = \min\{k \in \mathbb{N}^* / a^k = e\}$

<u>NB</u> $\langle a \rangle = \{e, a, \dots, a^{n-1}\}$

<u>ex</u> $\mathbb{U}_n = \{z \in \mathbb{C} / z^n = 1\} = \langle e^{\frac{2i\pi}{n}} \rangle = \{1, a, \dots, a^{n-1}\}$

Exercice : Th de Lagrange, csq

Soit G un gpe fini et H un SG de G

alors card H / card G

Si $a \in G$, $d = $ ordre (a) $\quad d / \text{card } G$

$(G, \cdot)$ $\quad \mathcal{R}$ relation sur G, $x, y \in G$

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

- Vérifier que $\mathcal{R}$ relation d'équivalence sur G
- classes d'équivalence
- Déduire le résultat

$\boxed{R}$ $x \in G$ $\quad x \mathcal{R} x$

$x^{-1} \cdot x = e \in H$ (SG)

$\boxed{S}$ $x, y \in G$ $\quad x \mathcal{R} y \Rightarrow y \mathcal{R} x$

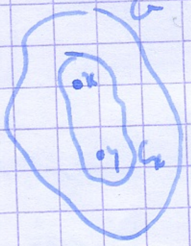
car $\left| \begin{array}{l} x^{-1} y = h \in H \\ h^{-1} = y^{-1} x \in H \end{array} \right.$

$\boxed{T}$ $x, y, z \in G$ $\quad \left. \begin{array}{l} x \mathcal{R} y \Leftrightarrow x^{-1} y \in H \\ y \mathcal{R} z \Leftrightarrow y^{-1} z \in H \end{array} \right) \begin{array}{l} x^{-1} z \in H \\ \Rightarrow x \mathcal{R} z \end{array}$

NB G ens, $\mathcal{R}$ rel eq

l'ens des classes d'équivalence

forme une partition de G



$C_x = \{ y \in G / x \mathcal{R} y \}$

$y \in C_x$ $\quad \exists h \in H$, $x^{-1} y = h$ $\quad y = xh$

$\Rightarrow C_x = xH = \{ xh / h \in H \}$ partition

$x, y \in G$ tq $C_x \neq C_y$ alors $C_x \cap C_y = \emptyset$

(sinon $z \in C_x \cap C_y$ $\quad z = xh = yh'$

$\Rightarrow x = y h' h^{-1} \in yH$ et $C_x = C_y$)

Si G fini, l'ens des classes d'eq est fini

$G = C_{x_1} \cup \dots \cup C_{x_p}$ $\quad C_{x_i} \cap C_{x_j} = \emptyset$ si $i \neq j$

$C_{x_i} = x_i H$

$\left. \begin{array}{l} h \mapsto x_i h \\ H \to x_i H \end{array} \right|$ bijective : — surjective par définition de C_{x_i}

— inj $x_i h = x_i h'$ $\quad h = h'$

Card $x_i H$ = Card H (lemme des bergers)

G gpe fini

classes d'eq même nb d'élts (card H)

$x_1 H, \dots, x_p H$ partition de G

mq Card $G = p \cdot$ Card H

$G = (x_1 H) \cup \dots \cup (x_p H)$

$\text{Card } G = \sum \text{card}(x_i H) = p \cdot \text{Card } H$

$\Rightarrow \text{Card } H \,/\, \text{card } G$ □

Si $a \in G$, $\langle a \rangle$ fini et $\underbrace{\text{card } \langle a \rangle}_{d} / \text{Card } G$

en particulier, $a^d = e$.
si $n = \text{card } G$, $a^n = e$.

(d) Congruence modulo n, $\mathbb{Z}/n\mathbb{Z}$

Def $n \in \mathbb{N}$; $(x,y) \in \mathbb{Z}^2$ congrus modulo n si $x - y \in n\mathbb{Z}$
noté $x \equiv y \ [n]$
(ie $\exists k \in \mathbb{Z} \,/\, x = y + nk$)

Prop La relation de congruence mod n est une relaq
sur $\mathbb{Z}$, compatible avec $+$
Pour $x \in \mathbb{Z}$, on note $\overline{x}$ (ou $\dot{x}$) sa classe d'eq
$\overline{x} = \{x + nk,\ k \in \mathbb{Z}\}$
L'ens de ces classes est fini, noté $\mathbb{Z}/n\mathbb{Z}$

démo $\boxed{R}$ $x \in \mathbb{Z}$, $x \mathcal{R} x$ car $x - x = 0 \in n\mathbb{Z}$
$\boxed{S}$ $x, y \in \mathbb{Z}$, $x - y \in n\mathbb{Z} \Rightarrow y - x \in n\mathbb{Z}$
donc $x \mathcal{R} y \Rightarrow y \mathcal{R} x$
$\boxed{T}$ $x, y, z \in \mathbb{Z}$ $\left.\begin{array}{l} x \mathcal{R} y \Rightarrow x - y \in n\mathbb{Z} \\ y \mathcal{R} z \Rightarrow y - z \in n\mathbb{Z} \end{array}\right\} \overset{\text{somme}}{} x - z \in n\mathbb{Z} \Rightarrow x \mathcal{R} z$

compatible avec $+$: $x \equiv y \ [n]$ $t \in \mathbb{Z}$
$x + t \equiv y + t$ car $(x+t) - (y+t) = x - y$

cas particulier (éliminé par la suite)
$n = 0$: cas d'égalité $\rightarrow$ $n \in \mathbb{N}^*$.

