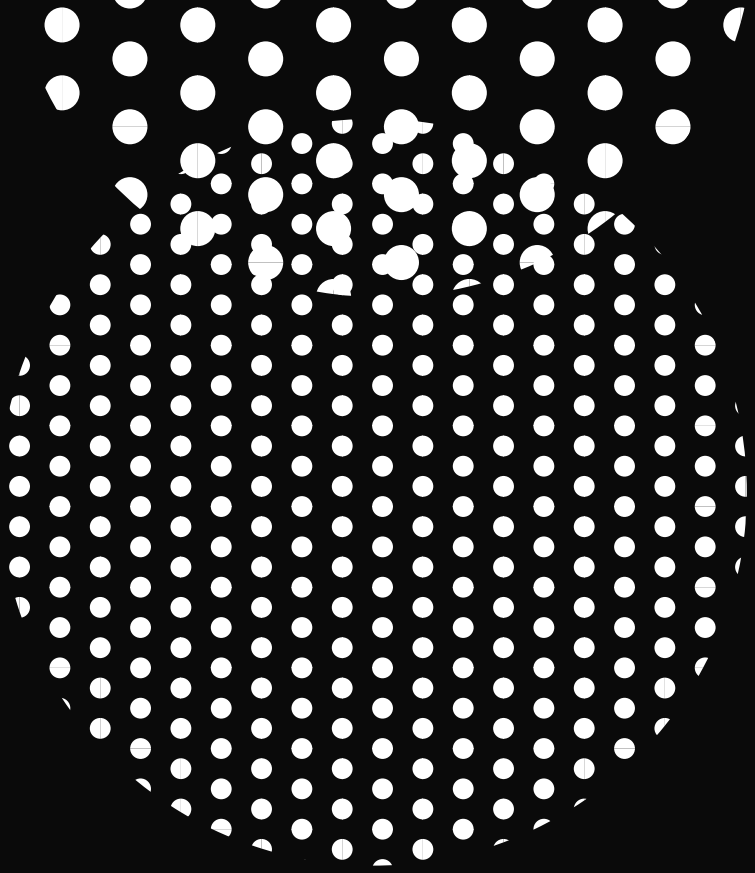


Déf: Soit $A=(A,+,\times)$. On note
$A^\times = \{a \in A : \exists a' \in A \text{ avec } aa' = 1_A\}$ groupe des inversibles de A

Ex: $\mathbb{Z}^\times = \{-1, 1\}$ **Ex:** $\mathbb{Z}/n\mathbb{Z} = \{\bar{a} : a \wedge n = 1\}$

Bézout*: $\exists u, v \in \mathbb{Z}$ $(au + nv = 1) \mod n$
$\bar{a}\bar{u} = 1$

Ass°: $(A^\times, \times)$ est un groupe

Obs: a' unique

Pbm: Bcp de $\mathbb{Z}/n\mathbb{Z}$
Comparer entre eux?

Idée: $\mathbb{Z}/mn\mathbb{Z} \rightsquigarrow \mathbb{Z}/m\mathbb{Z}$ et $\mathbb{Z}/n\mathbb{Z}$

Préliminaire théorique:

Déf: A, B anneaux commutatifs, $(A, +_A, \times_A)$, $(B, +_B, \times_B)$ (commutatifs)

$A \times B := \{(a,b) : a \in A, b \in B\}$
$(a,b)+(a',b') := (a+a', b+b')$
$(a,b)\times(a',b') := (a\times a', b\times b')$

$1_{A\times B} = (1_A, 1_B)$
$0_{A\times B} = (0_A, 0_B)$

Prop: Le gpe (groupe) des inversibles $(A\times B)^\times = A^\times \times B^\times$
NV: $(a,b)\times(a',b') = (aa', bb') = (1,1)$
a' inverse de a, b' inverse de b

$|\mathbb{Z}/mn\mathbb{Z}| = mn$ $|\mathbb{Z}/m\mathbb{Z}| = m$ $|\mathbb{Z}/n\mathbb{Z}| = n$
$\{\bar{0}, \bar{1}, \dots, \overline{n-1}\}$

Rappel: E, $|E| < \infty$, F, $|F| < \infty$

E => $|E \times F| = |E| \cdot |F|$

? même chose ?

