1) Quelques rappels de théorie élémentaire des groupes

- ordre d'un élément d'un groupe
- groupe cyclique (description des sous groupes d'un groupe cyclique)

2) Notions de base de théorie des anneaux = "fondements de l'algèbre commutative"

Constructions produit d'anneaux
anneaux quotients
$\mathbb{R}[X]$ $\mathbb{C}[X]$ $\mathbb{Z}[X]$ $A[X]$ (A anneau quelconque)

⚠ $\mathbb{Z}[X]$ est "plus compliqué" que $\mathbb{Q}[X]$ ou $\mathbb{R}[X]$

$A[[X]]$

Notions élément inéductible, algèbre

SLOGAN : « propriété universelle »

3) Quotients de Z et de K[X] (K un corps)

↓ Théorie des corps finis → Théorie des extensions de corps

4) Corps finis

Le groupe des inversibles d'un corps fini est cyclique (cryptographie)
Théorème de classification des corps finis (Galois)
Construction des corps finis Ex Construction du corps à 4 éléments

$\mathbb{Z}/2\mathbb{Z}$ ~~$\mathbb{Z}/4\mathbb{Z}$~~

(Théorie des codes correcteurs d'erreur)

5) Localisation

Corps des fractions $\mathbb{Z} \rightsquigarrow \mathbb{Q}$

Résultat Soit A un anneau
$\mathfrak{p}$ idéal premier de A
Alors la localisé $A_{\mathfrak{p}}$ est un anneau local.

6) Anneaux euclidiens, principaux, factoriels

euclidien ⇒ principal ⇒ factoriel
Il existe des anneaux intègres non factoriels

L'ARITHMÉTIQUE EST DIFFICILE !!

Éléments inversibles d'un anneau

$(A, +, \times)$ anneau $\quad (A, +)$ groupe commutatif

$(A, \times)$ n'est généralement un groupe sauf si $A = \{0\}$

$\forall a \in A, 0 \times a = 0$

$0 \neq 1$

$(\mathbb{Z} \setminus \{0\}, \times)$ $\quad (A \setminus \{0_A\}, \times)$ n'est pas un groupe en général

$\mathbb{Z}^\times = \{1, -1\}$ $\quad n \in \mathbb{Z}^\times \Leftrightarrow \exists m \in \mathbb{Z}, n \times m = 1$

$\mathbb{Z}^\times \subsetneq \mathbb{Z} \cap \mathbb{Q}^\times$

$A^\times$ $\quad A^*$

$\mathbb{Z}^* = \mathbb{Z} \setminus \{0\} \neq \mathbb{Z}^\times$

$\mathbb{R}^* = \mathbb{R} \setminus \{0\}$

$(A^\times, \times)$ est un groupe

$(A, +, \times) \to (A, +)$

$(A, +, \times) \to (A^\times, \times)$

A anneau

$\underset{\text{anneaux}}{\mathrm{Hom}}(\mathbb{Z}, A) = \{\cdot\}$

$n \longmapsto n \cdot 1_A = \underbrace{1_A + 1_A + 1_A \cdots + 1_A}_{n \text{ fois}}$ (si n est ≥ 1)

Idéal

A anneau → Sous-anneau

A anneau → idéal

$B \subset A$

B sous anneau de A
$(B,+)$ sous groupe de $(A,+)$
$\forall x \in B, \forall y \in B, xy \in B$
$1_A \in B$

B idéal de A
$(B,+)$ sous groupe de $(A,+)$
$\forall x \in B, \forall y \in A, xy \in B$
$x = 1_A$ $y \in A$ $y \in B$

Rq Si B est un idéal et $1_A \in B$, alors $B = A$

$A = \mathbb{Z}$

Sous anneaux de $\mathbb{Z}$: $\{\mathbb{Z}\}$
idéaux de $\mathbb{Z}$: $\{n\mathbb{Z}\}_{n \in \mathbb{N}}$

$A = \mathbb{Q}[X]$ idéaux de $\mathbb{Q}[X]$: $\{P \cdot \mathbb{Q}[X]\}_{P \in \mathbb{Q}[X]}$

