Proposition : Soient $B_1, \dots, B_k$ des anneaux.

Alors $B_1 \times \dots \times B_k$ est un anneau avec les opérations suivantes :

$$+ : \begin{cases} (B_1 \times \dots \times B_k) \times (B_1 \times \dots \times B_k) \to B_1 \times \dots \times B_k \\ ((b_1, \dots, b_k), (b_1', \dots, b_k')) \mapsto (b_1 + b_1', \dots, b_k + b_k') \end{cases}$$

et

$$\cdot : \begin{cases} (B_1 \times \dots \times B_k) \times (B_1 \times \dots \times B_k) \to B_1 \times \dots \times B_k \\ ((b_1, \dots, b_k), (b_1', \dots, b_k')) \mapsto (b_1 b_1', \dots, b_k b_k') \end{cases}$$

De plus si A est anneau et pour tout $i = 1, \dots, k$

$$\varphi_i : A \to B_i$$

est un homomorphisme d'anneaux, alors

$$\varphi : \begin{cases} A \to B_1 \times \dots \times B_k \\ a \mapsto (\varphi_1(a), \dots, \varphi_k(a)) \end{cases}$$

est un homomorphisme d'anneaux.

Dém : par exercice.

Exemple : Le théorème des restes chinois peut être aussi énoncé de la façon suivante.

Soient $n_1, \dots, n_k$ des entiers premiers entre eux deux à deux, et soit $N = n_1 \cdots n_k$.

Alors l'application :

$$\theta : \frac{\mathbb{Z}}{N\mathbb{Z}} \longrightarrow \frac{\mathbb{Z}}{n_1\mathbb{Z}} \times \cdots \times \frac{\mathbb{Z}}{n_k\mathbb{Z}}$$

$$[a]_N \longmapsto ([a]_{n_1}, \ldots, [a]_{n_k})$$

est un isomorphisme d'anneaux.

De plus θ induit un isomorphisme de groupes multiplicatifs.

$$\left(\frac{\mathbb{Z}}{N\mathbb{Z}}\right)^\times \simeq \left(\frac{\mathbb{Z}}{n_1\mathbb{Z}}\right)^\times \times \cdots \times \left(\frac{\mathbb{Z}}{n_k\mathbb{Z}}\right)^\times$$

Exemple

1) $\frac{\mathbb{Z}}{3\mathbb{Z}} \times \frac{\mathbb{Z}}{2\mathbb{Z}} \simeq \frac{\mathbb{Z}}{6\mathbb{Z}}$ ↑ théorème des restes chinois $\Rightarrow$ en tant que groupe $\frac{\mathbb{Z}}{3\mathbb{Z}} \times \frac{\mathbb{Z}}{2\mathbb{Z}}$ est cyclique

et un générateur est $(1,1)$ *

Proposition (par exercice)

Si $\varphi : A \to B$ est un isomorphisme de groupes. Alors :

1) A est cyclique $\iff$ B est cyclique

2) $a \in A$ est générateur de $A \iff \varphi(a)$ est un générateur de B.

* $(1,1)$

$2(1,1) = (2,0)$

$3(1,1) = (0,1)$

$4(1,1) = (1,0)$

$5(1,1) = (2,1)$

$6(1,1) = (0,0)$

$\Rightarrow \frac{\mathbb{Z}}{3\mathbb{Z}} \times \frac{\mathbb{Z}}{2\mathbb{Z}} = \langle (1,1) \rangle$

en tant que groupe abélien (additif)

2) $\frac{\mathbb{Z}}{6\mathbb{Z}} \times \frac{\mathbb{Z}}{5\mathbb{Z}} \times \frac{\mathbb{Z}}{11\mathbb{Z}} \simeq \frac{\mathbb{Z}}{330\mathbb{Z}}$

3) Attention : $\frac{\mathbb{Z}}{2\mathbb{Z}} \times \frac{\mathbb{Z}}{2\mathbb{Z}} \not\simeq \frac{\mathbb{Z}}{4\mathbb{Z}}$

