

*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

**Définition 1.** *Un anneau est dit commutatif si la loi de multiplication est commutative.*

**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 2.** *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 3.** *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 4.** *L'ensembles des éléments inversibles d'un anneau  $A$  est noté  $U(A)$ .*

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

**Définition 5.** *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 6.** *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 7.** *On appelle  $A \times B$  l'anneau produit de  $A$  et  $B$ .*

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

**Définition 8.** 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 9.** 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  $A \longrightarrow A/I$  est aussi un homomorphisme d'anneaux.

**Définition 10.** 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  $f : A \longrightarrow B$  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 11.** 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.*

**Définition 12.** *Un corps est un anneau où tout élément non nul est inversible.*

**Proposition 15.** *Un corps est intègre.*

**Définition 13.** *Un sous-corps d'un corps est un sous-anneau qui contient l'inverse de chaque éléments non nuls qu'il contient.*

**Remarque 1.** *Un sous-corps est un corps.*

**Proposition 16.** *L'anneau commutatif  $A$  est un corps si et seulement si ses seuls idéaux sont  $\{0\}$  et  $A$ .*

**Proposition 17.**  *$p$  est premiers si et seulement si  $\mathbb{Z}/p\mathbb{Z}$  est un corps.*

**Définition 14.** *Un idéal  $I \neq A$  d'un anneau commutatif  $A$  est dit maximal si :  $\forall J$  idéal de  $A$ ,  $I \subseteq J \subseteq A$ , on a  $J = I$  ou  $J = A$ .*

**Proposition 18.** *Soit  $A$  un anneau commutatif et  $I$  un idéal. Alors  $I$  est maximal si et seulement si  $A/I$  est un corps.*

**Corollaire 5.** *Les idéaux (ou sous-groupes) maximaux de  $\mathbb{Z}$  sont les  $p\mathbb{Z}$ ,  $p$  premier.*

**Proposition 19.** *Si un corps  $K$  est de caractéristique non nulle, celle-ci étant un nombre premier, et  $K$  contient un sous-corps isomorphe à  $\mathbb{Z}/p\mathbb{Z}$ , à savoir son sous-corps premier.*

**Proposition 20.** *Soit  $K$  un corps et  $A$  un anneau). Si  $f : K \rightarrow A$  est un homomorphisme d'anneaux, alors  $f$  est injectif.*

**Proposition 21.** *L'ensemble  $\{a + b \cdot i \mid a, b \in \mathbb{Z}\}$  est un sous-anneau de  $\mathbb{C}$  dont les éléments inversibles sont  $\{-1, 1, -i, i\}$*

**Proposition 22.** *Soit  $E$  et  $A$  un anneau. L'ensemble  $A^E$  des fonctions de  $E$  dans  $A$  est un anneau. La somme et le produit sont défini par :*

1.  $(f + g)(e) = f(e) + g(e)$ .
2.  $(f \cdot g)(e) = f(e) \cdot g(e)$ .

*Les éléments neutres pour l'addition et la multiplication sont les fonctions constantes égale, l'une à 0, l'autre à 1.*

## Chapitre 2

**Définition 15.** *Dans un anneau, on dit que  $a$  divise  $b$ , noté  $a|b$ , s'il existe  $c$  tel que  $ac = b$ . Alors  $b$  s'appelle multiple de  $a$  et  $a$  un diviseur de  $b$ . Note, aucun rapport avec diviseur de 0.*

- Remarque 2.** 1. si  $a$  est inversible,  $a$  divise n'importe quel  $b$ , car  $b = a(a^{-1}b)$   
 2. si  $a$  divise  $b$  et si  $u$  est inversible, alors  $au$  divise aussi  $b$ , car  $b = ac \Rightarrow b = (au)(u^{-1}c)$ .

**Définition 16.** Deux éléments  $a$  et  $b$  de  $A$ , anneau commutatif, sont dits associés, s'il existe  $u \in A$ ,  $u$  inversible, tel que  $b = au$ .