$x \in \mathbb{Z}$ DE par n : $\exists! (q,r) \in \mathbb{Z}^2 \ \left| \begin{array}{l} x = nq + r \\ 0 \leq r \leq n-1 \end{array}\right.$ $x \equiv r \ [n]$

r unique : $\begin{cases} x \equiv r \\ x \equiv r' \end{cases}$ $r, r' \in \{0, \dots, n-1\}$ $r' \geq r$ $r' - r \in n\mathbb{Z}$ $0 \leq r' - r < n$ $r' = r$

Bilan

Prop Pour $n \in \mathbb{N}^*$, $\mathbb{Z}/n\mathbb{Z} = \{\overline{0}, \overline{1}, \dots, \overline{n-1}\}$

Def/Prop $n \in \mathbb{N}^*$. On définit sur $\mathbb{Z}/n\mathbb{Z}$ une addition par $\forall (x, y) \in \mathbb{Z}^2$ $\overline{x} + \overline{y} = \overline{x+y}$

$(\mathbb{Z}/n\mathbb{Z}, +)$ gpe commutatif et $s : \begin{array}{l} k \mapsto \overline{k} \\ \mathbb{Z} \to \mathbb{Z}/n\mathbb{Z} \end{array}$

(surjection canonique) morphisme de groupes

Prop $n \in \mathbb{N}^*$ alors $(\mathbb{Z}/n\mathbb{Z}, +)$ est un gpe cyclique dont les générateurs sont de la forme $\overline{k}$, avec $k \in \mathbb{Z}$ tq pgcd $(k, n) = 1$

démo • $\overline{1}$ engendre $(\mathbb{Z}/n\mathbb{Z}, +)$

$\mathbb{Z}/n\mathbb{Z} = \{\overline{0}, \overline{1}, \dots, \overline{n-1}\} = \{k \cdot \overline{1} / k \in \mathbb{Z}\}$

$= \{k\overline{1} \,/\, k \in [\![0, n-1]\!]\}$

• $k \in \mathbb{Z}$ tq $\overline{k}$ engendre $\mathbb{Z}/n\mathbb{Z}$

il existe $t \in \mathbb{Z}$

$\overline{1} = t \cdot \overline{k} \Rightarrow tk - 1 \in n\mathbb{Z}$

$\Rightarrow \exists u \in \mathbb{Z},\ tk + un = 1 \Rightarrow k \wedge n = 1$

Rec $k \wedge n = 1$; identité de Bezout :

$\exists u, v \in \mathbb{Z} \,/\, ku + vn = 1$

mod n : $\overline{ku} = \overline{1}$

$\overline{u} = \overline{r}$ $r \in [\![0, n-1]\!]$ $r\overline{k} = \overline{1}$

$\Rightarrow \forall s \in \mathbb{Z}$ $\overline{s} = (sr)\overline{k}$ $\mathbb{Z}/n\mathbb{Z} = \langle \overline{k} \rangle$

Def (indicateur d'Euler) Pour $n \in \mathbb{N}^*$, on note $\varphi(n) = \mathrm{Card}\{k \in [\![1, n]\!] / k \wedge n = 1\}$

Par la prop précédente, $\varphi(n) =$ nb de générateurs de $\mathbb{Z}/n\mathbb{Z}$

$\varphi : \mathbb{N}^* \to \mathbb{N}^*$ $\varphi(1) = \varphi(2) = 1$ $\varphi(3) = \varphi(4) = 2$

$\varphi(p^\alpha)$? $\alpha \in \mathbb{N}^*$ $k \in [\![1, p^\alpha]\!]$

$k \wedge p^\alpha \neq 1 \iff p / k$

$E = [\![1, p^\alpha]\!] = A \cup B$ avec $\left| \begin{array}{l} A = \{ k \in E / k \wedge p^\alpha = 1 \} \\ B = \{ k \in E / k \wedge p^\alpha \neq 1 \} \end{array} \right.$

$A \cap B = \emptyset$

ie $B = \{ pu / u \in [\![1, p^{\alpha-1}]\!] \}$ ($u \mapsto pu$ bij)

$\Rightarrow$ card $B = p^{\alpha-1}$

$\Rightarrow$ card $A = p^\alpha - p^{\alpha-1}$

d'où $\forall p \in \mathbb{P}, \forall \alpha \in \mathbb{N}^*, \varphi(p^\alpha) = p^\alpha - p^{\alpha-1}$

démontré plus tard : $\varphi(mn) = \varphi(m)\varphi(n)$

ex générateurs de $(\mathbb{Z}/8\mathbb{Z}, +)$?

$\longrightarrow \bar{1}, \bar{3}, \bar{5}, \bar{7}$

dans $\mathbb{Z}/8\mathbb{Z}$: $\overline{6} = 2 . \bar{7}$

Retour sur les grps cycliques :

$(G, \cdot)$ gpe (resp $(G, +)$), $a \in G$

$\langle a \rangle = \{ a^k / k \in \mathbb{Z} \}$ (resp $\{ ka / k \in \mathbb{Z} \}$)

$f_a : \begin{array}{l} k \longmapsto a^k \\ \mathbb{Z} \longrightarrow G \end{array}$ (resp $k \mapsto ka$) morphisme de groupes

donc $\operatorname{Ker} f_a = n\mathbb{Z}$, $n \in \mathbb{Z}$

2 cas – $n = 0 \Rightarrow f_a$ injective $\Rightarrow \langle a \rangle$ infini

– $n \in \mathbb{N}^*$ $\langle a \rangle = \{ e, a, \dots, a^{n-1} \}$

n ordre de a

et $\begin{array}{l} \bar{k} \longmapsto a^k \\ \mathbb{Z}/n\mathbb{Z} \longrightarrow \langle a \rangle \end{array}$ isomorph

$(\mathbb{Z}/n\mathbb{Z})$ est le modèle std d'1 gp cyclique d'ordre n

ex $\mathbb{U}_n = \{a^k,\ k \in [\![1, n-1]\!]\}$ où $a = e^{2i\frac{\pi}{n}}$

$g : \begin{cases} \mathbb{Z}/n\mathbb{Z} \to \mathbb{U}_n \\ k \mapsto a^k \end{cases}$

csq : générateurs de $(\mathbb{U}_n, \cdot)$:

$e^{\frac{2ik\pi}{n}}$ avec $k \in [\![1, n-1]\!]$ et $k \wedge n = 1$

("racines primitives n^{e} de l'unité")

PN cyclotomiques

$$X^n - 1 = \prod_{k=0}^{n-1} \left(X - e^{\frac{2ik\pi}{n}}\right)$$

$$\phi_n(X) = \prod_{\substack{k \in [\![1, n-1]\!] \\ k \wedge n}} \left(X - e^{\frac{2ik\pi}{n}}\right)$$

ex de prop : $X^n - 1 = \prod_{d/n} \phi_d(X)$

(e) Produit de 2 groupes

Prop Soient $(G, \times)$ et $(H, +)$ 2 gpes

sur $G \times H = \{(g, h) / g \in G, h \in H\}$ on définit la loi (dite produit) par :

$\forall (g, h), (g', h') \in (G \times H)^2$, $(g, h) * (g', h') = (g \times g', h + h')$

Alors $(G \times H, *)$ est un gpe.

