Théorème.

Les trois propriétés suivantes sont équivalentes :

(i) $(\mathbb{Z}/n\mathbb{Z}, +, \times)$ est un corps ;

(ii) $(\mathbb{Z}/n\mathbb{Z}, +, \times)$ est un anneau intègre ;

(iii) n est premier.

Notation. Pour p nombre premier, on note $\mathbb{F}_p$ le corps $\mathbb{Z}/p\mathbb{Z}$.

Preuve: $\boxed{i \Rightarrow ii}$ clair

(On suppose que $\mathbb{Z}/n\mathbb{Z}$ corps, ie $\forall x \in \mathbb{Z}/n\mathbb{Z} \setminus \{\bar{0}\}$, x inversible

Soit $x, y \in \mathbb{Z}/n\mathbb{Z}$ tq $xy = \bar{0}$

Si $x \neq \bar{0}$, $x^{-1} x y = x^{-1} \bar{0}$

ie $y = \bar{0}$)

$\boxed{(ii) \Rightarrow (iii)}$ par contraposée.

On suppose que n n'est pas premier, $\exists a, b$ tq $n = ab$

où $a \in \{2, .., n-1\}$ et $b \in \{2, .., n-1\}$

Alors $\bar{a}\,\bar{b} = \bar{n}$

$= \bar{0}$

et pourtant $\bar{a} \neq \bar{0}$ et $\bar{b} \neq \bar{0}$

car $n \nmid a$ et $n \nmid b$

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

$\boxed{(iii) \Rightarrow (i)}$ On suppose n premier.

Montrons $\mathbb{Z}/n\mathbb{Z}$ est un corps ie $(\mathbb{Z}/n\mathbb{Z})^* = \mathbb{Z}/n\mathbb{Z} \setminus \{\bar{0}\}$

$\forall k \in \{1, .., n-1\}, \quad k \wedge n = 1$

donc $\exists u, v$ tq $ku + nv = 1$

donc $\bar{k}\,\bar{u} = \bar{1}$ dans $\mathbb{Z}/n\mathbb{Z}$

donc $\bar{k} \in (\mathbb{Z}/n\mathbb{Z})^*$

<u>Remarque:</u> A anneau fini

A intègre $\Leftrightarrow$ A corps

<u>Preuve:</u> Soit $x \in A \setminus \{0\}$

<u>Mq x inversible</u>.

Soit $\varphi : A \longrightarrow A$

$y \longmapsto xy$

- φ est un morphisme de groupe $(A, +)$

$\forall y, z \in A, \quad \varphi(y+z) = x(y+z)$

$= xy + xz$

$= \varphi(y) + \varphi(z)$

- $y \in \ker \varphi \Leftrightarrow \varphi(y) = 0$

$\Leftrightarrow xy = 0$ avec $x \neq 0$

$\Leftrightarrow y = 0$ A intègre

donc $\ker \varphi = \{0\}$

$\varphi : A \to A$

donc φ injective

- A de cardinal fini

donc φ est surjective

donc $1_A \in \operatorname{Im} \varphi$:

$\exists y \in A$ tq $\varphi(y) = 1$

i.e. $xy = 1$

donc x inversible, d'inverse y.

Rmq : φ morphisme d'anneau

lorsque : $\begin{cases} \varphi(x+y) = \varphi(x) + \varphi(y) \\ \varphi(x \times y) = \varphi(x) \times \varphi(y) \\ \varphi(1) = 1 \end{cases}$

4 Le théorème chinois

4.1 Présentation du problème chinois

Exemple.

1. Déterminer une relation de Bézout entre 14 et 25.

2. Déterminer x_1 et x_2 dans $\mathbb{Z}$ tels que :

$$\begin{cases} x_1 \equiv 1\ [14] \\ x_1 \equiv 0\ [25] \end{cases} \quad \text{et} \quad \begin{cases} x_2 \equiv 0\ [14] \\ x_2 \equiv 1\ [25] \end{cases}$$

3. Utiliser x_1 et x_2 pour déterminer une solution du système :

$$\begin{cases} x \equiv 2\ [14] \\ x \equiv 3\ [25] \end{cases}$$

4. Déterminer toutes les solutions du système précédent.

1. Algo. d'Euclide:

$$25 = 14 \times 1 + \boxed{11}$$
$$14 = 11 \times 1 + \boxed{3}$$
$$11 = 3 \times 3 + \boxed{2}$$
$$3 = 2 \times 1 + \boxed{1}$$

donc
$$\boxed{1} = 3 - \boxed{2} \times 1$$
$$= 3 - (11 - 3 \times 3) \times 1$$
$$= -11 + 4 \times \boxed{3}$$
$$= -11 + 4(14 - 11)$$
$$= 4 \times 14 - 5 \times \boxed{11}$$
$$= 4 \times 14 - 5(25 - 14)$$
$$= -5 \times 25 + 9 \times 14$$