**Proposition 23.** Si  $A$  est intègre, alors  $a$  et  $b$  associés est une relation d'équivalence. On a

$$Aa = Ab \Leftrightarrow a \text{ et } b \text{ associés.}$$

**Définition 17.** Un élément non nul et non inversible d'un anneau commutatif intègre  $A$  est dit irréductible si et seulement si  $\forall b, c \in A$ ,  $a = bc \Rightarrow b$  ou  $c$  inversible.

**Définition 18.** Deux éléments  $a$  et  $b$  d'un anneau commutatif intègre  $A$  sont dits premiers entre eux si :  $\forall x \in A$ ,  $x$  divise  $a$  et  $x$  divise  $b \Rightarrow x$  inversible.

**Définition 19.** Soient  $A$  un anneau intègre et  $\sigma : A^* \rightarrow \mathbb{N}$  une application. L'anneau  $A$  est euclidien pour  $\sigma$  si :

1. pour tous  $a, b \in A^*$  tel que  $a$  divise  $b$ , on a  $\sigma(a) \leq \sigma(b)$ .
2. pour tous  $a \in A$  et  $b \in A^*$ , il existe  $q$  et  $r \in A$  tel que  $a = bq + r$  avec  $r = 0$  ou  $\sigma(r) < \sigma(b)$ .

L'application  $\sigma$  s'appelle parfois un stahme (ou une valuation).

**Définition 20.** Un anneau commutatif est dit principal si tout idéal est principal.

1. Un idéal d'un anneau commutatif  $A$  est dit principal s'il est de la forme  $Aa$ ,  $a \in A$ .

**Remarque 3.**  $Aa =$  ensemble des multiples de  $A$ .

**Théorème 2.** Tout anneau euclidien est principal.

**Définition 21.** Soit  $A$  un anneau commutatif intègre. Il est dit factoriel si :

1. Tout élément  $a$  de  $A$ , qui n'est ni nul ni inversible, est un produit d'éléments irréductibles.

$$a = p_1 \dots p_i$$

2. Si pour un élément de  $a$   $p_1 \dots p_n = q_1 \dots q_m$ , alors  $m = n$  et il existe une permutation  $\sigma$  de l'ensemble  $\{1, \dots, n\}$  ainsi que des éléments inversibles  $u_1, \dots, u_n$  tel que  $p_i = u_i q_{\sigma(i)}$  pour tout  $i$ .

**Définition 22.** Un anneau commutatif  $A$  satisfait la condition de chaîne ascendante si pour toute suite croissante d'idéaux

$$I_1 \subseteq I_2 \subseteq I_3 \subseteq \dots \subseteq I_n \subseteq \dots$$

Il existe  $r$  tel que  $I_s = I_r$ ,  $\forall s \geq r$ .

**Lemme 1.** Un anneau principal satisfait à la condition de chaîne ascendante.

**Lemme 2.** Soit  $A$  un anneau principal intègre. Alors  $a, b$  sont premiers entre eux  $\Leftrightarrow \exists x, y \in A$  tel que  $ax + by = 1$ .

**Lemme 3.** Soit  $A$  un anneau commutatif intègre principal. Si  $a \perp b$  et si  $a$  divise  $bc$ , alors  $a$  divise  $c$ .

**Théorème 3.** Soit  $A$  un anneau commutatif intègre. Si  $A$  est principal,  $A$  est factoriel.

**Corollaire 6.**  $\mathbb{Z}$  et  $K[x]$  sont factoriels ( $K$  corps commutatif).

**Théorème 4.** Si  $A$  est un anneau factoriel, alors  $A[x]$  est un anneau factoriel.

**Corollaire 7.** Si  $A$  est un anneau factoriel, alors  $A[x_1, \dots, x_n]$  est un anneau factoriel.

**Lemme 4.**  $A[x_1, \dots, x_n] \simeq B[x_n]$  où  $B = A[x_1, \dots, x_{n-1}]$

**Remarque 4.** Le corollaire implique que  $\mathbb{Z}[x]$  est factoriel. Les éléments irréductibles de  $\mathbb{Z}[x]$  sont les  $+p$  ou  $-p$ ,  $p$  premier dans  $\mathbb{N}$ , et les polynômes  $P(x) \in \mathbb{Z}[x]$ , de degré  $\geq 1$ , qui sont irréductibles dans  $\mathbb{Q}[x]$ , et qui sont primitifs.