Si de plus G et H sont commutatifs, $G \times H$ aussi.

démo : ASSOC : ...

ELT.NT : $(1_G, 0_H)$

SYM : $(g, h) * (g^{-1}, -h) = (1_G, 0_H)$

ex : groupe de Klein : $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$

$+$	$(\bar 0, \bar 0)$	$(\bar 0, \bar 1)$	$(\bar 1, \bar 0)$	$(\bar 1, \bar 1)$
$(\bar 0, \bar 0)$	$(\bar 0, \bar 0)$	$(\bar 0, \bar 1)$	$(\bar 1, \bar 0)$	$(\bar 1, \bar 1)$
$(\bar 0, \bar 1)$	$(\bar 0, \bar 1)$	$(\bar 0, \bar 0)$	$(\bar 1, \bar 1)$	$(\bar 1, \bar 0)$
$(\bar 1, \bar 0)$	$(\bar 1, \bar 0)$	$(\bar 1, \bar 1)$	$(\bar 0, \bar 0)$	$(\bar 0, \bar 1)$
$(\bar 1, \bar 1)$	$(\bar 1, \bar 1)$	$(\bar 1, \bar 0)$	$(\bar 0, \bar 1)$	$(\bar 0, \bar 0)$

groupe cyclique ?

$\langle(\bar 0, \bar 0)\rangle = \{(\bar 0, \bar 0)\}$ ordre 1

ts les autres d'ordre 2

$\longrightarrow$ non cyclique

Rem 1 G groupe de cardinal $p \in \mathbb{P}$
G cyclique
$a \in G, a \neq e \quad \langle a \rangle = G \quad$ (Th de Lagrange)

III Anneaux, corps

1) Idéaux d'1 anneau commutatif, compléments

a) Morphismes d'anneaux

Déf Soient $(A,+,\times)$, $(B,+,\times)$ 2 anneaux. L'appli $f : A \to B$ est un morph d'anneaux si :

- $\forall (a,a') \in A^2$, $f(a+a') = f(a) + f(a')$
$\qquad f(a \times a') = f(a) \times f(a')$
- $f(1_A) = 1_B$

Si de plus f bij, f est un isomorph d'anneaux.

Rem $\mathrm{Im} f = f(A)$ SA de B
$\mathrm{Ker} f$ ne contient pas 1_A $(f(1_A) = 1_B \neq 0_B)$
si $a \in \mathrm{Ker} f$, $a' \in A$ alors $a \times a' \in \mathrm{Ker} f$
car $f(a \times a') = \underbrace{f(a)}_{0} \times f(a') = 0$

b) Idéal

Déf Soit $(A,+,\times)$ un anneau commutatif et $I \subset A$.
ODQ I est un idéal de A si :
① $(I,+)$ SG de $(A,+)$
② $\forall a \in I, \forall x \in A, a\, x \in I$
ie $\forall a \in I, aA \subset I$

Rem : ▸ ex : dans $\mathbb{Z} = A$, $n\mathbb{Z}$ idéal
▸ A anneau comm qcq, $x \in A$
$I = xA = \{xh \,/\, h \in A\}$ idéal de A, engendré par x
(idéal principal)

▶ I, J idéaux de A alors $I+J$ idéal de A

Vérif $I+J = \{ i+j \mid (i,j) \in I \times J \}$

- SG additif, inclus ds A, $\neq \emptyset$

$(i+j)-(i'+j') = \underbrace{(i-i')}_{\in I} + \underbrace{(j-j')}_{\in J}$

- $\left.\begin{array}{l} i \in I \\ j \in J \\ z \in A \end{array}\right\}$ $z.(i+j) = \underbrace{zi}_{\in I} + \underbrace{zj}_{\in J} \in I+J$

▶ toute intersection d'idéaux de A est un idéal de A

▶ I idéal de A – si $1_A \in I$ alors $I = A$

– dès que I contient 1 elt inversible u, $I = A$

▶ A anneau comm, B anneau

$f : A \longrightarrow B$ morphisme d'anneaux

alors $\operatorname{Ker} f$ idéal de A :

- SG add

- $\left.\begin{array}{l} a \in \operatorname{Ker} f \\ x \in A \end{array}\right\}$ $ax \in \operatorname{Ker} f$ cf $f(ax) = 0$

▶ (cf chap Réduction)

E $\mathbb{K}$ev, $u \in \mathcal{L}(E)$

"$\operatorname{Ann}(u)$" $= \{ P \in \mathbb{K}[X] \mid P(u) = 0 \}$

idéal de $\mathbb{K}[X]$

<u>Prop</u> Soit A anneau comm <u>intègre</u>, $x, y \in A$

$x \mid y \iff \exists k \in A, y = xk \iff y \in xA \iff yA \subset xA$

Arithmétique ds A : étude des idéaux de A

2 cas (déjà vus en MPSI) : $\mathbb{Z}$, $\mathbb{K}[X]$ cf DE

Th. ① les idéaux de $\mathbb{Z}$ sont tous de la forme $n\mathbb{Z}$, $n \in \mathbb{N}$

② $\mathbb{K}$ corps commutatif. Les idéaux de $\mathbb{K}[X]$ sont de la forme $P.\mathbb{K}[X]$, $P \in \mathbb{K}[X]$.

