Algèbre et Arithmétique Effectives — 06/11/25

Cours 9

On rappelle du cours 8 :

Théorème (Premier théorème d'isomorphisme)
Soit $\varphi : G \to G'$ un homomorphisme de groupes.
Alors

$$G/_{\ker(\varphi)} \simeq \mathrm{Im}(\varphi)$$

via l'isomorphisme :

$$\hat{\varphi} : G/_{\ker(\varphi)} \longrightarrow \mathrm{Im}(\varphi)$$
$$[a]_{\ker(\varphi)} \longmapsto \varphi(a)$$

Exemple

$$G = \mathbb{Z} \times \mathbb{Z} = \{(x,y) : x,y \in \mathbb{Z}\}$$

$$+ : (\mathbb{Z}\times\mathbb{Z}) \times (\mathbb{Z}\times\mathbb{Z}) \longrightarrow \mathbb{Z}\times\mathbb{Z}$$
$$((x,y), (x',y')) \longmapsto (x,y)+(x',y') = (x+x', y+y')$$

On peut facilement montrer que $(\mathbb{Z}\times\mathbb{Z}, +)$ est un groupe commutatif.

On considère l'application suivante :

$$\varphi : (\mathbb{Z}\times\mathbb{Z}, +) \longrightarrow (\mathbb{Z}, +)$$
$$(x,y) \longmapsto x+y$$

Montrons que φ est un homomorphisme de groupes.

Soient $(x,y), (x',y') \in \mathbb{Z}\times\mathbb{Z}$. Alors on a :

$$\varphi((x,y)+(x',y')) = \varphi(x+x', y+y') = x+x'+y+y' =$$
$$= (x+y)+(x'+y') = \varphi(x,y)+\varphi(x',y')$$

$\mathrm{Ker}(\varphi) = \{(x,y) \in \mathbb{Z}\times\mathbb{Z} : \varphi(x,y) = 0\} = \{(x,y) \in \mathbb{Z}\times\mathbb{Z} : x+y = 0\} =$
$= \{(x, -x) : x \in \mathbb{Z}$

$\mathrm{Im}(\varphi) = \mathbb{Z}$, car $\forall\, y \in \mathbb{Z}$ on a $\varphi(0,y) = y$.

Donc, d'après le 1er théorème d'isomorphisme, on a que:

$$\frac{\mathbb{Z}\times\mathbb{Z}}{\mathrm{Ker}(\varphi)} \simeq \mathbb{Z}$$

On peut facilement voir que $\mathrm{Ker}(\varphi) \simeq \mathbb{Z}$ (un isomorphisme est donné par $\varphi : \mathrm{Ker}(\varphi) \to \mathbb{Z}$, $\varphi(x,-x) = x$).
En conclusion, on a donc montré que $\dfrac{\mathbb{Z}\times\mathbb{Z}}{\mathbb{Z}} \simeq \mathbb{Z}$.

Anneaux

Def: Un <u>anneau</u> $(A, +, \cdot)$ est un ensemble muni de deux opérations binaires internes A:

addition: $+ : A \times A \to A$

multiplication $\cdot : A \times A \to A$

telles que:

1) $(A,+)$ est un groupe abélien.
2) l'opération $\cdot$ est associative et il existe un élément neutre par rapport à $\cdot$
3) $\cdot$ est distributive sur $+$:

$$a\cdot(b+c) = ab + ac$$
$$(a+b)\cdot c = ac + b\cdot c$$

Si $\cdot$ est aussi commutative alors $(A,+,\cdot)$ est dit un anneau commutatif.

Def: Un corps est un anneau commutatif $(K,+,\cdot)$ où tout élément non nul possède un inverse par rapport à $\cdot$.

Remarque : Un anneau commutatif $(A,+,\cdot)$ est un corps $\Longleftrightarrow$ $(A\setminus\{0\},\cdot)$ est un groupe abélien.

Exemples

- $(\mathbb{Z},+,\cdot)$, $(\mathbb{Q},+,\cdot)$, $(\mathbb{R},+,\cdot)$, $(\mathbb{C},+,\cdot)$, $(\mathbb{Z}/n\mathbb{Z},+,\cdot)$ sont des anneaux
- $(\mathbb{Z},+,\cdot)$ n'est pas un corps car $\forall\, a \neq 1,-1$, a n'est pas inversible.
- $(\mathbb{Z}/n\mathbb{Z},+,\cdot)$ est un corps $\Longleftrightarrow$ n est un nombre premier.

