Définition 2.8 - *éléments associés*

Deux un éléments d'un anneaux sont dits *associés* lorsqu'ils sont égaux à multiplication près par un élément inversible.

Définition 2.20 (1) - *diviseurs de zéro*

Soit $(A, +, \times)$ un anneau. on appelle *diviseurs de zéro* deux éléments a et b de A,tels que $ab = 0_A$

Définition 2.20 (2) - *anneau intègre*

Soit $(A, +, \times)$ un anneau. on dit que *A est intègre* lorsque :

1. $A \neq \{0_A\}$
2. $\times$ est commutative
3. A n'admet pas de diviseur zéro : $\forall (a, b) \in A^2,\ a \neq 0 \text{et} b \neq \Longrightarrow\ ab \neq 0$

Théorème 2.23 - *caractérisation de la structure de corps*

Soit $(\mathbb{K}, +, \times)$ un ensemble muni de deux lois de composition internes. $\mathbb{K}$ est un corps si et seulement si :

1. $(\mathbb{K}, +)$ est un groupe abélien
2. $(\mathbb{K} \setminus \{0_{\mathbb{K}}\}, \times)$ est un groupe abélien
3. $\times$ est distributive sur $+$

Théorème 2.26 - *caractérisation de sous-corps*

Soit $(\mathbb{K}, +, \times)$ un corps et $L \subset \mathbb{K}$. L est un sous-corps de $\mathbb{K}$ si et seulement si :

1. L est un sous-anneau de $\mathbb{K}$
2. tout élément non nul de L est inversible dans L

Proposition 2.29 - *condition suffisante de caractère de corps*

Tout anneau intègre fini est un corps.

Définition 2.30 - *structure d'idéal*

Soit $(A, +, \times)$ un anneau commutatif. On appelle *idéal de A* une partie I de A telle que :

1. $(I, +)$ est un sous-groupe de $(A, +)$
2. I est attracteur pour $\times$: $\forall i \in I, \forall a \in A, ai = ia \in I$

Proposition 2.32 - *images directe et réciproque d'un idéal*

Soit A et B deux anneaux commutatifs, $f : A \to B$ un morphisme d'anneaux.

1. L'image directe d'un idéal de A par f est un idéal de B
2. L'image réciproque d'un idéal de B par f est un idéal de A

Définition 2.34 - *idéal engendré par un élément*

Soit $(A, +, \times)$ un anneau commutatif. Soit $x \in A$ L'ensemble xA des multiples de x dans A est un idéal de A, appelé *idéal engendré par x*. On le note (x).

Théorème 2.36 - *idéaux de $(\mathbb{Z}, +, \times)$*

L'ensemble des idéaux de $(\mathbb{Z}, +, \times)$ est $\{n\mathbb{Z}, n \in \mathbb{Z}\}$: $\mathbb{Z}$ est principal (car intègre aussi).

Définition 2.37 - *plus grand commun diviseur de deux entiers*

Étant donnés deux entiers a et b, l'ensemble $a\mathbb{Z} + b\mathbb{Z}$ est un idéal de $\mathbb{Z}$, son unique générateur positif est appelé *le plus grand diviseur commun de a et b*. Ainsi,

$$a\mathbb{Z} + b\mathbb{Z} = (a \wedge b)\mathbb{Z}$$

Définition 2.39 - *plus petit commun multiple de deux entiers*

Étant donnés deux entiers a et b, l'ensemble $a\mathbb{Z} \cap b\mathbb{Z}$ est un idéal de $\mathbb{Z}$, son unique générateur positif est appelé *plus petit commun multiple de a et b*. Ainsi,

$$a\mathbb{Z} \cap b\mathbb{Z} = (a \vee b)\mathbb{Z}$$

Théorème 2.44 - *produit d'anneaux quotients*

Soit $(n, p) \in \mathbb{N}^2$. Si n et p sont premiers entre eux, alors les anneaux $\mathbb{Z}/np\mathbb{Z}$ et $\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$ sont isomorphes.

Théorème 2.45 - *inversibles de* $(\mathbb{Z}/n\mathbb{Z}, +, \times)$

Soit $k \in \mathbb{Z}$. la classe $\mathrm{cl}(k)$ est inversible dans $(\mathbb{Z}/n\mathbb{Z}, +, \times)$ si et seulement si $k \wedge n = 1$.