(les anneaux $\mathbb{Z}$ et $\mathbb{K}[X]$ sont dits principaux *)

démo ① cas de $\mathbb{Z}$: cf SG adds de $\mathbb{Z}$

si I idéal de $\mathbb{Z}$ $\exists n \in \mathbb{N}$, $n\mathbb{Z} = I$ (nécessairement SG add)

réciproquement, $n\mathbb{Z}$ idéal de $\mathbb{Z}$

② cas de $\mathbb{K}[X]$

$(\mathbb{K}[X], +, \times)$ anneau comm intègre

Rem générale : A anneau

$U(A) = A^{\circ}$ ens des élts inversibles de A

alors $(U(A), \times)$ groupe

ici, $U(\mathbb{K}[X]) = \mathbb{K}^*$

I idéal de $\mathbb{K}[X]$. 2 cas :

- soit $I = \{0\} = 0.\mathbb{K}[X]$
- soit $I \neq \{0\}$. soit $C = \{d^\circ(Q) / Q \in I, Q \neq 0\} \subset \mathbb{N}$ non vide

possède un minimum $p = d^\circ(P)$, $P \in I$, $I \neq \emptyset$

* $P.\mathbb{K}[X] \subset I$ car $P \in I$, I idéal

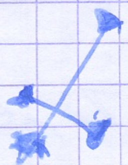
* récipt $R \in I$ Df par P

$\exists U, V \in \mathbb{K}[X]$, $R = P \times U + V$ $d^\circ V < d^\circ P$

$V = \underset{\in I}{R} - \underset{\in I}{P} \times U$, $\Rightarrow V \in I$ donc $V = 0$ sinon $d^\circ V \in C$ or $d^\circ V < C$ absurde

donc $R = PU \in P.\mathbb{K}[X]$

$\Rightarrow I = P.\mathbb{K}[X]$



2) Idéaux, Arithmétique dans $\mathbb{Z}$ et $\mathbb{K}[X]$

A : $\mathbb{Z}$ ou $\mathbb{K}[X]$

* <u>idéaux</u> (1) les idéaux de $\mathbb{Z}$ sont de la forme $n\mathbb{Z}$.

(2) les idéaux de $\mathbb{K}[X]$ ——— $P\,\mathbb{K}[X]$ avec $P \in \mathbb{K}[X]$.

générateur d'1 idéal :

$\boxed{\mathbb{Z}}$ idéal I :
- $I = \{0\} = 0\mathbb{Z}$ (0 seul générateur)
- $I \neq \{0\}$ $\exists! n \in \mathbb{N}$, $I = n\mathbb{Z}$ avec $n = \min(I \cap \mathbb{N}^*)$

$a, b \in \mathbb{Z}^*$ $a\mathbb{Z} = b\mathbb{Z} \Leftrightarrow a/b$ et $b/a \Rightarrow a = \pm b$

ens des inversibles $\longrightarrow U(\mathbb{Z}) = \{-1, 1\}$

1 seul générateur $n \in \mathbb{N}^*$ de I

$\boxed{\mathbb{K}[X]}$ idéal I :
- $I = \{0\} = 0\,\mathbb{K}[X]$
- $I \neq \{0\}$ $\exists! P \in \mathbb{K}[X]$, $I = P\,\mathbb{K}[X]$ P non unique ?

$2P\,\mathbb{K}[X] = P\,\mathbb{K}[X]$

$U(\mathbb{K}[X]) = \mathbb{K}$

il y a 1 seul générateur unitaire de coef dominant 1

$P = \sum_{k=0}^{p} a_k X^k$ $(a_k \in \mathbb{K})$; $d°P = p \in \mathbb{N}$, $a_p \neq 0$

P unitaire si $a_p = 1$

* <u>Prop</u> $\mathbb{K}$ corps comm

Etant donné I idéal non nul de $\mathbb{K}[X]$, il existe un <u>unique</u> $P \in \mathbb{K}[X]$, non nul, unitaire tq $I = P.\mathbb{K}[X]$.

P est le polynôme <u>minimum</u> de I

$d°P = \min\{d°Q,\ Q \in I \setminus \{0\}\}$

<u>NB</u> $R \neq 0$, $d°(R.P) = \underbrace{d°R}_{\geq 0} + d°P$

Ex $I = \{ U \in \mathbb{Q}[X] / U(\sqrt{2}) = 0 \}$

Mq I est un idéal de $\mathbb{Q}[X]$, trouver son PN minimal

▶ mq I SG de $(\mathbb{Q}[X], +)$

$I \subset \mathbb{Q}[X]$ $\quad 0 \in I$

$\forall P, Q \in I \quad P - Q \in I$

mq I idéal : $\forall P \in I \ \forall Q \in \mathbb{Q}[X], \ PQ \in I$

remarque : $f \left| \begin{array}{l} U \mapsto U(\sqrt{2}) \\ \mathbb{Q}[X] \to \mathbb{R} \end{array} \right.$ morphisme d'anneaux et $I = \mathrm{Ker}\, f$ donc ...