Supposons par l'absurde qu'il existe un isomorphisme d'anneaux :

$$\varphi : \frac{\mathbb{Z}}{4\mathbb{Z}} \longrightarrow \frac{\mathbb{Z}}{2\mathbb{Z}} \times \frac{\mathbb{Z}}{2\mathbb{Z}}$$

Soit $\varphi(1) = (a,b) \in \frac{\mathbb{Z}}{2\mathbb{Z}} \times \frac{\mathbb{Z}}{2\mathbb{Z}} \Longrightarrow$

$$2\varphi(1) = 2(a,b) = (a,b) + (a,b) = (2a, 2b) = (0,0)$$

$2\varphi(1) = \varphi(1) + \varphi(1) = \varphi(2)$

$\Longrightarrow \varphi(2) = (0,0)$ ↯ car $\varphi(0) = (0,0)$ et φ est injective.

Vers une petite introduction aux corps finis.

Un corps fini est un corps avec un nombre fini d'éléments.

<u>Exemple</u> : • $\forall$ nombre premier p, $\frac{\mathbb{Z}}{p\mathbb{Z}}$ est un corps fini avec p éléments.

• $\frac{\mathbb{Z}}{2\mathbb{Z}} = \{0, 1\}$ est le corps (fini) de taille minimale (en effet, tout corps doit avoir au moins deux éléments, 0 et 1 distincts)

Soit K un corps.

On considère $(K[X], +, \cdot)$ l'anneau des polynômes à 1 variable et à coefficients dans K.

Sur $K[X]$ les opérations d'addition et multiplication sont définies de la façon suivante :

Soient $P = \sum_{i \in \mathbb{N}} a_i X^i$ (somme finie) et $Q = \sum_{i \in \mathbb{N}} b_i X^i$ (somme finie), alors :

$$P + Q := \sum_{i \in \mathbb{N}} (a_i + b_i) X^i$$

$$PQ := \sum_{i \in \mathbb{N}} \left(\sum_{j+k=i} a_j b_k \right) X^i$$

Somme finie signifie que le nombre de coefficients a_i non nuls est fini.

Exemple : $P = a_0 + a_1 X + a_2 X^2$

$Q = b_0 + b_1 X + b_2 X^2 + b_3 X^3$

$$PQ = (a_0 + a_1 X + a_2 X^2)(b_0 + b_1 X + b_2 X^2 + b_3 X^3)$$
$$= \underbrace{a_0 b_0}_{i=0 : j+k=0} + \underbrace{(a_0 b_1 + a_1 b_0) X}_{i=1 : j+k=1} + \underbrace{(a_0 b_2 + a_1 b_1 + a_2 b_0) X^2}_{i=2 : j+k=2} + \cdots$$

L'ensemble des éléments inversibles de $K[X]$ est $(K[X])^\times = \{ a_0 : a_0 \in K \text{ et } a_0 \neq 0 \} = K \setminus \{0\}$

↑ polynômes constants non nuls

$A \in K[X]$ t.q. $\exists\, B \in K[X]$ t.q. $AB = 1$

Exemple : $2 \in (\mathbb{R}[X])^\times$ car $2 \cdot \frac{1}{2} = 1$, $\frac{1}{2} \in \mathbb{R}[X]$

Déf : Soit A un anneau intègre.
Un élément non nul $p \in A \setminus \{0\}$ est dit <u>irréductible</u> si

1) p n'est pas inversible ;
2) si $p = xy$, $xy \in A \Rightarrow$ x est inversible ou y est inversible.

Exemple : 1) Soit $A = \mathbb{Z}$.

- les inversibles de $\mathbb{Z}$ sont ± 1.
- $6 = 3 \cdot 2$ et 3 et 2 ne sont pas inversibles, donc 6 n'est pas irréductible.
- $7 = 1 \cdot 7 = (-1)\cdot(-7)$ et il n'y a pas d'autres façons d'écrire 7 comme produit de deux entiers.