Ici: $|\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}| = m \cdot n = |\mathbb{Z}/mn\mathbb{Z}|$

Iso := "le même" MORPHISME = "application conservant la forme"

Isomorphismes:

$$\mathbb{Z}/mn\mathbb{Z} \xrightarrow[\text{bijection}]{f} \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$$

f morphisme d'anneaux

Déf: Un **morphisme** d'anneaux, c'est une appl

$$(A, +_A, \times_A) \xrightarrow{f} (B, +_B, \times_B)$$

satisfaisant

(1) $f(a +_A a') = f(a) +_B f(a')$ $\forall a, a' \in A$

(2) $f(a \times_A a') = f(a) \times_B f(a')$

(3) $f(0_A) = 0_B$

(4) $f(1_A) = 1_B$

Rem: Si f bijective, on dit isomorphisme

Déf: Noyau déf $\operatorname{Ker} f := \{a \in A : f(a) = 0_B\}$

Image déf $\operatorname{Im} f := \{b \in B : \exists a \in A, f(a) = b\}$
$:= \{f(a) \in B : a \in A\}$

Déf: Un sous-anneau B d'un anneau A, c'est un ss-ensemble satisfaisant

(1) $\forall b, b' \in B$ $b +_A b' \in B$

(2) $\forall b, b' \in B$ $b \times_A b' \in B$

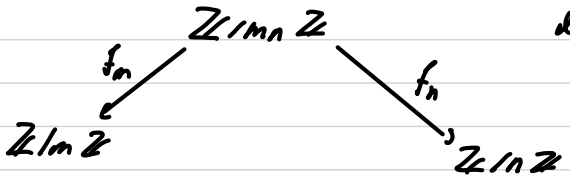
(3) $1_A \in B$, $0_A \in B$

Fait: $(B, +_A|_B, \times_A|_B)$

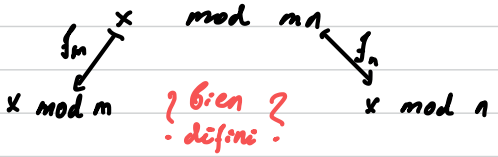
Thm*?: Si $m \wedge n = 1$ alors $\mathbb{Z}/mn\mathbb{Z}$ et $\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ sont isomorphes

+ motivation poly

pv:



deux morphismes



? bien ? défini !

$x = x' + k\,mn$

$x = x'$ dans $\mathbb{Z}/mn\mathbb{Z}$

$x \bmod m$; $x' \bmod m$

$x - x' = k\,mn$

$= (kn)\,m$

$x - x' \equiv 0 \bmod m$

CCL: L'image de $x \bmod mn$ dans $\mathbb{Z}/m\mathbb{Z}$ ne dépend que de x, x', x'' : choisi

f_m et f_n bien définies

Aff°: f_m est un morphisme d'anneaux

pv: $a + mn\,k$, $b + mn\,l$ $\rightsquigarrow$ $a + mnk + b + mnl \bmod m$

autres représentants $a + mnk'$, $b + mnl'$ $\rightsquigarrow$ $a + mnk' + b + mnl' \bmod m$

Donc on a bien $f_m(\bar{a} + \bar{b}) = f_m(\bar{a}) + f_m(\bar{b})$

($\bar{a}, \bar{b}$ dans $\mathbb{Z}/mn\mathbb{Z}$; $+$ addition dans $\mathbb{Z}/m\mathbb{Z}$)

De même, on vérifie que $f_m(\bar{a} \times \bar{b}) = f_m(\bar{a}) \times f_m(\bar{b})$

($\bar{a}, \bar{b}$ dans $\mathbb{Z}/mn\mathbb{Z}$; $\times$ dans $\mathbb{Z}/m\mathbb{Z}$)

Enfin, $f_m(\bar{0}) = \bar{0}$, $f_m(\bar{1}) = \bar{1}$

Thm *7 : Si $m \wedge n = 1$ alors $\mathbb{Z}/mn\mathbb{Z}$ et $\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ sont isomorphes

$m = n = 2$ pas isomorphisme

$$f : \mathbb{Z}/mn\mathbb{Z} \longrightarrow \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$$
$$x \bmod mn \longmapsto (x \bmod m,\ x \bmod n)$$
$$x \longmapsto (f_m(x),\ f_n(x))$$

sont des morphismes

f est un isomorphisme OK

isomorphismes = bijection morphismes vu

Coordonnées égaux à gauche et à droite $= mn$

Rappel : $E \xrightarrow{f} F$ avec $|E| = |F| < +\infty$

f bijection $\Leftrightarrow$ f injection

Il suffit ici de mq f injective

Soient $x, x' \in \mathbb{Z}/mn\mathbb{Z}$ avec :
$f(x) = f(x')$ But : mq $x = x'$

f morphisme $\Downarrow$
$f(x - x') = f(x) - f(x') = 0_{\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}}$

y

$y \in \mathbb{Z}/mn\mathbb{Z}$ $\Updownarrow$ $f(y) = (0,0)$ dans le produit

$(y \bmod m,\ y \bmod n) = (0,0)$

y est mult de m $\quad y = mk = n\ell$ (m div mais $mn = 1$ donc $m \mid \ell$ donc $\ell = m\ell'$)
et y est mult de n
$\Downarrow$
donc y mult de mn $\quad y = kmn\ell' \equiv 0 \bmod mn$
$y = \bar{0}$ dans $\mathbb{Z}/mn\mathbb{Z}$
càd $x = x'$ ——— □