▶ soit $P_1 = X^2 - 2 \in I$, on cherche le PN minimal P

OSQ P / P_1 donc $d^\circ P \leq 2$

supposons que $d^\circ P = 0$: $P = 1$ ne s'annule pas en 1 impossible

——————————— 1 : $P = X - \sqrt{2} \notin \mathbb{Q}[X]$ impossible

donc $d^\circ P = 2$ or P / P_1 et P et P_1 unitaires

donc $P = P_1 = X^2 - 2$

Rem $\int$ nombres algébriques

$\alpha \in \mathbb{C}$ algébrique si $\exists P \in \mathbb{Q}[X]^*, P(\alpha) = 0$

$I_\alpha = \{ V \in \mathbb{Q}[X] / V(\alpha) = 0 \}$ idéal non nul de $\mathbb{Q}[X]$

* PGCD / PPCM dans $\mathbb{Z}$ / $\mathbb{K}[X]$

$\boxed{\mathbb{Z}}$ $a, b \in \mathbb{Z}^*$ $\quad a\mathbb{Z}$ ens des multiples de a, idéal de $\mathbb{Z}$

$a\mathbb{Z} + b\mathbb{Z}$ et $a\mathbb{Z} \cap b\mathbb{Z}$ idéaux de $\mathbb{Z}$

$d, m \in \mathbb{N}$ générateurs respectifs

$d = \mathrm{pgcd}(a,b)$: $d\mathbb{Z} = a\mathbb{Z} + b\mathbb{Z}$ ou $\left| \begin{array}{l} d/a \text{ et } d/b \\ \forall \delta \in \mathbb{Z}, \ \delta/a \text{ et } \delta/b \Rightarrow \delta/d \end{array} \right.$

$m = \mathrm{ppcm}(a,b)$: $m\mathbb{Z} = a\mathbb{Z} \cap b\mathbb{Z}$ ou $\left| \begin{array}{l} a/m \text{ et } b/m \\ \forall \mu \in \mathbb{Z}, \ a/\mu \text{ et } b/\mu \Rightarrow m/\mu \end{array} \right.$

$\boxed{\mathbb{K}[X]}$ $A, B \in \mathbb{K}[X]^*$

$A\mathbb{K}[X] + B\mathbb{K}[X]$ et $A\mathbb{K}[X] \cap B\mathbb{K}[X]$ idéaux de $\mathbb{K}[X]$

$D = \operatorname{pgcd}(A,B)$ caractérisé par $\left| \begin{array}{l} D \in \mathbb{K}[X] \text{ non nul, unitaire}, \ D\mathbb{K}[X] = A\mathbb{K}[X] + B\mathbb{K}[X] \end{array}\right.$

ou de façon équiv $\left| \begin{array}{l} D/A \text{ et } D/B \\ \forall \Delta \in \mathbb{K}[X] \quad \Delta/A \text{ et } \Delta/B \Rightarrow \Delta/D \end{array}\right.$

$M = \operatorname{ppcm}(A,B)$: $\left| \begin{array}{l} M \in \mathbb{K}[X] \text{ non nul, unitaire}, \ M\mathbb{K}[X] = A\mathbb{K}[X] \cap B\mathbb{K}[X] \end{array}\right.$

ou $\left| \begin{array}{l} A/M \text{ et } B/M \\ \forall \mu \in \mathbb{K}[X] \quad A/\mu \text{ et } B/\mu \Rightarrow M/\mu \end{array}\right.$

<u>Cf</u> : <u>dans $\mathbb{Z}$</u>

- <u>prop 1</u> soient $a, b \in \mathbb{Z}$, $d = \operatorname{pgcd}(a,b)$

  alors il existe $u, v \in \mathbb{Z}$, $au + bv = d$

  <u>démo</u> $d\mathbb{Z} = a\mathbb{Z} + b\mathbb{Z}$ et $d \in d\mathbb{Z}$ □

  <u>Rem</u> pr 1 telle relation si δ/a, δ/b alors δ/d

- <u>prop 2</u> $a, b \in \mathbb{Z}$ $\quad \operatorname{pgcd}(a,b) = 1 \Leftrightarrow \exists (u,v) \in \mathbb{Z}^2 ; au + bv = 1$

  démo $\Rightarrow$ cf 1

  $\Leftarrow$ $1 \in a\mathbb{Z} + b\mathbb{Z} = d\mathbb{Z}$ $\quad d = \operatorname{pgcd}(a,b)$

  $d/1$, $d = 1$ car $d \in \mathbb{N}$ □

- <u>prop 3</u> $a, b, c \in \mathbb{Z}$ $\quad$ si a/bc et $a \wedge b = 1$ alors a/c

  démo $\exists (u,v) \in \mathbb{Z}$ $\quad au + bv = 1$ $\quad auc + bvc = c$

  or $a/bc \Rightarrow a/bvc$, et $a/auc \Rightarrow a/auc + bvc$
  $\Rightarrow a/c$ □

idem ds $\mathbb{K}[X]$ ...

<u>Recherche pratique du pgcd ds $\mathbb{Z}$, ds $\mathbb{K}[X]$</u>

1) $|a| \geq |b|$ $\quad b \neq 0$ $\quad a = bq + r$ $\quad 0 \leq r < |b|$

   $\operatorname{pgcd}(a,b) = \operatorname{pgcd}(b,r)$ $\quad$ et $\operatorname{pgcd}(a,b) =$ dernier reste $\neq 0$

   idem ds $\mathbb{K}[X]$

2) utilisation des facteurs premiers ou irréductibles

   $\boxed{\mathbb{Z}}$ $\mathbb{P}$ ensemble des nbs premiers

   $a \in \mathbb{N}^*$ se factorise de manière unique $a = p_1^{\alpha_1} \times \dots \times p_r^{\alpha_r}$, $p_1 \dots p_r \in \mathbb{P}$

$a, b \in \mathbb{Z}^*$, $a = \pm\, p_1^{\alpha_1} \times \dots \times p_r^{\alpha_r}$ et $b = \pm\, p_1^{\beta_1} \times \dots \times p_r^{\beta_r}$

alors $d = a \wedge b = \prod_{i=1}^{r} p_i^{\min(\alpha_i, \beta_i)}$ $\quad$ $m = a \vee b = \prod_{i=1}^{r} p_i^{\max(\alpha_i, \beta_i)}$, $dm = |ab|$

$\boxed{\mathbb{K}[X]}$ $\mathbb{K}$ sous-corps de $\mathbb{C}$

$P \in \mathbb{K}[X]$ irréductible dans $\mathbb{K}[X]$ $\quad d°P \geq 1$ si pour tous

