Anneaux et corps.

Def: Un anneau est un triplet $(A,+,\cdot)$ tel que.
- $(A,+)$ est un groupe abélien
- $(A,\cdot)$ est un semi-groupe

On dit que $(A,+,\cdot)$ est commutatif (ou abélien) si $(A,\cdot)$ est abélien.

De plus $\forall x,y,z \in A$ $\quad x\cdot(y+z) = x\cdot y + x\cdot z$

$(x+y)\cdot z = xz + yz$

L'élément neutre de $(A,\cdot)$, s'il existe, est appelé l'élément unité de A. Dans ce cas on dit que A est un anneau unitaire.

Def: Soit $(A,+,\cdot)$ ~~est~~ un anneau. et $a \in A$

- On dit que a est inversible dans $(A,+,\cdot)$ si a est inversible dans le semi-groupe $(A,\cdot)$
- On dit que a est un diviseur de zéro si $a \neq 0$ et s'il existe $b \neq 0$ tel que $a\cdot b = 0$.

Exemple: 1) $(\mathbb{Z},+,\cdot)$ est un anneau unitaire (unité $=1$) commutatif

de même $(\mathbb{Q},+,\cdot)$; $(\mathbb{R},+,\cdot)$; $(\mathbb{C},+,\cdot)$ sont des anneaux unitaires commutatifs

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

3) $(2\mathbb{Z}, +, \cdot)$ est un anneau non-unitaire
$$\underset{\mathbb{Z}}{\cap} \qquad 1 \notin 2\mathbb{Z} \subset \mathbb{Z}$$

$$2\mathbb{Z} = \{\text{nombres pairs}\}$$

4) Les éléments inversibles de $(\mathbb{Z}, +, \cdot)$ sont $+1$ et -1

5) Soit V $(= \mathbb{R}^n)$ un $\mathbb{R}$-espace vectoriel. Alors.

$$(End(V), +, \circ)$$

addition des endomorphismes

composition des endo.

est un anneau non-commutatif unitaire.

- unité $1 = Id_V : v \mapsto v$.
- non-commutatif : $n = 2$ $V \cong \mathbb{R}^2$

$$End(V) = Mat_2(\mathbb{R})$$

prenons f et g définis par leurs matrices

$$A = Mat_{can}(f) = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \quad \text{et} \quad B = Mat_{can}(g) = \begin{pmatrix} 1 & 0 \\ 0 & 2 \end{pmatrix}$$

alors $AB \neq BA$

$$\Leftrightarrow fg \neq gf$$

<u>Exercice</u> 1) $f \in End(V)$ inversible $\Leftrightarrow \det(Mat_{can}(f)) \neq 0$

$\Leftrightarrow f$ inversible en tant que endo.

2) $f \in End(V)$ diviseur de zéro $\Leftrightarrow f$ non-inversible.

Rappels d'arithmétique dans $\mathbb{Z}$ (voir L1).

1) **Lemme de Gauss** $a, b \in \mathbb{Z}$ et $n \in \mathbb{N}^*$

Si $\text{pgcd}(a, n) = 1$ (a et n premiers entre eux).

alors on a l'implication. (preuve voir L1)

$$n \mid a \cdot b \implies n \mid b.$$

2) **Identité de Bézout** $a, b \in \mathbb{Z}$. Si $\text{pgcd}(a, b) = 1$, alors il existe $x, y \in \mathbb{Z}$ tel que

$$ax + by = 1.$$

Prop. Les diviseurs de zéro de l'anneau $(\mathbb{Z}/_{n\mathbb{Z}}, +, \cdot)$ sont les classes $\bar{a}$ avec $a \in \mathbb{Z}$ et $1 < \text{pgcd}(a, n) < n$

Preuve : • Si $\bar{a}$ est un diviseur de zéro, alors (par définition) il existe $\bar{b} \in \mathbb{Z}/_{n\mathbb{Z}}$ tel que.

$$\bar{a} \cdot \bar{b} = \bar{0}. \iff n \mid a \cdot b.$$

or. $\bar{a} \neq \bar{0} \iff n \nmid a$ et $\bar{b} \neq 0 \iff n \nmid b$.

supposons par l'absurde que $\text{pgcd}(a, n) = 1$, donc d'après le lemme de Gauss on obtient $n \mid b$. contradiction.

• Inversement, si $1 < \text{pgcd}(a, n) < n$, alors on pose $b = \dfrac{n}{\text{pgcd}(a, n)} < n$

Comme $b < n$, on a $n \nmid b \iff \bar{b} \neq \bar{0}$

par définition $\text{pgcd}(a, n) \cdot b = n$

on définit $k = \dfrac{a}{\text{pgcd}(a, n)}$

on multiplie par k : $a b = k \cdot n$

donc $\bar{a} \cdot \bar{b} = \bar{0}$ $\Leftrightarrow$ $\bar{a}$ est un diviseur de zéro.

De plus $\bar{a} \neq \bar{0}$, car $n \nmid a$ (on a supposé $\operatorname{pgcd}(a,n) < n$).