**Remarque 5.** On dit que  $0 \neq P(x) = a_n x^n + \dots + a_0 \in \mathbb{Z}[x]$  est primitif si  $\text{pgcd}(a_n, \dots, a_0) = 1$

**Définition 23.**  $A = \mathbb{Z}[i] = \{a + bi | a, b \in \mathbb{Z}$

$$N(a + bi) = a^2 + b^2.$$

On sait que  $z \in A$  est inversible si et seulement si  $N(z) = 1 \Leftrightarrow z = 1, -1, i, -i$ .

**Théorème 5.**  $A$  est euclidien.

**Corollaire 8.**  $\mathbb{Z}[i]$  est principal et factoriel.

**Théorème 6.** Soit  $p$  un nombre premier,  $p \neq 2$ . Alors les conditions suivantes sont équivalentes :

1.  $p \equiv 1 \pmod{4}$
2.  $-1$  est un carré dans  $\mathbb{Z}/p\mathbb{Z}$ .
3. il existe  $a, b \in \mathbb{Z}$  tel que  $p = a^2 + b^2$ .
4.  $p$  n'est pas irréductible dans  $\mathbb{Z}[i]$ .

**Corollaire 9.** Les éléments irréductibles de  $\mathbb{Z}[i]$  sont :

1.  $1 + i$
2. les  $p$  premiers dans  $\mathbb{N}$  avec  $p \equiv 3 \pmod{4}$ .
3. les  $a + bi$ ,  $a - bi$  tel que  $a^2 + b^2$  est premier dans  $\mathbb{N}$  et leurs associés.

De plus la décomposition  $p = a^2 + b^2$  d'un nombre premier est unique.

**Corollaire 10.** Soit  $n = \prod p^{n_p}$ , pour  $p$  premiers distincts (voir chap 2 bis page 5). Alors  $n$  est somme de deux carré si et seulement si  $\forall p \equiv 3 \pmod{4}$ , on a  $n_p$  pair.

Note : À partir de maintenant on prend  $A = \mathbb{Z}$  pour  $A[x]$ . C'est juste pour se simplifier la vie. Donc on parle ici de  $\mathbb{Z}[x]$ .

**Définition 24.** Un polynôme  $p \in \mathbb{Z}[x]$  est dit primitif si le pgcd de ses coefficient est 1. Il est en particulier non nul.

**Lemme de Gauss**

**Lemme 5.** Si  $P$  et  $Q$  sont primitif, alors  $PQ$  aussi.

**Définition 25.** Le dénominateur commun d'une famille de nombre rationnel  $r_1, \dots, r_n$  est un  $d \in \mathbb{N}^*$  tel que  $dr_1, \dots, dr_n \in \mathbb{Z}$

**Définition 26.** Le plus petit commun diviseur, appelé ppdc, est le plus petit d'entre eux.

**Remarque 6.** Vu que l'ensemble des dénominateurs communs des  $r_i$  forme un idéal de  $\mathbb{Z}$ , alors le ppdc des  $r_i$  les divise tous.

**Lemme 6.** Soient  $r_1, \dots, r_n$  des rationnels non nuls. Il existe un unique rationnel  $c > 0$  tel que  $r_1/c, \dots, r_n/c$  soient des entiers premiers entre eux. On a

$$c = \frac{1}{d} \text{pgcd}(dr_1, \dots, dr_n)$$

où  $d$  est le ppdc( $r_1, \dots, r_n$ ).

**Remarque 7.**  $r_1, \dots, r_n \in \mathbb{Z} \Leftrightarrow d = 1 \Leftrightarrow c \in \mathbb{N}^*$ . Dans ce cas,  $\text{pgcd}(r_i) = 1 \Leftrightarrow c = 1$ .