$Q, R \in \mathbb{K}[X]$, $P = QR$ alors Q ou R constant

facteurs irréductibles $\boxed{\text{dans } \mathbb{C}[X]}$: PN de degré 1

cf Th de D'Alembert - Gauss

Si $P \in \mathbb{C}[X]$, $d°P \geq 1$, alors P a une racine dans $\mathbb{C}$

Csq $P \in \mathbb{C}[X]$, $d°P \geq 1$

$z_1, \dots, z_r$ racines de multiplicité resp $\alpha_1, \dots, \alpha_r$; λ coef domi

P scindé dans $\mathbb{C}$: $P = \lambda \prod_{j=1}^{r} (X - z_j)^{\alpha_j}$

$\boxed{\text{dans } \mathbb{R}[X]}$ PN irréductibles : — PN de degré 1

— ——— 2, de discriminant < 0

Csq $P \in \mathbb{R}[X]$, $d°P \geq 1$; λ coef domi

factorisable sous la forme

$$P = \lambda \prod_{j=1}^{r} (X - z_j)^{m_j} \prod_{j=1}^{s} (X^2 + p_j X + q_j)^{n_j}$$

$P \in \mathbb{R}[X]$, $\alpha \in \mathbb{C} \setminus \mathbb{R}$ $\quad P(\alpha) = 0 \iff P(\bar{\alpha}) = 0$

$(\overline{P(\alpha)} = \bar{P}(\bar{\alpha}) = P(\bar{\alpha}))$

NB $P \in \mathbb{R}[X] \iff P = \bar{P}$

Ex $P = X^4 + 1$ $\quad$ ① $z^4 = -1 = e^{i\pi}$

$z_k = e^{\frac{i\pi}{4} + \frac{2ik\pi}{4}}$, $0 \leq k \leq 3$ $\quad z_0 = e^{i\pi/4}$ $\quad z_1 = i e^{i\pi/4}$ $\quad z_2 = -e^{i\pi/4}$

$z_3 = -i e^{i\pi/4} = \bar{z_0}$

$$X^4 + 1 = \left((X - e^{i\pi/4})(X - e^{-i\pi/4})\right)\left((X - e^{3i\pi/4})(X - e^{-3i\pi/4})\right)$$
$$= \left(X^2 - 2\cos\frac{\pi}{4} X + 1\right)\left(X^2 - 2X\cos\frac{3\pi}{4} + 1\right)$$

$$\Rightarrow X^4 + 1 = (X^2 - \sqrt{2} X + 1)(X^2 + \sqrt{2} X + 1)$$

② $X^4 + 1 = (X^2 + 1)^2 - 2X^2 = (X^2 - \sqrt{2} X + 1)(X^2 + \sqrt{2} X + 1)$

Csq recherche pgcd, ppcm

dans $\mathbb{K}[X]$ A, B factorisés en FI $\quad \begin{cases} A = \lambda P_1^{\alpha_1} \dots P_r^{\alpha_r} \\ B = \mu P_1^{\beta_1} \dots P_r^{\beta_r} \end{cases}$

$$\text{pgcd}(A, B) = \prod_{i=1}^{r} P_i^{\min(\alpha_i, \beta_i)} \; ; \; \text{ppcm}(A, B) = \prod_{i=1}^{r} P_i^{\max(\alpha_i, \beta_i)}$$

* $\mathbb{Z}/n\mathbb{Z}$ $\quad n \in \mathbb{N}, n \geq 2$

on a vu $(\mathbb{Z}/n\mathbb{Z}, +)$ groupe

congruence mod n dans $\mathbb{Z}$: $x, y \in \mathbb{Z}$ $\quad x \equiv y\,(n) \Leftrightarrow x-y \in n\mathbb{Z}$

$(\mathbb{Z}, +, \times)$ anneau

$s : \mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$, $k \mapsto \bar{k}$ | surject° canonique

$+$ dans $\mathbb{Z}/n\mathbb{Z}$ tq s morph de $(\mathbb{Z}, +)$ vers $(\mathbb{Z}/n\mathbb{Z}, +)$

$x, y, z \in \mathbb{Z}$, $x \equiv y\,(n) \Rightarrow xz \equiv yz\,(n)$

Def/Prop Soit $n \in \mathbb{N}$, $n \geq 2$

On définit $\times$ dans $\mathbb{Z}/n\mathbb{Z}$ par $\forall x, y$, $\bar{x} \times \bar{y} = \overline{xy}$

Alors $(\mathbb{Z}/n\mathbb{Z}, +, \times)$ est un anneau comm et

$s : k \mapsto \bar{k}$ morphisme d'anneaux de $\mathbb{Z}$ sur $\mathbb{Z}/n\mathbb{Z}$.

vérif $(\mathbb{Z}/n\mathbb{Z}, +)$ groupe comm comme

$\times$ assoc, comm, distrib / $+$, elt neutre $\bar{1}$

ex : $\bar{x} \times \bar{y} = \overline{xy} = \overline{yx} = \bar{y} \times \bar{x}$

Prop $n \in \mathbb{N}, n \geq 2$

(1) Les elts inversibles de $\mathbb{Z}/n\mathbb{Z}$ sont de la forme $\bar{k}$ où $k \in \mathbb{Z}$

et pgcd$(k, n) = 1$. $\varphi(n) = \text{Card}(U(\mathbb{Z}/n\mathbb{Z}))$

(2) $\mathbb{Z}/n\mathbb{Z}$ est un corps ssi n est premier

démo (1) $\Rightarrow$ si $\bar{k}$ inversible, $\exists k' \in \mathbb{Z} / \bar{k} \times \bar{k'} = \bar{1}$

$\Rightarrow \overline{kk'} = 1 \Rightarrow kk' \equiv 1\,(n)$

$\exists u, k' \in \mathbb{Z}$ $\underbrace{kk' + un = 1}_{\text{(Bézout)}}$, $\quad k \wedge n = 1$

$\Leftarrow$ si $k \wedge n = 1$ Bézout $\exists u, k' \in \mathbb{Z}$, $kk' + un = 1$