$\square$

Def : Soit $(A,+,\cdot)$ un anneau unitaire. On note

$A^* = \{a \in A \mid a \text{ inversible}\}$ le groupe des éléments inversibles.

Rem : Il est clair que $(A^*, \cdot)$ est un groupe (exercice).

Exemples (1) $(A,+,\cdot) = (\mathbb{Z},+,\cdot)$

(2) $(\mathbb{Z}^*, \cdot) = (\{\pm 1\}, \cdot)$.

(3) $(\mathbb{Q}^*, \cdot)$; $(\mathbb{R}^*, \cdot)$; $(\mathbb{C}^*, \cdot)$ sont des groupes.

Ici notation $*$ coïncide avec la notation précédente $*$ " = sans 0".

Prop :
$$\boxed{\left(\mathbb{Z}/_{n\mathbb{Z}}\right)^* = \{\bar{a} \in \mathbb{Z}/_{n\mathbb{Z}} \mid \operatorname{pgcd}(a,n) = 1\}}$$

Preuve : • Si $\bar{a} \in \mathbb{Z}/_{n\mathbb{Z}}$ est inversible, alors il existe $\bar{b} \in \mathbb{Z}/_{n\mathbb{Z}}$ tel que $\bar{a} \cdot \bar{b} = \bar{1}$ dans $\mathbb{Z}/_{n\mathbb{Z}}$

$\Leftrightarrow$ $\overline{ab} = \bar{1}$ dans $\mathbb{Z}/_{n\mathbb{Z}}$

$\Leftrightarrow$ $ab - 1 = kn$ pour un $k \in \mathbb{Z}$

$\Leftrightarrow$ $1 = ab - kn$

Soit $d = \operatorname{pgcd}(a,n)$, alors $d \mid ab - kn = 1 \Rightarrow d = 1$.

• Si $\operatorname{pgcd}(a,n) = 1$, alors d'après l'identité de Bézout il existe $x, y \in \mathbb{Z}$ tels que $ax + ny = 1$.

On réduit modulo n : $\bar{a}\bar{x} + \bar{n}\cdot\bar{y} = \bar{1} \iff \bar{a}\cdot\bar{x} = \bar{1}$

car $\bar{n} = \bar{0}$

donc $\bar{a}$ est inversible dans $\mathbb{Z}/n\mathbb{Z}$ (d'inverse $\bar{x}$). $\square$.

<u>Exemple</u> : $\left(\mathbb{Z}/12\mathbb{Z}\right)^* = \{\bar{1}, \bar{5}, \bar{7}, \overline{11}\}$.

avec la ~~comp~~ loi de composition

$\bar{5}\cdot\bar{5} = \bar{1}$ $\quad \bar{7}\cdot\bar{7} = \overline{(-5)}\,\overline{(-5)} = \bar{1}$

$\overline{11}\cdot\overline{11} = \overline{(-1)}\cdot\overline{(-1)} = \bar{1}$

<u>Exercice</u> : On peut montrer que les 2 groupes
$\left(\left(\mathbb{Z}/12\mathbb{Z}\right)^*, \cdot\right)$ et $\left(\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}, +\right)$
sont isomorphes.

<u>Déf</u> : Soit $f : (A, +, \cdot) \longrightarrow (B, +, \cdot)$ une application entre deux anneaux commutatifs. On dit que f est un **homomorphisme d'anneaux** si

1) $f : (A, +) \longrightarrow (B, +)$ est un homomorphisme de groupes
2) $f(a_1 \cdot a_2) = f(a_1)\cdot f(a_2)$ $\quad \forall a_1, a_2 \in A$.

<u>Déf</u> : On dit que $f : A \to B$ est un **isomorphisme d'anneaux** si

1) f est un homomorphisme d'anneaux
2) f est une bijection

<u>Rem</u> : (2) $\iff$ $\ker(f) = \{e_{(A,+)}\}$ et $\mathrm{im}(f) = B$.

Déf : Un corps est un anneau $(A, +, \cdot)$ tel que tout $a \in (A, \cdot)$ non nul admet un inverse, c'est-à-dire tel que le groupe des inversibles

$$\boxed{A^* = A \setminus \{0\}}$$

où 0 = neutre du groupe $(A, +)$. Dans ce cas, on dit que $(A^*, \cdot)$ est le groupe multiplicatif du corps $(A, +, \cdot)$

Exemples : $(\mathbb{Q}, +, \cdot)$, $(\mathbb{R}, +, \cdot)$, $(\mathbb{C}, +, \cdot)$ sont des corps.

Prop : L'anneau $(\mathbb{Z}/_{n\mathbb{Z}}, +, \cdot)$ est un corps $\Longleftrightarrow$ n premier.

Preuve : $\mathbb{Z}/_{n\mathbb{Z}}$ corps $\Longleftrightarrow$ $\forall \bar{a} \in \mathbb{Z}/_{n\mathbb{Z}}, \bar{a} \neq \bar{0}$, $\bar{a}$ inversible.