Sous anneaux de $\mathbb{Q}[X]$: $\mathbb{Q} \subset \mathbb{Q}[X]$
$\cup$
B B sous anneau

ex $\mathbb{Z}\left[\frac{1}{n}\right] = \left\{\frac{a}{n^k}\right\}_{\substack{a \in \mathbb{Z} \\ k \in \mathbb{N}}}$ $n \in \mathbb{N} \setminus \{0\}$

I, J idéaux de A anneaux

$$I + J = \{ x + y \}_{\substack{x \in I \\ y \in J}}$$

$$2\mathbb{Z} + 3\mathbb{Z} \neq 5\mathbb{Z}$$

$m, n \in \mathbb{Z}$ $\quad m\mathbb{Z} + n\mathbb{Z} = d\mathbb{Z}$ avec $d = pgcd(n, m)$

(Théorème de Bezout)

Montrons $m\mathbb{Z} + n\mathbb{Z} \subset d\mathbb{Z}$

Soit $x \in m\mathbb{Z} + n\mathbb{Z}$

Il existe $y_1 \in \mathbb{Z}$ et $y_2 \in \mathbb{Z}$ tels que $x = m \cdot y_1 + n \cdot y_2$

d/n d/m

donc d/x donc $x \in d\mathbb{Z}$ □

Montrons que $d\mathbb{Z} \subset m\mathbb{Z} + n\mathbb{Z}$

Il suffit de montrer que $d \in m\mathbb{Z} + n\mathbb{Z}$

En effet, $m\mathbb{Z} + n\mathbb{Z}$ est un idéal

donc $d\mathbb{Z} \subset m\mathbb{Z} + n\mathbb{Z}$

↳ idéal de $\mathbb{Z}$ engendré par d

= plus petit idéal de $\mathbb{Z}$ contenant d.

↳ Théorème de Bezout

$$\exists y_1 \in \mathbb{Z}, \exists y_2 \in \mathbb{Z}, \; m y_1 + n y_2 = pgcd(m, n) = d$$

$$2\mathbb{Z} + 3\mathbb{Z} = \mathbb{Z}$$

A anneau

I, J

$S = \{ x \times y \}_{\substack{x \in I \\ y \in J}}$ En général, S n'est pas un idéal de A

$A = \mathbb{Z}$ $\quad I = m\mathbb{Z}$ $\quad J = n\mathbb{Z}$ $\quad m, n \in \mathbb{Z}$ $\quad S = \{ x \times y \}_{\substack{x \in I \\ y \in J}} = mn\mathbb{Z}$

En général, $I \cdot J$ est défini comme l'idéal engendré par S

Soit $x \in A$

$x \in I \cdot J \iff \exists n \in \mathbb{N} \setminus \{0\}$ $\exists (a_1, \dots, a_n) \in I^n$, $\exists (b_1, \dots, b_n) \in J^n$, $x = \sum_{i=1}^{n} \underbrace{a_i \times b_i}_{\in I \cap J}$ ($a_i \in I$, $b_i \in J$)

$m, n \in \mathbb{Z}$ $\quad (m\mathbb{Z}) \cdot (n\mathbb{Z}) = mn\mathbb{Z}$

$(m\mathbb{Z}) \cap (n\mathbb{Z}) = \text{ppcm}(m, n)\mathbb{Z}$

A anneau

I, J idéaux de A

$$I \cdot J \subsetneq I \cap J$$

$\mathrm{Hom}_{\text{anneaux}}(\mathbb{Q}, \mathbb{Z}) \overset{?}{=} \emptyset$

Indication Utilisez (proposition 14)
Si $\varphi \in \mathrm{Hom}_{\text{anneaux}}(A, B)$ alors $\varphi(A^\times) \subset B^\times$

$\varphi \in \mathrm{Hom}_{\text{anneaux}}(\mathbb{Q}, \mathbb{Z})$

$\varphi(\mathbb{Q}^\times) \subset \mathbb{Z}^\times = \{1, -1\}$

$x \in \mathbb{Q}^\times$ tq $\varphi(x) \notin \{1, -1\}$?

$\mathbb{Q}^\times = \mathbb{Q} \setminus \{0\}$

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

$= \varphi(1) + \varphi(1)$ (φ est un morphisme de groupes)

$= 1 + 1$ (φ est un morphisme d'anneaux)

$= 2 \notin \{1, -1\}$

CONTRADICTION !!