$\Rightarrow \bar{k}\bar{k'} = \bar{1}$

$\Rightarrow \bar{k}$ inversible $\square$

(2) Si n premier tout elt $k \in \{1, \ldots, n-1\}$ premier avec n

$\Rightarrow \bar{k} \in U(\mathbb{Z}/n\mathbb{Z})$

$\Rightarrow$ tous les elts $\neq \bar{0}$ de $\mathbb{Z}/n\mathbb{Z}$ inversibles. $\mathbb{Z}/n\mathbb{Z}$ corps

($\Leftarrow$) contraposée :

si n non premier $\exists r,s \in [\![1,n]\!]$, $n = r \times s$

avec $r<n$, $s<n$ d'où $\overline{0} = \overline{r} \times \overline{s}$ $\quad(\overline{n} = \overline{0})$

donc $\mathbb{Z}/n\mathbb{Z}$ non intègre $\to$ non corps $\square$

Ex/ Petit Th de Fermat

Soit $p \in \mathbb{P}$ alors (1) $\forall a \in \mathbb{Z}$, $a^p \equiv a\,[p]$

(2) $\forall a \in \mathbb{Z} \setminus p\mathbb{Z}$, $a^{p-1} \equiv 1\,[p]$

Démo (1) $p=2$ évident : un nb et son carré ont la même parité

* $a \in \mathbb{N}$, récurrence sur a
* $a = 0$ vrai
* $\mathcal{P}(a) \Rightarrow \mathcal{P}(a+1)$

$(a+1)^p = \sum_{0}^{p} \binom{p}{k} a^k$ si $1 \leq k \leq p-1$ alors $p \mid \binom{p}{k}$

$\left(k\binom{p}{k} = p\binom{p-1}{k-1} \right)$

$\left. \begin{array}{l} p \mid k\binom{p}{k} \\ p \wedge k = 1 \end{array} \right\} p \mid \binom{p}{k}$

$\Rightarrow (a+1)^p \equiv 1 + a^p\,[p]$

$\equiv 1 + a\,[p]$ (HR)

* $a \in \mathbb{Z}^-$, $-a \in \mathbb{N}$

$a^p = -(-a)^p \equiv -(-a)\,[p] \equiv a\,[p]$ $\square$

(2) $a \in \mathbb{Z}$, $\overline{a}^p = \overline{a} \Rightarrow \overline{a}.\overline{a}^{p-1} = \overline{a}$

$a \in \mathbb{Z} \setminus p\mathbb{Z} \Rightarrow \overline{a} \neq 0 \Rightarrow \overline{a}^{p-1} = \overline{1}$

$\Rightarrow a^{p-1} \equiv 1\,[p]$

Retour sur l'indicateur d'Euler

Mq pour $n, m \in \mathbb{N}$ $n \geq 2$, $m \geq 2$ $\operatorname{pgcd}(n,m) = 1$

alors $\varphi(nm) = \varphi(n)\varphi(m)$

Soit $f : \mathbb{Z}/nm\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$ – ① Vérifier que f isomorphisme d'anneaux.

$\overline{\overline{\overline{k}}} \longmapsto (\overline{k}, \overline{\overline{k}})$

② En déduire 1 isomorphisme entre $U(\mathbb{Z}/nm\mathbb{Z})$ et $U(\mathbb{Z}/n\mathbb{Z}) \times U(\mathbb{Z}/m\mathbb{Z})$

③ Conclure.

① f morphisme d'anneaux

NB : $\left| \begin{array}{l} A, B \text{ anneaux} \\ A \times B \text{ anneau pour les lois produits} \end{array} \right.$

$f(\overline{\overline{k}} \underset{\times}{+} \overline{\overline{k'}}) = (\overline{k} \underset{\times}{+} \overline{k'}, \overline{k} \underset{\times}{+} \overline{k'}) = (\overline{k}, \overline{k}) \underset{\times}{+} (\overline{k'}, \overline{k'})$ idem

$f(\overline{\overline{1}}) = (\overline{1}, \overline{1})$ neutre de $\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$

bijectif : cf m̂ card en départ/arrivée

inj moyen ! $k \in \mathbb{Z}$ $(\overline{k}, \overline{k}) = (\overline{0}, \overline{0}) \Rightarrow k \in n\mathbb{Z} \cap m\mathbb{Z}$

$k \in mn\mathbb{Z} \Rightarrow \overline{\overline{k}} = \overline{\overline{0}}$ $\quad n \wedge m = 1 \Rightarrow ppcm(n, m) = nm$

② $(\overline{k}, \overline{k})$ inversible ds $\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$ ssi $\left| \begin{array}{l} \overline{k} \in U(\mathbb{Z}/n\mathbb{Z}) \\ \overline{k} \in U(\mathbb{Z}/m\mathbb{Z}) \end{array} \right.$

2 résultats utiles

(1) $\left\{ \begin{array}{l} f : A \to B \text{ isomorphisme d'anneaux induit isomorphisme} \\ \text{de } U(A) \text{ sur } U(B) \end{array} \right.$

$a \in A$ inversible $\quad f(a)$ inversible ds B

$f(\underbrace{a \times a^{-1}}_{1_A}) = f(a) \cdot f(a^{-1}) = 1_B$

récip $b \in U_B \Rightarrow f^{-1}(b) \in U_A$

(2) $B = B' \times B''$ $\quad B', B''$ deux anneaux $\quad U_B = U_{B'} \times U_{B''}$

$b = (b', b'')$ si b inversible, $\exists\, b_1 = (b_1', b_1'')$

tq $b \times b_1 = (1_{B'}, 1_{B''})$ $\quad \left\{ \begin{array}{l} b' \times b_1' = 1_{B'} \\ b'' \times b_1'' = 1_{B''} \end{array} \right.$

Csq $f : U(\mathbb{Z}/nm\mathbb{Z}) \to U(\mathbb{Z}/n\mathbb{Z}) \times U(\mathbb{Z}/m\mathbb{Z})$

isomorphisme de groupes

$\to$ égalité des cardinaux donc :

