3

Fiche de révisions chapitre 3 : Théorie des anneaux et des corps SEC301

I. Notions de base :

- Un anneau $(A, +, *)$ est une structure algébrique consistant en un ensemble A muni de 2 opérations binaires et qui possède les propriétés suivantes :
  - $(A, +)$ est un groupe commutatif (avec 0 pour neutre)
  - $(A, *)$ possède un élément neutre $1 (\neq 0)$
  - $(A, *)$ est associative $\forall a, b, c \quad a * (b * c) = (a * b) * c$
  - $*$ est distributive par rapport à $+ \quad \forall a, b, c \quad a * (b + c) = a * b + a * c$

- Soient $(A, +_A, *_A)$ et $(B, +_B, *_B)$ deux anneaux.
  Un homomorphisme d'anneaux est une application $\phi : A \to B$ telle que :
  $\phi(x +_A y) = \phi(x) +_B \phi(y) \quad \forall x, y \in A$
  $\phi(x *_A y) = \phi(x) *_B \phi(y) \quad \forall x, y \in A$

  ex : $\phi : \mathbb{C} \to M \quad a + bi \to \begin{pmatrix} a & -b \\ b & a \end{pmatrix}$

II. Anneaux intègres et euclidiens

- Soit A un anneau, un élément non nul $a \in A$ est un <u>diviseur de zéro</u> si il existe un $b \in A$ non nul tq $a \cdot b = 0$ ou $b \cdot a = 0$.

- Un anneau commutatif est appelé <u>domaine intégral</u> s'il ne possède <u>pas</u> de diviseurs de zéro.
  ex : $(\mathbb{Z}, +, \times), (\mathbb{Q}, +, \times), (\mathbb{R}, +, \times), (\mathbb{C}, +, \times)$

- Un anneau dont tous les éléments non nuls sont inversibles pour la multiplication est un <u>corps</u>
  ex : $(\mathbb{Q}, +, \times), (\mathbb{R}, +, \times), (\mathbb{C}, +, \times)$

- Tout corps commutatif est un domaine intégral.

- Tout application $N : A \to \mathbb{Z}^+$ avec $N(0) = 0$ est appelé <u>norme</u> sur le domaine intégral.

- Un domaine intégral est dit <u>domaine euclidien</u> : il existe une norme N tq $\forall a, d \in A \; \exists q, r \in A$ tq $a = q \cdot d + r$ avec $(r = 0$ ou $N(r) < N(d))$
  ex : $(\mathbb{Z}, +, \times)$

- PGCD(a, b) : élément non nul $c \in A$ tq $c | a$ et $c | b$.
  et si $\exists c' \in A$ tq $c' | a$ et $c' | b$ alors $c' | c$

- PPCM(a, b) : élément non nul $c \in A$ tq $a | c$ et $b | c$
  et si $\exists c' \in A$ tq $a | c'$ et $b | c'$ alors $c | c'$

- Soit A un domaine intégral, on dit que : <u>x associé à y</u> $\Leftrightarrow x | y$ et $y | x$
  Preuve : exo 1 TD3.

III. $(\mathbb{Z}, +, \times)$

- Un nombre naturel non nul est dit premier s'il n'est divisible que par deux nombres distincts : 1 et lui-même. ex: 2, 3, 7, ...

- Théorème fondamental de l'arithmétique: Soit $n \in \mathbb{N} \setminus \{0,1\}$

$$n = \prod_{i \in I} p_i^{\alpha_i} \quad \left| \begin{array}{l} p_i \text{ nombres premiers distincts.} \\ \alpha_i \in \mathbb{N} \setminus \{0\} \end{array} \right.$$

$$PGCD(m,n) = \prod_{i \in I \cap J} p_i^{\min(\alpha_i, \beta_i)} \quad \text{et} \quad PPCM(m,n) = \prod_{i \in I \cup J} p_i^{\max(\alpha_i, \beta_i)}$$

$$m \times n = PGCD(m,n) \times PPCM(m,n)$$

IV. $(F[x], +, \times)$

- Un polynome $P \in F[x]$ non constant est dit irréductible si toute écriture de $P = Q \cdot R$ avec $Q, R \in F[x]$ implique que au moins Q ou R soient constants non nuls.
ex: X^2+1 polynome irréductible $X^2+1 \in \mathbb{R}[x]$
$X^2+1 \in \mathbb{C}[x]$ n'est pas irréductible car $(X-i)(X+i) = X^2+1$

- Théorème de décomposition de polynômes de $F[x]$:

Tout polynome $P \in F[x]$ peut s'écrire comme le produit de puissances de polynômes irréductibles de coefficients dominants 1 le tout multiplié par une valeur C non nulle de F.

$$P(x) = C \cdot \prod_{i \in I} Q_i(x)^{e_i} \quad \left| \begin{array}{l} Q_i(x) \text{ polynome irréductible de coeff dominant 1} \\ C \in F \setminus \{0\} \\ e_i \in \mathbb{N} \setminus \{0\} \end{array} \right.$$

- PGCD, PPCM et algorithme d'Euclide

Lemme: Soit A un domaine euclidien et $q, d, r \in A$ (d et r non nuls simultanément). Alors $PGCD(d, q.d+r) = PGCD(d,r)$

- Relation de Bézout

Théorème de Bézout: Soit A un domaine euclidien et a et b deux éléments non nuls simultanément de A. Alors il existe $x, y \in A$ tq $ax + by = PGCD(a,b)$.