$\overset{\text{prop. préc.}}{\Longleftrightarrow}$ $\forall a \in \mathbb{Z}$ $0 < a < n$; $\mathrm{pgcd}(a, n) = 1$

$\Longleftrightarrow$ n premier.

Notation : On note le plus souvent $\mathbb{F}_p$ (= field en anglais) pour $\mathbb{Z}/_{p\mathbb{Z}}$ avec p premier.

Thm (Théorème des restes chinois). Soient n_1, n_2 des entiers positifs premiers entre eux, c'est-à-dire $\mathrm{pgcd}(n_1, n_2) = 1$, et on note $n = n_1 \cdot n_2$. Alors on a un isomorphisme d'anneaux

$$\boxed{\Phi : \mathbb{Z}/_{n\mathbb{Z}} \xrightarrow{\sim} \mathbb{Z}/_{n_1\mathbb{Z}} \times \mathbb{Z}/_{n_2\mathbb{Z}}}$$

$$\bar{x} = x \bmod n \longmapsto (x \bmod n_1, \ x \bmod n_2).$$

<u>Rem</u> : On a la généralisation suivante. Soient $m_1, \dots, m_k$ des entiers positifs 2 à 2 premiers entre eux, c'est-à-dire $\mathrm{pgcd}(m_i, m_j) = 1$ $\forall i, j$. et on note $m = m_1 \cdot m_2 \cdots m_k$. Alors

$$\boxed{\Phi : \mathbb{Z}/m\mathbb{Z} \xrightarrow{\sim} \mathbb{Z}/m_1\mathbb{Z} \times \mathbb{Z}/m_2\mathbb{Z} \times \cdots \times \mathbb{Z}/m_k\mathbb{Z}.}$$

(par récurrence sur le nombre de facteurs k).

Dans la preuve on va utiliser ~~le~~ résultat suivant.

<u>Prop</u> : Soient $m_1, m_2 \in \mathbb{Z}$ avec m_1 et m_2 premiers entre eux et $x \in \mathbb{Z}$. Si $m_1 | x$ et $m_2 | x$, alors $m_1 \cdot m_2 | x$.

<u>Preuve</u> : D'après l'identité de Bézout, on a

$$(*) \quad 1 = m_1 a + m_2 b \quad \text{pour des entiers } a, b \in \mathbb{Z}.$$

Comme $m_1 | x$, on peut écrire $x = m_1 \cdot k_1$. ; $k_1 \in \mathbb{Z}$.

Comme $m_2 | x$, on peut écrire $x = m_2 \cdot k_2$; $k_2 \in \mathbb{Z}$.

On multiplie $(*)$ avec x :

$$x = m_1 a x + m_2 b x$$

et on remplace x par les égalités précédentes

$$x = m_1 a (m_2 k_2) + m_2 b (m_1 k_1)$$

$$= m_1 m_2 (a k_2 + b k_1)$$

donc $m_1 m_2 | x$. $\square$

Démonstration du théo. des restes chinois

- On vérifie d'abord que Φ est bien défini, c'est-à-dire que $(x \bmod n_1, x \bmod n_2)$ ne dépend que de $\bar{x}$ mod n
(ce qui est clair, car $x + kn \equiv x \bmod n_i$).
- De plus Φ est un homomorphisme d'anneaux, ce qui est clair d'après les propriétés sur les congruences.
- $\left|\mathbb{Z}/_{n\mathbb{Z}}\right| = n$ et $\left|\mathbb{Z}/_{n_1\mathbb{Z}} \times \mathbb{Z}/_{n_2\mathbb{Z}}\right| = \left|\mathbb{Z}/_{n_1\mathbb{Z}}\right| \cdot \left|\mathbb{Z}/_{n_2\mathbb{Z}}\right| = n_1 \cdot n_2 = n$.
Les anneaux ont même cardinal.
Donc pour montrer que Φ est bijectif, il suffit de montrer que Φ est injectif, donc que $\ker \Phi = \{\bar{0}\}$.
car Φ est un homomorphisme de groupes.
- montrons que $\ker(\Phi) = \{\bar{0}\}$. Supposons que $\bar{x} \in \ker(\Phi)$, c'est-à-dire $\Phi(\bar{x}) = (\bar{0}, \bar{0})$ donc $n_1 | x$ et $n_2 | x$. D'après la proposition précédente, $n_1 \cdot n_2 | x \Leftrightarrow \bar{x} = \bar{0}$.

<u>Rem</u> : On verra plus tard une manière de calculer l'~~inverse~~ antécédent $\bar{x} \in \mathbb{Z}/_{n\mathbb{Z}}$ d'un élément $(\bar{a}_1, \dots, \bar{a}_k) \in \mathbb{Z}/_{n_1\mathbb{Z}} \times \dots \times \mathbb{Z}/_{n_k\mathbb{Z}}$ ce qui revient à résoudre un système de k congruences.

$$x \equiv a_i \bmod n_i \quad \text{pour } i = 1, \dots, k.$$