Définition 2.48 - *fonction indicatrice d'Euler*

On appelle *fonction indicatrice d'Euler* la fonction $\varphi : \mathbb{N}^* \to \mathbb{N}$ qui à n associe le nombre $\varphi(n)$ d'entiers de l'intervalle $[\![1, n]\!]$ premiers avec n. En fait,

$$\forall n \in \mathbb{N}^*, \varphi(n) = \mathcal{U}\Big((\mathbb{Z}/n\mathbb{Z}, +, \times)\Big)$$

Proposition 2.48 bis - *image de la fonction indicatrice d'Euler par un entier premier*

Soit $p \in \mathbb{P}$. On a :

$$\varphi(p) = p - 1$$

Proposition 2.49 - *théorème d'Euler*

Soit k et n deux entiers premiers entre eux. Alors on a :

$$k^{\varphi(n)} \equiv 1\,[n]$$
$$\text{et donc} \quad k^{\varphi(n)+1} \equiv k\,[n]$$

Proposition 2.50 - *caractérisation du caractère de corps de* $\mathbb{Z}/n\mathbb{Z}$

$\mathbb{Z}/n\mathbb{Z}$ est un corps si et seulement si n est premier.

Théorème 2.51 - *petit théorème de Fermat*

Soit $p \in \mathbb{P}$. Pour tout entier x,

$$x^p \equiv x\,[p]$$

Théorème 2.52 - *groupe des inversibles de* $\mathbb{Z}/p\mathbb{Z}$, $p \in \mathbb{P}$

Soit $p \in \mathbb{P}$. Alors le groupe multiplicatif $\mathcal{U}(\mathbb{Z}/p\mathbb{Z})$ est isomorphe au groupe additif $\mathbb{Z}/(p-1)\mathbb{Z}$

Proposition 2.54 - *indicatrice d'Euler du produit de premiers entre eux*

Soit m et n premiers entre eux. Alors :

$$\varphi(mn) = \varphi(m)\varphi(n)$$

Proposition 2.55 - *indicatrice d'Euler d'une puissance d'un premier*

Soit p un nombre premier et $\alpha \in \mathbb{N}^*$. Alors :

$$\varphi(p^\alpha) = p^\alpha - p^{\alpha-1}$$

Définition 2.72 - *stucture d'algèbre*

Un ensemble $(\mathcal{A}, +, \times, \cdot)$: muni de deux lois de composition internes $+$ et $\times$, et d'une loi $\cdot$ externe sur $\mathbb{K}$, est une *$\mathbb{K}$-algèbre* si :

1. $(\mathcal{A}, +, \times)$ est un anneau.
2. $(\mathcal{A}, +, \cdot)$ est un $\mathbb{K}$-espace vectoriel.
3. $\times$ et $\cdot$ sont compatibles :

$$\forall (a,b) \in \mathcal{A}^2, \forall (\lambda, \mu) \in \mathbb{K}^2, (a \cdot x) \times (b \cdot y) = (ab) \cdot (x \times y)$$

Définition 2.74 - *sous-algèbre*

Un ensemble $\mathcal{B}$ est une *sous-algèbre* d'une algèbre $\mathcal{A}$ si :

1. $\mathcal{B}$ est un sous-anneau de $\mathcal{A}$.
2. $\mathcal{B}$ est un sous-espace vectoriel de $\mathcal{A}$.

mais il suffit d'avoir :

1. $1_\mathcal{A} \in \mathcal{B}$
2. $\mathcal{B}$ stable par $\times$
3. $\mathcal{B}$ stable par combinaison linéaire

Définition 2.76 - *morphisme d'algèbre*

Soit $(\mathcal{A}, +_\mathcal{A}, \times_\mathcal{A}, \cdot_\mathcal{A})$ et $(\mathcal{B}, +_\mathcal{B}, \times_\mathcal{B}, \cdot_\mathcal{B})$ deux $\mathbb{K}$-algèbres. $f : A \to B$ est un *morphisme de $\mathbb{K}$-algèbres* si :

1. f est linéaire.
2. f respecte le produit.