- $(\mathbb{Q},+,\cdot)$, $(\mathbb{R},+,\cdot)$, $(\mathbb{C},+,\cdot)$ sont des exemples de corps.
- $(n\mathbb{Z},+,\cdot)$ est un anneau $\Longleftrightarrow n=1,-1 \Longleftrightarrow n\mathbb{Z}=\mathbb{Z}$ car sinon $1 \notin n\mathbb{Z}$.

- $(\mathbb{Z}/n\mathbb{Z})^*$ n'est pas un anneau :

$1, \underbrace{n-1}_{= -1} \in (\mathbb{Z}/n\mathbb{Z})^*$, mais $1+n-1 = n = 0$ n'est pas inversible.

Déf : Soit $(A,+,\cdot)$ un anneau. Un élément non nul $a \in A\setminus\{0\}$ est un <u>diviseur de zéro</u> s'il existe $b \in A\setminus\{0\}$ tel que $ab=0$.

Un anneau sans diviseur de zéro est appelé un <u>anneau intègre</u>.

Exemple : Si n n'est pas premier, alors $\mathbb{Z}/n\mathbb{Z}$ n'est pas intègre.

Si n n'est pas premier, alors il existe $1<a,b<n$ tel que $n=ab \Rightarrow a$ et b sont deux diviseurs de zéro.

<u>Déf</u> : Soit $(A,+,\cdot)$ un anneau commutatif.
Un <u>idéal</u> de A est un sous-ensemble I de A tel que $(I,+)$ est un sous-groupe de $(A,+)$ et tel que $\forall x \in I$, $\forall a \in A$, $ax \in I$.

<u>Exemple</u> : $(\mathbb{Z},+,\cdot)$ est un anneau commutatif.
On montre que $\forall n \in \mathbb{Z}_{\geq 0}$, $I = n\mathbb{Z}$ est un idéal.

On a déjà vu que $(n\mathbb{Z},+)$ est un sous-groupe de $(\mathbb{Z},+)$.

Soient $x \in n\mathbb{Z}$ et $a \in \mathbb{Z}$ $\Rightarrow$ $\exists\, k \in \mathbb{Z}$ tel que $x = nk$. Donc on a :

$$xa = nka = n\underbrace{(ka)}_{\in \mathbb{Z}} \in n\mathbb{Z}.$$

Soient $(A,+,\cdot)$ un anneau commutatif et I un idéal de A. On considère la relation suivante :

$$\forall a,b \in A, \quad a \sim_I b \iff a-b \in I$$

On a vu hier que $\sim_I$ est une relation d'équivalence dont, $\forall a \in A$, la classe d'équivalence de a est :

$$[a]_I = \{a+x : x \in I\}$$

On note l'ensemble des classes d'équivalence :

$$A/_I = \{[a]_I,\ a \in A\}$$

On peut définir deux opérations sur $A/_I$:

(addition) : $$+ : A/_I \times A/_I \longrightarrow A/_I$$
$$([a]_I, [b]_I) \longmapsto [a]_I \mathbin{+_I} [b]_I := [a+b]_I$$

(multiplication) : $\cdot \quad A/_I \times A/_I \longrightarrow A/_I$

$$([a]_I, [b]_I) \longmapsto [a]_I \cdot [b]_I := [ab]_I$$

On a déjà vu que l'addition est bien définie.
Montrons que la multiplication est aussi bien définie :

Soient $a' \sim_I a$ et $b' \sim_I b$. On veut montrer que $a'b' \sim_I ab$.

$a' \sim_I a$, $b' \sim_I b \Rightarrow a' - a \in I$ et $b' - b \in I \Rightarrow$

$\Rightarrow \exists\ x, y \in I$ tels que $a' - a = x$ et $b' - b = y$.

Alors on a :

$$a'b' = (x+a)(y+b) = xy + xb + ay + ab \Rightarrow$$

$$\Rightarrow a'b' - ab = \underbrace{xy + xb + ay}_{\in I \text{ parce que } I \text{ est un idéal!}}$$

$\Rightarrow a'b' \sim_I ab$

(Note que si I n'était pas un idéal l'opération de multiplication ne serait pas bien définie).

<u>Proposition</u> : Soit $(A, +, \cdot)$ un anneau commutatif et soit I un idéal de A.

Alors $(A/_I, +, \cdot)$ est un anneau commutatif, appelé <u>anneau quotient</u>.