(b) $1 = -5\times 25 + 9\times 14$

donc $1 \equiv -5\times 25 \quad [14]$

donc $x_1 = -125$ convient

et $1 \equiv 9\times 14 \quad [25]$

donc $x_2 = 9\times 14$ convient

$= 126$

(c) Notons $x = 2x_1 + 3x_2$

on a $x \equiv 2x_1 + 3x_2 \quad [14]$

$\equiv 2 + 0 \quad [14]$

et $x \equiv 2x_1 + 3x_2 \quad [25]$

$\equiv 0 + 3 \quad [25]$

Donc $x = 3\times 126 - 2\times 125$

$= 3 + 3\times 125 - 2\times 125$

$= 128$

(d) y sol $\Leftrightarrow \begin{cases} y \equiv 2 \quad [14] \\ y \equiv 3 \quad [25] \end{cases}$

$\Leftrightarrow \begin{cases} y \equiv x \quad [14] \\ y \equiv x \quad [25] \end{cases}$

$$\iff \begin{cases} 14 \mid y-x \\ 25 \mid y-x \end{cases}$$

$$\iff 14 \times 25 \mid y-x$$

car $14 \wedge 25 = 1$

$$\iff \exists k \in \mathbb{Z} \text{ tq } y = 128 + k \times 14 \times 25$$

$$= 128 + k \times 350$$

$$y = \{ 128 + k\,350 \,,\; k \in \mathbb{Z} \}$$

Remarque. *Pourquoi le système :*

$$\begin{cases} x & \equiv 2\ [26] \\ x & \equiv 3\ [38] \end{cases}$$

n'a pas de solution ?

Si $x \equiv 2 \quad [26]$

$\exists k \in \mathbb{Z}$ tq $x = 2 + 26k$

$\equiv 0 \quad [2]$ pair

Si $x \equiv 3 \quad [38]$

$\exists k' \in \mathbb{Z}$ tq $x = 3 + 38k'$

$\equiv 1 \quad [2]$ impair

absurde

4.2 Structure d'anneau produit

Définition. Soit $(A, +, *)$ et $(B, +, \star)$ deux anneaux. On définit **l'anneau produit** en munissant le produit cartésien $A \times B$ des lois :

$$(a, b) + (a', b') = (a + a', b + b')$$
$$(a, b) \times (a', b') = (a * a', b \star b')$$

Proposition. Muni de cette structure, $A \times B$ est un anneau.

Remarque. *On peut étendre cette définition et cette proposition au cas d'un nombre fini d'anneaux.*

Preuve :

- Mque $(A \times B, +)$ groupe
  - $+$ loi de compostn interne ie

    $\forall (a, b), (a', b') \in A \times B$

    $(a, b) + (a', b') = (\underbrace{a + a'}_{\in A}, \underbrace{b + b'}_{\in B})$

    $\in A \times B$

  - Existence d'un neutre

    $\forall (a, b) \in A \times B$

    $(0_A, 0_B) + (a, b) = (0_A + a, 0_B + b)$
    $= (a, b)$
    $= (a, b) + (0_A, 0_B)$

    donc $(0_A, 0_B)$ neutre de $(A \times B, +)$

  - Existence d'un symétrique (opposé)

    $\forall (a, b) \in A \times B$

    $(a, b) + (\underset{\text{dans } A}{-a}, \underset{\text{dans } B}{-b}) = (a - a, b - b)$

$$= (0,0)$$
$$= (-a,-b)+(a,b)$$

donc $-(a,b) = (-a,-b)$

- $+$ est commutatif.

$\forall (a,b),(a',b') \in A\times B$

$$(a,b)+(a',b') = (a+a', b+b')$$
$$= (a'+a, b'+b)$$
$$= (a',b')+(a,b)$$

- Loi $\times$ est une loi de composition interne

$\forall (a,b),(a',b') \in A\times B$

$$(a,b)\times(a',b') = (\overbrace{a * a'}^{\in A}, \overbrace{b * b'}^{\in B})$$
$$\in A\times B$$

- Existence d'un neutre pour $\times$

$\forall (a,b)\in A\times B$

$$(1_A, 1_B)\times(a,b) = (1_A * a, 1_B * b)$$
$$= (a,b)$$
$$= (a,b)\times(1_A, 1_B)$$

