Pour lu : exo au choix à rédiger à envoyer avant 7h30

12.7, 54.24, 54.25

Pour ma : 12.2, 54.4 + { MPI* : 12.10 ; MPI : 54.28

Pour jé : problème à rédiger, à envoyer

B sous-anneau de A

$B \subset A$

B stable par + et B stable par opposé

B stable par ×

$1_A \in B$

$\mathbb{N} \subset \mathbb{Z}$ et $\mathbb{N}$ n'est pas un anneau.

2 Idéaux d'un anneau commutatif

2.1 Définition

Remarque. *Si $f : A \to B$ est un morphisme d'anneaux, son image $\operatorname{Im} f$ est un sous-anneau de B, mais son noyau $\operatorname{Ker} f$ n'est pas en général un sous-anneau de A.*

Définition. Soit $(A, +, \times)$ un anneau commutatif. Une partie I de A est un **idéal** de A lorsque :

- I est un sous-groupe de $(A, +)$
- I est **absorbant**, i.e. :

$$\forall a \in A,\ \forall x \in I,\ a \times x \in I$$

Exemple: Dans $(\mathbb{Z}, +, \times)$, notons $I = \{\text{entiers pairs}\}$

c'est un idéal. Si $x \in I$, $a \in \mathbb{Z}$

xa a pair donc $xa \in I$.

Théorème.

Si $f : A \to B$ est un morphisme d'anneaux commutatifs. Alors son noyau $\operatorname{Ker} f$ est un idéal de A.

- On sait déjà que f est un morphisme de groupes,

  donc $\operatorname{Ker} f = f^{-1}(\{0_B\})$ est un sous-groupe de A

- Mq $\operatorname{Ker} f$ est absorbant.

  Soit $x \in \operatorname{Ker} f$ ie $f(x) = 0_B$

  Soit $a \in A$

  On calcule: $f(ax) = f(a) f(x)$ car f morphisme d'anneaux

  $= f(a)\, 0_B$

  $= 0_B$

  donc $ax \in \operatorname{Ker} f$.

Proposition. Si $a \in A$, alors aA est un idéal de A, qu'on appelle **idéal engendré par** a.

Remarque.

- *On peut utiliser la notation (a) pour désigner aA, idéal engendré par a.*
- *Un idéal I pour lequel il existe a tel que $I = aA$ est parfois qualifié de principal. Si tous les idéaux de A sont principaux, on qualifie l'anneau de principal. Ce vocabulaire n'est pas dans le programme officiel.*

exemple. $2\mathbb{Z}$ est l'idéal engendré par 2 dans $\mathbb{Z}$.

Exemple. Que dire d'un idéal qui contient 1_A ?

Exemple. Quels sont les idéaux d'un corps ?

- Soit I idéal de A tq $1_A \in I$.

  $\forall x \in A$, $x \times 1_A = x$ car 1_A neutre

  $\uparrow$ I car I est absorbant et $1_A \in I$

  donc $x \in I$

  Bref $A \subset I$ donc $I = A$.

- Si A est un corps et I idéal de A.

  1er cas : $I = \{0_A\}$

  2e cas : $I \neq \{0_A\}$

  Soit $a \in I$, $a \neq 0$

  $a \neq 0$ donc a^{-1} existe (dans A)

  donc $1_A = a \times a^{-1} \in I$ car I absorbant

  et donc $I = A$

2.2 Idéaux de $\mathbb{Z}$, PGCD d'entiers

Proposition. Les idéaux de $(\mathbb{Z}, +, \times)$ sont les $n\mathbb{Z}$, avec $n \in \mathbb{N}$.

Preuve :

$\Leftarrow$ Soit $n \in \mathbb{N}$ Mq $n\mathbb{Z}$ idéal de $\mathbb{Z}$

- $n\mathbb{Z}$ sous-groupe de $(\mathbb{Z}, +)$
- $n\mathbb{Z}$ est absorbant

  Si $a \in n\mathbb{Z}$, $a = np$ où $p \in \mathbb{Z}$

  pour $x \in \mathbb{Z}$, $ax = npx \in n\mathbb{Z}$

Rmq : $n\mathbb{Z} = (n)$ idéal engendré par n

$\Rightarrow$ Soit I idéal de $\mathbb{Z}$

donc I est d'abord un sous-groupe de $(\mathbb{Z}, +)$

donc $\exists n \in \mathbb{Z}$ tq $I = n\mathbb{Z}$.

(div. euclidienne)

Proposition. Soit $a, b \in \mathbb{Z}$. Alors :

$$(a) + (b) = a\mathbb{Z} + b\mathbb{Z} = \{au + bv,\ u, v \in \mathbb{Z}\}$$

est un idéal de $\mathbb{Z}$.

