Structure d'anneaux

Ensemble A et deux lois de composition interne, $+$ et $\times$

i) $(A,+)$ est 1 groupe

ii) $\times$ est associative $\forall a,b,c \in A$ $a\times(b\times c) = (a\times b)\times c$

iii) $\times$ possède un élément neutre 1_A

iv) $\times$ est distributive à droite et à gauche par rapport à $+$

$\forall a,b,c \in A$ $a\times(b+c) = a\times b + a\times c$

$(b+c)\times a = b\times a + c\times b$

⚠ dans un anneau, tous les éléments de A n'admettent pas forcément d'inverse pour la loi $\times$.

Si c'est le cas, a est inversible et on le note a^{-1}

Caractérisation d'un sous-anneau

Une partie B de A est 1 sous-anneau ssi :

i) $1_A \in B$

ii) $\forall a,b \in B$ $a-b \in B$ ⊕ $0_A \in B$ (sous-groupe de A)

iii) $\forall a,b \in B$ $a\times b \in B$.

Dans un anneau commutatif $(a+b)^n = \sum_{k=0}^{n} \binom{n}{k} a^k b^{n-k}$.

Morphisme d'anneau

A et B deux anneaux $f: A \to B$ est 1 morphisme d'anneau si :

i) $f(1_A) = 1_B$

ii) $\forall a,b \in A$ $f(a+b) = f(a)+f(b)$

iii) $\forall a,b \in A$ $f(a\times b) = f(a)\times f(b)$

Anneaux particuliers.

A est intègre si $a \times b = 0 \Rightarrow a = 0$ ou $b = 0$

Un **corps** est un anneau commutatif dans lequel tout élément non nul est inversible (pour $\times$)

Sous-corps

K un corps, L une partie de K est 1 sous-corps si L est un sous-anneau de K qui est 1 corps, ssi

i) $1_K \in L$

ii) $\forall a, b \in L \quad a - b \in L$

iii) $\forall a, b \in L \quad a \times b \in L$

iv) $\forall a \in L$ non nul, $a^{-1} \in L$

Idéaux et divisibilité

A un anneau commutatif.

- Une partie I de A est un idéal si $(I, +)$ est un groupe et si $\forall a \in A$ et $u \in I$ alors $au \in I$ (prop d'absorption)

Le noyau d'un morphisme est un idéal.

Prop Une partie I de A est 1 ideal ssi
I est non vide et vérifie

i) $\forall x, y \in I \quad x - y \in I$

ii) $\forall x \in I \; \forall a \in A \quad ax \in I$

Si x est un élément de A alors $xA := \{xa, a \in A\}$ est un ideal de A et c'est le plus petit idéal contenant x.
C'est l'idéal engendré par x

Si A est intègre, $x, y \in A$ alors on dit que $x | y$ ssi
$\exists c \in A$ tq $cx = y$

Prop Soit A anneau commutatif intègre et $x, y \in A$
Alors $x | y$ ssi $yA \subset xA$

Idéaux de $\mathbb{Z}$, anneau $\mathbb{Z}/n\mathbb{Z}$

Théorème : Les idéaux de $\mathbb{Z}$ sont les ensembles $n\mathbb{Z}$, pour $n \in \mathbb{N}$

On définit la relation de congruence modulo n comme une relation d'équivalence sur $\mathbb{Z}$. $a \equiv b [n] \Leftrightarrow a - b \in n\mathbb{Z}$
$\bar{a}$ classe d'équivalence de a et $\mathbb{Z}/n\mathbb{Z}$ l'ensemble des classes d'équivalence pour cette relation.

Théorème : on munit de $\mathbb{Z}/n\mathbb{Z}$ d'une structure d'anneau avec
$$\bar{a} + \bar{b} = \overline{a+b}$$
$$\bar{a} \times \bar{b} = \overline{a \times b}$$

Théorème : $\bar{k}$ est inversible dans $\mathbb{Z}/n\mathbb{Z}$ ssi $k \wedge n = 1$

Corollaire : $\mathbb{Z}/n\mathbb{Z}$ est un corps, muni de $+$ et $\times$ ssi n premier

Théorème chinois : Si $n, m \geq 2$ sont tq $n \wedge m = 1$ alors
l'anneau produit $\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$ est isomorphe à $\mathbb{Z}/nm\mathbb{Z}$

Idéaux et arithmétique de polynômes

$\mathbb{K}$ sous-corps de $\mathbb{C}$

Théorème : Les idéaux de $\mathbb{K}[X]$ sont les idéaux (P) engendrés par un polynôme $P \in \mathbb{K}[X]$
$$(P) := \{AP ; A \in \mathbb{K}[X]\}$$

de plus $(P) = (Q)$ ssi $\exists \lambda \in \mathbb{K}^*$ $P = \lambda Q$

Rq $P, Q \in \mathbb{K}[X]$ l'ensbl $\{AP + BQ,\ A, B \in \mathbb{K}[X]\} = (P) + (Q)$ est un ideal de $\mathbb{K}[X]$. Il existe un polynôme unitaire D unique tel que $(P) + (Q) = (D)$. D est le pgcd (A, B)

Th. de Bézout : Soient $A, B \in \mathbb{K}[X]$ non nuls.
Alors $A \wedge B$ ssi $\exists\, U, V \in \mathbb{K}[X]$ $AU + BV = 1$

Lemme de Gauss : $A, B, C \in \mathbb{K}[X]$ non nuls. On suppose $A \wedge B = 1$
Alors si $A \mid BC$, on a $A \mid C$

Un polynôme P est irréductible s'il est de degré supérieur ou égal à 1 et si tous ses diviseurs sont les polynômes constants ou associés à P

Théorème : Les polynômes irréductibles de $\mathbb{C}[X]$ sont les polynômes de degré 1

Théorème : les polynômes irréductibles de $\mathbb{R}[X]$ sont les polynômes de degré 1 et les polynômes de degré 2 dont le discriminant est négatif.

Algèbre

On appelle $\mathbb{K}$-algèbre muni de 2 lois internes $+, \times$ et d'1 loi externe.

$(E, +, \times)$ anneau

$(E, +, \cdot)$ espace vectoriel sur $\mathbb{K}$.

$\forall a \in \mathbb{K}$ $\forall (x,y) \in E^2$ $(a \cdot x) \times y = x \times (a \cdot y) = a \cdot (x \times y)$

Si E et F sont deux algèbres, $f : E \to F$ est un morphisme d'algèbre ssi - c'est 1 morphisme d'anneau
- une application linéaire