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

• distributivité

$\forall (a,b), (a',b'), (a'',b'')$

$(a,b) \times ((a',b') + (a'',b''))$

$= [\dots]$

4.3 À propos de la notation

Remarque. *Pour $a \in \mathbb{Z}$, on note $\overline{a}$ l'élément de $\mathbb{Z}/n\mathbb{Z}$ qui est la classe de a. Mais si on travaille à la fois dans $\mathbb{Z}/n\mathbb{Z}$ et $\mathbb{Z}/m\mathbb{Z}$, la notation devient ambiguë.*

Notation. Pour $n \geqslant 2$ et $a \in \mathbb{Z}$, on note :

$$(a \bmod n) \text{ ou } [a]_n$$

la classe de a modulo n, que l'on note aussi $\overline{a}$ lorsqu'il n'y a pas d'ambiguité.

Exemple. Préciser le diagramme de l'application :

$$\phi \;:\; a \mapsto (a \bmod 14, a \bmod 25)$$

Est-ce un morphisme d'anneaux ?
Quel est son noyau ?

Sol $x \in \mathbb{Z}/14\mathbb{Z}$ ie $\exists a \in \mathbb{Z}$ tq $x = \overline{a}^{14} = (a \bmod 14)$

$y \in \mathbb{Z}/25\mathbb{Z}$ ie $\exists b \in \mathbb{Z}$ tq $y = \overline{b}^{25} = (b \bmod 25)$

$$\phi : \mathbb{Z} \longrightarrow \mathbb{Z}/14\mathbb{Z} \times \mathbb{Z}/25\mathbb{Z}$$
$$a \longmapsto (a \bmod 14,\ a \bmod 25)$$

§41. $\boxed{4}$ on cherche $\begin{cases} x \equiv 2 \ [14] \\ x \equiv 3 \ [25] \end{cases}$

ie x tq $\phi(x) = (2 \bmod 14,\ 3 \bmod 25)$

$$S = \phi^{-1}\left(\{(2 \bmod 14, 3 \bmod 25)\}\right)$$

<u>ϕ morphisme d'anneaux</u> :

$$\phi(a+b) = \left((a \underset{\mathbb{Z}}{+} b) \bmod 14,\ (a+b) \bmod 25\right)$$
$$= \left(a \bmod 14 \underset{\mathbb{Z}/14\mathbb{Z}}{+} b \bmod 14,\ \dots\right)$$
$$= (a \bmod 14,\ a \bmod 25) \underset{\mathbb{Z}/14\mathbb{Z} \times \mathbb{Z}/25\mathbb{Z}}{+} \dots$$
$$= \phi(a) + \phi(b)$$

$$\phi(a \times b) = (a \times b \bmod 14,\ a \times b \bmod 25)$$
$$= (a \bmod 14 \times b \bmod 14,\ \dots)$$
$$= (a \bmod 14,\ a \bmod 25) \times (\dots$$
$$= \phi(a) \times \phi(b)$$

$$\phi(1) = (1 \bmod 14,\ 1 \bmod 25)$$
$$= 1_{\mathbb{Z}/14\mathbb{Z} \times \mathbb{Z}/25\mathbb{Z}}$$

donc ϕ morphisme d'anneaux.

- $a \in \ker \phi$

$$\iff \phi(a) = (0,0)$$

$$\iff \begin{cases} a \bmod 14 = 0_{\mathbb{Z}/14\mathbb{Z}} \\ a \bmod 25 = 0_{\mathbb{Z}/25\mathbb{Z}} \end{cases}$$

$$\iff \begin{cases} a \equiv 0 \ [14] \\ a \equiv 0 \ [25] \end{cases}$$

lemme de Gauss

$$\iff a \equiv 0 \ [\underbrace{350}_{14 \times 25}]$$

Donc $\ker \phi = \{ a \in \mathbb{Z} \text{ tq } a \equiv 0 \ [350] \}$

4.4 Le théorème chinois

Théorème chinois.

> Soit m, n entiers $\geqslant 2$, premiers entre eux. Alors l'application :
>
> $$\phi \quad \begin{array}{rcl} \mathbb{Z}/mn\mathbb{Z} & \to & \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z} \\ a \bmod mn & \mapsto & (a \bmod m, a \bmod n) \end{array}$$
>
> est correctement définie, et est un isomorphisme d'anneaux.

