

*Note de l'auteur, c'est un résumé des notes de cours de théorie des anneaux, pas tous les théorèmes, définitions, et autres y sont écrites, seules celles que je veux retenir et qui ne sont pas évidentes.*

## Chapitre 1

**Proposition 1.** *Soit  $A$  un anneau. Alors l'ensemble  $A^{n \times n}$  des matrices de tailles  $n \times n$  sur  $A$  est un anneau.*

**Proposition 2.**  $\mathbb{Z}/n\mathbb{Z}$  est un anneau.

**Définition 1.** *Un sous-anneau  $B$  de l'anneau  $A$  est un sous-groupe additif de  $A$  tel que :*

1.  $\forall a, b \in B, ab \in B$
2.  $1 \in B$

**Corollaire 1.** *L'intersection de tous les sous-anneaux de l'anneau  $A$  est l'ensemble  $\{n \cdot 1 | n \in \mathbb{Z}\}$ , avec la notation usuelles des groupes additifs.*

**Définition 2.** *Si  $A$  est un anneau, on dit qu'un élément  $a$  de  $A$  est inversible s'il existe  $b$  de  $A$  tel que  $ab = ba = 1$ . Un tel élément  $b$  est alors unique et est appelé inverse de  $a$ .*

**Définition 3.** *L'ensembles des éléments inversibles d'un anneau  $A$  est noté  $U(A)$ .*

**Proposition 3.**  $U(A)$  est un groupe sous la multiplication.

**Définition 4.** *Dans un anneau  $A$  un diviseur de 0 est un élément  $a$  de  $A$ , tel que  $a \neq 0$  et :*

1.  $ab = 0$  ( $a$  est un diviseur de 0 à gauche).
2.  $ba = 0$  ( $a$  est un diviseur de 0 à droite).

**Définition 5.** *Un anneau est dit intègre s'il n'a aucun diviseur de 0.*

**Proposition 4.** *Si  $a, b, c \in A$ , un anneau intègre. Alors  $ab = 0 \Rightarrow a = 0$  ou  $b = 0$ . De plus, si  $a \neq 0$  et  $ab = ac \Rightarrow b = c$  et  $ba = ca \Rightarrow b = c$ .*

**Proposition 5.** *Soient  $A, B$  deux anneaux. L'ensemble  $A \times B$  muni de l'addition*

$$(a, b) + (a', b') = (a + a', b + b')$$

*et de la multiplication*

$$(a, b) \cdot (a', b') = (aa', bb')$$

*est un anneau, avec  $0_{A \times B} = (0, 0)$  et l'élément neutre  $1_{A \times B} = (1, 1)$ . Il est commutatif si et seulement si  $A$  et  $B$  le sont aussi. L'anneau  $A \times B$  n'est pas intègre.*

**Définition 6.** *On appelle  $A \times B$  l'anneau produit de  $A$  et  $B$ .*

**Proposition 6.**  $U(A \times B) = U(A) \times U(B)$

**Définition 7.** *Un homomorphisme d'anneau  $f : A \longrightarrow B$  est une fonction tel que :*

1.  $f$  est un homomorphisme de groupes additifs.
2.  $\forall a, b \in A, f(aa') = f(a)f(a')$ .
3.  $f(1_A) = 1_B$ .

**Définition 8.** Un idéal dans un anneau  $A$  est un sous-ensemble  $I$  tel que :

1.  $I$  est un sous-groupe additif.
2.  $\forall a \in A, \forall x \in I, ax, xa \in I$ .

**Proposition 7.** Le noyau d'un homomorphisme est un idéal.

**Proposition 8.** Soit  $I$  un idéal d'un anneau  $A$ , tel que  $I \neq A$ . On construit le groupe additif  $A/I$ , quotient des groupes additifs  $A$  et  $I$ . Alors  $A/I$  est un anneau, tel que l'homomorphisme canonique de groupe  $A \rightarrow A/I$  est aussi un homomorphisme d'anneaux.

**Définition 9.** On appelle  $A/I$  l'anneau quotient de  $A$  par l'idéal  $I$ .

**Théorème 1.** Il est à la fin de la page 7(chapitre 1), il n'est pas copiable à cause d'une figure. À lire.

**Corollaire 2.** Si  $f : A \rightarrow B$  est un isomorphisme d'anneau, on a toujours l'isomorphisme d'anneau  $A/\ker(f) \simeq f(A)$

**Proposition 9.** L'image et l'image réciproque d'un sous-anneau est un sous-anneau. L'image réciproque d'un idéal est un idéal. Si l'homomorphisme est surjectif, alors l'image d'un idéal est un idéal.

**Proposition 10.**  $\mathbb{Z}/m\mathbb{Z}$  est intègre si et seulement si  $m$  est premier.

**Proposition 11.** Les éléments inversibles de  $\mathbb{Z}/m\mathbb{Z}$  sont les  $n$  avec  $n \perp m$ .

**Corollaire 3.**  $U(\mathbb{Z}/m\mathbb{Z})$  est en bijection avec  $\{n | 0 \leq n \leq m-1, n \perp m\}$ . En particulier  $|U(\mathbb{Z}/m\mathbb{Z})| = \varphi(m)$ .

**Rappel 1.**  $\varphi(m) = |\{n | 0 \leq n \leq m-1\}|$ .  $\varphi$  est appelé l'indicateur d'Euler, ou fonction d'Euler.

**Proposition 12.** Si  $m, p$  sont premier entre eux, alors  $\varphi(mp) = \varphi(m)\varphi(p)$ .

**Corollaire 4.** Si  $m = p_1^{m_1} \dots p_k^{m_k}$ ,  $p_i$  premiers distincts, alors

$$\begin{aligned}\varphi(m) &= \prod_{i=1}^k (p_i^{m_i} - p_i^{m_i-1}) \\ &= m \prod_{i=1}^k \left(1 - \frac{1}{p_i}\right)\end{aligned}$$

**Définition 10.** La caractéristique d'un anneau  $A$  est l'ordre pour la loi additive de l'élément neutre de la loi multiplicative. Par exemple, la caractéristique de  $\mathbb{Z}/n\mathbb{Z}$  est  $n$ , car  $n \cdot 1 = 0 \bmod n$

**Proposition 13.** Si la caractéristique d'un anneau intègre n'est pas nulle, c'est un nombre premier.

**Proposition 14.** Si  $A$  est un anneau commutatif de caractéristique  $p$ , un nombre premier, alors l'application  $F : A \rightarrow A, x \mapsto x^p$ , est un homomorphisme d'anneaux. On l'appelle l'homomorphisme de Frobenius.