- Mq $a\mathbb{Z} + b\mathbb{Z}$ est un sous-groupe de $(\mathbb{Z}, +)$

  * $a\mathbb{Z} + b\mathbb{Z} \subset \mathbb{Z}$

  * $0 = a0 + b0 \in a\mathbb{Z} + b\mathbb{Z}$

  * Soit $x_1, x_2 \in a\mathbb{Z} + b\mathbb{Z}$ donc $\exists u_1, v_1, u_2, v_2 \in \mathbb{Z}$

ξ $x_1 = a u_1 + b v_1$ $\quad x_2 = a u_2 + b v_2$

Alors : $x_1 + x_2 = a(u_1+u_2) + b(v_1+v_2)$

$\in a\mathbb{Z} + b\mathbb{Z}$

$x_1 - x_2$

et $-x_1 = a(-u_1) + b(-v_1)$

$\in a\mathbb{Z} + b\mathbb{Z}$

- Rque $a\mathbb{Z} + b\mathbb{Z}$ est absorbant

Soit $x \in a\mathbb{Z} + b\mathbb{Z}$, ie $\exists u, v \in \mathbb{Z}$ ξ $x = au + bv$.

$y \in \mathbb{Z}$

On calcule $xy = (au + bv)y$

$= a(uy) + b(vy)$

$\in a\mathbb{Z} + b\mathbb{Z}$ $\quad uy, vy \in \mathbb{Z}$

Définition. Soit $a, b \in \mathbb{Z}$, non tous les deux nuls. Alors il existe un unique entier $d \in \mathbb{N}$, appelé **PGCD de a et b**, tel que :

$$(a) + (b) = (d) \text{ i.e. } a\mathbb{Z} + b\mathbb{Z} = d\mathbb{Z}$$

Notation.

- On note $a \wedge b$ le PGCD de a et b.
- La relation $au + bv = a \wedge b$ s'appelle **relation de Bézout**.

Proposition. Soit $a, b \in \mathbb{Z}$ deux entiers non nuls. Les diviseurs communs à a et b sont les diviseurs de $a \wedge b$.

On note $d = a \wedge b$

$$a\mathbb{Z} + b\mathbb{Z} = d\mathbb{Z}$$

$\Leftarrow$ Soit $x \in \mathbb{Z}$ diviseur de d

$$a = a1 + b0 \in a\mathbb{Z} + b\mathbb{Z} = d\mathbb{Z}$$

donc $\exists p \in \mathbb{Z}$ tq $a = dp$

donc x divise a car x divise d.

De même x divise b.

($\Rightarrow$) Soit $x \in \mathbb{Z}$ diviseur commun à a et b

$d = d1 \in d\mathbb{Z} = a\mathbb{Z} + b\mathbb{Z}$

donc $\exists u, v \in \mathbb{Z}$ tq $d = au + bv$

car x divise a et b, donc divise $au + bv$

donc divise d.

Remarque. *On retrouve la définition de première année : $a \wedge b$ est le plus grand (au sens de l'ordre naturel, au sens de la divisibilité) entier naturel qui divise à la fois A et B.*

Définition. Soit $a_1, \ldots, a_n \in \mathbb{Z}$, non tous nuls. On appelle **PGCD de** $a_1, \ldots, a_n$ l'unique $d \in \mathbb{N}$ tel que :

$$a_1\mathbb{Z} + \cdots + a_n\mathbb{Z} = d\mathbb{Z}$$

2.3 Idéaux de $\mathbb{K}[X]$

Proposition. Les idéaux de $(\mathbb{K}[X], +, \times)$ sont les $P\,\mathbb{K}[X] = \{PQ,\ Q \in \mathbb{K}[X]\}$, avec $P \in \mathbb{K}[X]$.

2.4 Divisibilité dans un anneau, idéal engendré par un élément

Définition. Soit $(A, +, \times)$ un anneau commutatif, $a, b \in A$. On dit que a **divise** b, et on note $a \mid b$, lorsqu'il existe $c \in A$ tel que $b = ac$, i.e. b est un multiple de a.

Remarque. $a \mid b \iff bA \subset aA$

Définition. Dans $(A, +, \times)$ anneau commutatif, pour $a, b \in A$, on dit que a et b sont **associés** si et seulement si $a \mid b$ et $b \mid a$, c'est-à-dire $aA = bA$.

Proposition.

- La relation *être associés* est une relation d'équivalence sur A.
- Lorsque A est intègre, a et b sont associés si et seulement s'il existe u inversible tel que $a = ub$.