Remarque. *Si l'on dispose d'une relation de Bézout :*

$$mu + nv = 1$$

l'isomorphisme réciproque est :

$$(a \bmod m, b \bmod n) \mapsto (anv + bmu \bmod mn)$$

Preuve: • ϕ est bien défini

$$\phi : \mathbb{Z}/mn\mathbb{Z} \longrightarrow (\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z})$$

$$x \longmapsto (a \bmod m, a \bmod n)$$

où $x = (a \bmod mn)$

donc la déf dépend a priori du choix de a, représentant de la classe x dans $\mathbb{Z}/mn\mathbb{Z}$.

Soit b un autre représentant de x.

ie $a \equiv b \; [mn]$ $\left(\begin{array}{l} a \in x \\ b \in x \end{array}\right)$

donc $\exists k \in \mathbb{Z}$

$$a = b + kmn$$

donc $\begin{cases} a \equiv b & [m] \\ a \equiv b & [n] \end{cases}$

donc $(a \bmod m, a \bmod n) = (b \bmod m, b \bmod n)$

- ϕ morphisme d'anneaux.

  ([...])

- $x \in \operatorname{Ker}\phi \iff \phi(x) = 0_{\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}}$

$x = (a \bmod mn)$

$$\iff \begin{cases} a \equiv 0 \ [m] \\ a \equiv 0 \ [n] \end{cases}$$

$$\iff a \equiv 0 \ [mn]$$

$$\iff x = (0 \bmod mn)$$

donc ϕ <u>injective</u>

- $\operatorname{Card}(\mathbb{Z}/mn\mathbb{Z}) = mn$

  $\operatorname{Card}(\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}) = m \times n$

  donc ϕ isomorphisme.

<u>Rmq.</u> Pour résoudre $\begin{cases} x \equiv 2 \ [14] \\ x \equiv 3 \ [25] \end{cases}$

on cherche 1 sol particulière (128)

$14 \wedge 25 = 1$ donc par le th Chinois

$\mathcal{S} = \{128 + 350k, \ k \in \mathbb{Z}\}$

Corollaire. Soit m, n entiers $\geqslant 2$, premiers entre eux. Alors le système de congruences :

$$\begin{cases} x \equiv a\ [m] \\ x \equiv b\ [n] \end{cases}$$

admet au moins une solution $x_0 \in \mathbb{Z}$.
L'ensemble des solutions est $x_0 + mn\mathbb{Z}$.

Généralisation. Soit $n_1, \ldots, n_k$ entiers $\geqslant 2$, deux à deux premiers entre eux, alors :

$$\begin{array}{ccc} \mathbb{Z}/(n_1 \ldots n_k)\mathbb{Z} & \to & \mathbb{Z}/n_1\mathbb{Z} \times \cdots \times \mathbb{Z}/n_k\mathbb{Z} \\ a \bmod n_1 \ldots n_k & \mapsto & (a \bmod n_1, \ldots, a \bmod n_k) \end{array}$$

est correctement définie, et est un isomorphisme d'anneaux.

Exemple. Résoudre le système de congruences :

$$\begin{cases} n \equiv 4\ [5] \\ n \equiv 1\ [7] \end{cases}$$

- Relation de Bézout par algo d'Euclide :

$$7 = 5 \times 1 + 2$$

$$5 = 2 \times 2 + 1$$

donc $1 = 5 - 2 \times 2$

$$= 5 - 2 \times (7 - 5)$$

$$= -2 \times 7 + 3 \times 5$$

- Posons $n_0 = -2 \times 7 \times 4 + 3 \times 5 \times 1 = -41$

alors $n_0 \equiv -2 \times 7 \times 4 \quad [5]$

$$\equiv -2 \times 7 \times 4 + 3 \times 5 \times 4 \quad [5]$$

$$\equiv 1 \times 4 \quad [5]$$

et $n_0 \equiv 1 \quad [7]$

- $5 \wedge 7 = 1$ donc par le th chinois

$$\mathcal{S} = \{-41 + 35k,\ k \in \mathbb{Z}\}$$

5 Indicatrice d'Euler

Rappel. Pour $n \geqslant 2$, $\varphi(n)$ désigne le nombre d'inversibles de $(\mathbb{Z}/n\mathbb{Z}, +, \times)$, ou encore le nombre d'entiers premiers avec n parmi $\{0, \ldots, n-1\}$, ou encore le nombre de générateurs du groupe cyclique $(\mathbb{Z}/n\mathbb{Z}, +)$.

Théorème d'Euler. Soit n entier, $n \geqslant 2$ et $a \in \mathbb{Z}$. Si a est premier avec n, alors $a^{\varphi(n)} \equiv 1\ [n]$.

Corollaire (petit théorème de Fermat). Soit p un nombre premier. Pour tout a non multiple de p, $a^{p-1} \equiv 1\ [p]$.