Prop Soient $n, m \in \mathbb{N}^*$, tq $n \wedge m = 1$

Alors $\varphi(nm) = \varphi(n)\varphi(m)$

Csq Calcul de $\varphi(n)$

$n \in \mathbb{N}^*$, $\varphi(1) = 1$ $\quad n \geq 2$: décomp en FP

$n = p_1^{\alpha_1} \times \dots \times p_r^{\alpha_r}$ $\quad p_1^{\alpha_1}, \dots, p_r^{\alpha_r}$ premiers entre eux 2 à 2

$\varphi(n) = \prod_{i=1}^{r} \varphi(p_i^{\alpha_i})$ et OSQ $\varphi(p_i^{\alpha_i}) = p_i^{\alpha_i} - p_i^{\alpha_i - 1}$

$\Rightarrow \varphi(n) = n \times \prod_{i=1}^{r} \left(1 - \frac{1}{p_i}\right)$

Rem $\varphi(n)$ utile en crypto (cf DM 1)

Prop A anneau

Soit $f : \mathbb{Z} \to A$, $k \mapsto k.1_A$ **le** morphisme d'anneaux

On suppose que $\ker f = n\mathbb{Z}$ avec $n \in \mathbb{N}^*$

On peut définir alors $\hat{f} : \mathbb{Z}/n\mathbb{Z} \to A$, $\bar{k} \mapsto k 1_A$ morphisme d'anneaux

tq $f = \hat{f} \circ s$ où $s : k \mapsto \bar{k}$ surject° canonique.

vérifications : $\hat{f}$ bien défini

$\bar{k} \in \mathbb{Z}/n\mathbb{Z}$, k représentant de cette classe

$k 1_A$ indépendant de k :

k' autre représentant $k \equiv k' [n]$

$k - k' \in \ker f$; $(k - k') 1_A = 0 \Rightarrow k 1_A = k' 1_A$

$\hat{f}$ morphisme d'anneaux

- $\hat{f}(\bar{1}) = 1_A$
- $\hat{f}(\bar{k} \underset{\times}{+} \bar{k'}) = \hat{f}(\overline{k \underset{\times}{+} k'}) = (k \underset{\times}{+} k') 1_A = k 1_A \underset{\times}{+} k' 1_A = \hat{f}(\bar{k}) \underset{\times}{+} \hat{f}(\bar{k'})$

$\ker \hat{f} = \{ \bar{k} / k \in n\mathbb{Z} \} = \{ \bar{0} \} \to \hat{f}$ inj

Retour à l'ex précédent $n, m \in \mathbb{N}^*$ $n \wedge m = 1$

$A = \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$

$f : \mathbb{Z} \to A$, $k \mapsto (\bar{k}, \bar{\bar{k}}) = k(e_n, e_m)$ $e_n = \bar{1}$, $e_m = \bar{\bar{1}}$

$\ker f = n\mathbb{Z} \cap m\mathbb{Z}$

soit $\hat{f} : \mathbb{Z}/nm\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$ isomorphisme

$f = \hat{f} \circ s \to f$ surjective

$\forall (\bar{u}, \bar{\bar{v}}) \in \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z} \quad \exists k \in \mathbb{Z} \quad \left| \begin{array}{l} \bar{k} = \bar{u} \\ \bar{\bar{k}} = \bar{\bar{v}} \end{array} \right.$

u et v donnés, système $\left| \begin{array}{l} k \equiv u \, [n] \\ k \equiv v \, [m] \end{array} \right.$

<u>résolution pratique</u> • recherche de sol part k_0

$n \wedge m = 1$, $\exists a, b \in \mathbb{Z}$ $\quad na + mb = 1$ $\to$ $nau + mbu = u$ $\to$ $mbu \equiv u \, [n]$

on prend $k_0 = nav + mbu \equiv mbu \, [n]$

$\longrightarrow \left| \begin{array}{l} k_0 \equiv u \, [n] \\ k_0 \equiv v \, [m] \end{array} \right.$

• sol générale k

$k \in \mathcal{S} \Leftrightarrow k - k_0 \in n\mathbb{Z} \wedge m\mathbb{Z}$ $\quad \mathcal{S} = \{k_0 + tnm \, / t \in \mathbb{Z}\}$

<u>ex</u> $\quad x \in \mathbb{Z}$ $\quad \left\{ \begin{array}{l} x \equiv 1 \, (4) \\ x \equiv 2 \, (5) \end{array} \right.$ $\quad 4 \wedge 5 = 1$

$5 \times 1 - 4 \times 1 = 1$

$k_0 = 5 \times 1 - 4 \times 2 = -3$

$\mathcal{S} = \{3 + 20t \, / \, t \in \mathbb{Z}\} = \{17 + 20t \, / \, t \in \mathbb{Z}\}$

<u>Def</u> $\quad$ <u>Caractéristique d'1 anneau A</u>

$f : \begin{array}{l} k \mapsto k 1_A \\ \mathbb{Z} \longrightarrow A \end{array}$ morphisme d'anneaux

Ker f idéal de $\mathbb{Z}$ de la forme $n\mathbb{Z}$ avec $n \in \mathbb{N}$

n est la caractéristique de A.

• $n = 0$

• $n \in \mathbb{N}^*$ $\quad k 1_A = 0 \Leftrightarrow n / k$

A intègre et en particulier A corps

$\to$ soit $n = 0$ soit n premier

en effet si $n \neq 0$ si n non premier $\quad n = r \times s$ $\quad \begin{array}{l} r < n \\ s < n \end{array}$

$n 1_A = 0 = (r 1_A) \times (s 1_A) \Rightarrow r 1_A = 0 \Rightarrow n / r$
ou $s 1_A = 0 \quad n / s$ $\quad$ ABSURDE

Ex : * $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ de caractéristique nulle

* $\mathbb{Z}/m\mathbb{Z}$ avec $m \in \mathbb{N}^*$, $m \geq 2$: de caract m