Thm: En restriction aux gpes des inversibles

$$(\mathbb{Z}/mn\mathbb{Z})^\times \xrightarrow[f]{\sim} (\mathbb{Z}/m\mathbb{Z})^\times \times (\mathbb{Z}/n\mathbb{Z})^\times$$

Bijection

est un isomorphisme de groupes pour la multiplication

a avec $\exists a', aa' = 1$
b avec $\exists b', bb' = 1$
$\Rightarrow$ ab a l'inverse $a'b'$

Rappel: Indicatrice d'Euler $\varphi(n) := \text{Card}\{1 \le a \le n : a \wedge n = 1\}$
$= \text{Card}\{1 \le a \le n, \exists n, an = 1\}$
$= \text{Card}\,(\mathbb{Z}/n\mathbb{Z})^\times$

Cor: $|(\mathbb{Z}/mn\mathbb{Z})^\times| = |(\mathbb{Z}/m\mathbb{Z})^\times| \cdot |(\mathbb{Z}/n\mathbb{Z})^\times|$
$\varphi(mn) = \varphi(m) \cdot \varphi(n)$ quand $m \wedge n = 1$

Thm: Si $n = p_1^{\alpha_1} \cdots p_r^{\alpha_r}$ déco en nbres premiers d'un $n \in \mathbb{N}$, ≥ 2 alors $\varphi(n) = (p_1^{\alpha_1} - p_1^{\alpha_1 - 1}) \cdots (p_r^{\alpha_r} - p_r^{\alpha_r - 1})$

Pv: $\varphi(n) = \varphi(p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_r^{\alpha_r}) = \varphi(p_1^{\alpha_1}) \cdot \varphi(p_2^{\alpha_2}) \cdots \varphi(p_r^{\alpha_r})$

car deux nbres premiers $\neq$ sont tjrs premiers entre eux

Lm: $\varphi(p^\alpha) = p^\alpha - p^{\alpha-1}$ où $p \in \mathcal{P}$ $\alpha \ge 1$

Pv: $\varphi(p^\alpha) = \text{Card}\{1 \le k \le p^\alpha : k \wedge p^\alpha = 1\}$ On regarde le complémentaire
$F := \{1 \le l \le p^\alpha : l \text{ et } p^\alpha \text{ pas premiers entre eux}\}$
$\iff l = pl'$ avec $l \in \mathbb{N}$ et $1 \le l' \le p^{\alpha-1}$, l' qlcq
donc il y a $p^{\alpha-1}$ entiers l non premiers avec p^α
donc il y'en a $p^\alpha - p^{\alpha-1}$ qui sont premiers avec p^α
□

Obs: Thm Fermat: $\forall a \wedge p,\ p \in \mathcal{P}$ $\quad a^{p-1} \equiv 1 \mod p$

$a^{p-1} = \bar{1}$ dans $\mathbb{Z}/p\mathbb{Z}$ corps

$a\,a^{p-2} = 1$

a^{p-2} l'inverse de a

Thm Euler*: Pour $n \in \mathbb{N}_{\geq 1}$, dans $\mathbb{Z}/n\mathbb{Z}$, $\forall a \in \mathbb{Z}$ avec $a \wedge n = 1$, on a

$a^{\varphi(n)} \equiv 1 \mod n$

OBS: $\varphi(p^1) = p^1 - p^0 = p - 1$

$= \{1 \leq k \leq p : k \wedge p = 1\} = \{1, 2, \dots, p-1\}$

pv: HYP $a \wedge n = 1$ **Aff°:** L'appl $(\mathbb{Z}/n\mathbb{Z})^\times \longrightarrow (\mathbb{Z}/n\mathbb{Z})^\times$ est une Bij°

$x \longmapsto ax = y$

$a^{-1}y \longleftarrow y$ d'inverse □

Csqce: $\{x \in (\mathbb{Z}/n\mathbb{Z})^\times\} = \{ax : x \in (\mathbb{Z}/n\mathbb{Z})^\times\}$

Produits: $\prod_{x \in (\mathbb{Z}/n\mathbb{Z})^\times} x = \prod_{x \in (\mathbb{Z}/n\mathbb{Z})^\times} ax$

$= a^{\varphi(n)} \prod_{x \in (\mathbb{Z}/n\mathbb{Z})^\times} x$

$1 = a^{\varphi(n)}$

□

$\varphi(n)$ termes dans ces produits

a est une constante