Théorème.

Soit $m, n \in \mathbb{N}^*$. Si m et n sont premiers entre eux, alors :

$$\varphi(mn) = \varphi(m)\varphi(n)$$

Preuve :
$$\phi : \mathbb{Z}/mn\mathbb{Z} \longrightarrow \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$$
$$a \bmod mn \longmapsto (a \bmod m, a \bmod n)$$

isomorphisme d'anneaux.

donc
$$\phi\left((\mathbb{Z}/mn\mathbb{Z})^*\right) = (\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z})^* = (\mathbb{Z}/m\mathbb{Z})^* \times (\mathbb{Z}/n\mathbb{Z})^*$$

donc
$$\mathrm{Card}(\mathbb{Z}/mn\mathbb{Z})^* = \mathrm{Card}(\mathbb{Z}/m\mathbb{Z})^* \times \mathrm{Card}(\mathbb{Z}/n\mathbb{Z})^*$$

ie
$$\varphi(mn) = \varphi(m)\varphi(n).$$

Proposition. Si p est premier et $k \in \mathbb{N}^*$, alors :

$$\varphi(p^k) = p^k - p^{k-1}$$

Preuve $\varphi(p^k) =$ nb d'inversible dans $\mathbb{Z}/p^k\mathbb{Z}$

Dans $\mathbb{Z}/p^k\mathbb{Z}$:

$x \in \{\overline{1}, \overline{2}, \dots, \overline{p-1}, \overline{p}, \overline{p+1}, \dots\} = \mathbb{Z}/p^k\mathbb{Z}$

$\underset{\overline{a}}{\overset{x}{\parallel}}$ inversible $\iff a \wedge p^k = 1$

$\iff a \wedge p = 1$

$\iff a$ n'est pas un multiple de p.

Les multiples de p dans $\{0, 1, \dots, p^k - 1\}$:

$0, p, 2p, 3p, \dots, (p^{k-1} - 1)p$: il y en a p^{k-1}

Donc $\varphi(p^k) = \mathrm{Card}\left(\mathbb{Z}/p^k\mathbb{Z}\right)^*$

$= p^k - p^{k-1}$

Théorème.

Soit $n \geqslant 2$ un entier. On a :

$$\varphi(n) = n \prod_{\substack{p \text{ premier} \\ p|n}} \left(1 - \frac{1}{p}\right)$$

Exemple. Calculer $\varphi(36)$.

Preuve: On écrit

$$n = \prod_{k=1}^{d} p_k^{m_k}$$

où les p_k premiers distincts

et $m_k \in \mathbb{N}$

$$\varphi(n) = \prod_{k=1}^{d} \varphi\left(p_k^{m_k}\right)$$

car les p_k sont premiers entre eux

$$= \prod_{k=1}^{d} p_k^{m_k} - p_k^{m_k - 1}$$

$$= \prod_{k=1}^{d} p_k^{m_k} \left(\prod_{k=1}^{d} 1 - \frac{1}{p_k} \right)$$

$$= n \prod_{k=1}^{d} \left(1 - \frac{1}{p_k}\right)$$

$$= n \prod_{\substack{p|n \\ p \text{ premier}}} \left(1 - \frac{1}{p}\right)$$

$36 = 2^2 \times 3^2$

donc $\varphi(36) = 36\left(1-\frac{1}{2}\right)\left(1-\frac{1}{3}\right)$

$= \cancel{6}\ 12$

$\boxed{14.4}$

(a) Dans $\mathbb{Z}/7\mathbb{Z}$:

$x^2 = \bar{1} \iff x^2 - \bar{1} = \bar{0}$

$\iff (x-\bar{1})(x+\bar{1}) = \bar{0}$

$\iff x - \bar{1} = \bar{0}$ ou $x + \bar{1} = \bar{0}$

car $\mathbb{Z}/7\mathbb{Z}$ intègre

$\iff x = \bar{1}$ ou $x = -\bar{1} = \bar{6}$

(b) Dans $\mathbb{Z}/8\mathbb{Z}$:

$\bar{0}^2 = \bar{0}$

$(-\bar{1})^2 = \bar{1}^2 = \bar{1}$

$(-\bar{2})^2 = \bar{2}^2 = \bar{4}$

$(-\bar{3})^2 = \bar{3}^2 = \bar{9} = \bar{1}$

$\bar{4}^2 = \bar{0}$

donc $x^2 = \bar{1} \iff x = \bar{1}$ ou $-\bar{1}$
ou $\bar{3}$ ou $-\bar{3}$

4 solutions.