**Définition 27.** Étant donné  $P \in \mathbb{Q}[x]$ , non nul, on note  $c(p)$  l'unique nombre rationnel  $> 0$  tel que  $P/c(p)$  soit dans  $\mathbb{Z}[x]$  et soit primitif.

**Lemme 7.**  $c(PQ) = c(P)c(Q)$

**Remarque 8.** Notons  $\overline{P}$  l'unique polynôme primitif tel que  $P = c(P)\overline{P}$ , où  $P \in \mathbb{Q}[x]$  et  $P \neq 0$ . Nous avons donc  $\forall P, Q \in \mathbb{Q}^*[x], \overline{P \cdot Q} = \overline{P} \cdot \overline{Q}$

**Théorème 7.**  $\mathbb{Z}[x]$  est factoriel. Ses éléments irréductibles sont les polynômes de la forme

1.  $P \in \mathbb{Z}[x]$  primitif irréductible dans  $\mathbb{Q}[x]$ .
2.  $\pm \in \mathbb{Z}$ ,  $p$  nombre premier.

### Théorème de Wedderburn

**Théorème 8.** Tout corps fini est commutatif.

### Chapitre 3

**Proposition 24.** La caractéristique d'un corps fini est un nombre premier.

**Proposition 25.** Le centre d'un corps est un sous-corps.

**Corollaire 11.** Un corps fini contient  $\mathbb{Z}/p\mathbb{Z}$  son centre, où  $p$  est sa caractéristique.

**Proposition 26.** Soit  $K$  un corps et  $F$  un sous-corps commutatif. Alors  $K$  est un espace vectoriel sur  $F$ , de manière naturelle.

**Corollaire 12.** Soit  $K$  un corps fini de caractéristique  $p$ . Il existe alors  $n$  tel que  $|K| = p^n$ .

**Théorème 9.** Soit  $K$  un corps commutatif et  $P(x) \in K[x]$ . Il existe un sous-corps  $L$  de  $K$  tel que

1.  $\exists \alpha_1, \dots, \alpha_n \in L, P(x) = \lambda \prod_{i=1}^n (x - \alpha_i), \lambda \in K$ .

2.  $L$  est engendré par  $K$  et  $\alpha_1, \dots, \alpha_n$ . De plus  $L$  est unique à isomorphisme près.

On appelle  $L$  le corps de rupture de  $P(x)$ .

**Proposition 27.** Si  $A$  est un anneau commutatif de caractéristique  $p$  première, et si  $n \in \mathbb{N}$ , alors  $a \mapsto a^{p^n}$ ,  $A \rightarrow A$ , est un endomorphisme d'anneaux.

**Corollaire 13.** Si  $K$  est un corps commutatif fini à  $p^n$  éléments, alors  $F : K \rightarrow K$ ,  $a \mapsto a^p$  est un automorphisme de Frobenius. On a  $F^n = \text{id}$ , ou de manière équivalente,  $a^{p^n} = a$ ,  $\forall a \in K$ .

**Remarque 9.** Si on prend  $K = \mathbb{Z}/p\mathbb{Z}$ , on trouve que  $a^p = a$  : c'est le petit théorème de Fermat.

**Corollaire 14.** Soit  $K$  un corps commutatif à  $p^n$  éléments. Alors on a l'égalité des polynômes (à coefficients dans  $K$ )

$$x^{p^n} - x = \prod_{a \in K} (x - a)$$

(note voir exemple page 5 du chapitre 3).

**Proposition 28.** Soit  $K$  un corps commutatif et  $G$  un endomorphisme de  $K$ . Alors  $L = \{a \in K \mid G(a) = a\}$  est un sous-corps de  $K$ .

**Théorème 10.** Pour tout nombre premier  $p$ , et tout entier  $n \geq 1$ , il existe un corps à  $p^n$  éléments, unique à isomorphisme près.