$\Rightarrow$ 7 est irréductible.

L'ensemble des irréductibles de $\mathbb{Z}$ est

$\{\dots, -5, -3, -2, 2, 3, 5, 7, \dots\}$

c'est-à-dire les nombres premiers et leurs opposés.

2) Dans $A = K[x]$, tous les polynômes de degré 1 sont irréductibles.

<u>Dém :</u> Soit $P = ax + b$, $a, b \in K$ $(a \neq 0)$ et soient $A, B \in K[x]$ tels que

$$P = AB \Rightarrow \deg(P) = \deg(A) + \deg(B)$$

$$\Rightarrow \deg(A) = 0 \text{ ou } \deg(B) = 0$$

Par convention $\deg(0) = -\infty$

$\deg(A), \deg(B) \geq 0$ (car $A, B \neq 0$)

$\Rightarrow$ A ou B est un polynôme constant non nul

$\Rightarrow$ A ou B est inversible

$\Rightarrow$ P est irréductible.

3) X^2+1 est irréductible dans $\mathbb{R}[X]$, car $\Delta<0$, mais il n'est pas irréductible dans $\mathbb{C}[X]$ car $x^2+1=(x+i)(x-i)$ et $x-i$ et $x+i$ ne sont pas inversibles dans $\mathbb{C}[X]$

On sait que (MAT304) $K[X]$ est un anneau euclidien, c'est-à-dire $\forall A,B \in K[X]$, $B\neq 0$, $\exists$ un unique couple de polynômes $Q,R \in K[X]$ tels que

$$A = BQ+R, \text{ avec } \deg(R) < \deg(B).$$

($\deg(0) = -\infty$)

Soit $P \in K[X]$ un polynôme. Alors l'ensemble :

$$I = (P) := \{AP,\ A \in K[X]\}$$

est un idéal de $K[X]$ appelé idéal engendré par P.

(Par exercice, montrer que I est un idéal de $K[X]$)

Exemple : 1) Dans $\mathbb{Q}[X]$:

$$I = (x^2+2) = \{(x^2+2)A(x),\ A(x) \in \mathbb{Q}[X]\}$$

$x^3+2x \in I$ car $(x^2+2)\cdot x$

$x+1 \notin I$, pour de raisons de degré.

2) Dans $K[x]$, $P = a$, $a \in K \setminus \{0\}$.
Alors $(P) = K[x]$, car $1 \in (P)$
$\Rightarrow 1 \cdot K[x] \subseteq (P)$. $\quad 1 = a \cdot a^{-1}$

On peut considérer l'anneau quotient

$$\frac{K[x]}{(P)} := \{[B] : B \in K[x]\}$$

où $[B] = \{A \in K[x] : A - B \in (P)\}$

Supposons $P \neq 0$.
Soit $B \in K[x]$, alors $[B] = B + (P) = \{B + PA, A \in K[x]\}$
On va montrer que il y a une bijection :

$$K[x]_{<\deg(P)} \longrightarrow \frac{K[x]}{(P)}$$

$$R \quad (\deg(R) < \deg(P)) \longmapsto [R]$$

surjectivité

Soit $[B] \in \frac{K[x]}{(P)}$, $B \in K[x]$. En divisant B par P on obtient :

$$B = PQ + R, \quad \deg(R) < \deg(P)$$

$$\Rightarrow B - R = PQ \in (P) \Rightarrow [B] = [R].$$

injectivité

Si $[R_1] = [R_2]$ avec $\deg(R_1) < \deg(P)$ et $\deg(R_2) < \deg(P)$

$$\Rightarrow R_1 - R_2 \in (P) \Rightarrow R_1 - R_2 = 0 \Rightarrow R_1 = R_2$$

$\uparrow$ $\deg(R_1 - R_2) < \deg(P)$