**Développements :**

- Théorème chinois
- Cyclicité de $(\mathbb{Z}/n\mathbb{Z})^\times$

**Références :**

- Algèbre - Le grand combat, Berhuy
- Carnet de voyage en Algébrie, Caldero, Peronnier
- Cours d'algèbre, Perrin
- Mathématiques pour l'agrégation, Rombaldi
- Théorie de Galois, Gozard

On fixe un entier $n \geq 2$.

# 1. L'anneau $\mathbb{Z}/n\mathbb{Z}$

## 1.1. Construction [Rombaldi]

- Def : on dit que $a, b \in \mathbb{Z}$ sont congrus modulo $n$ lorsque $n \mid (a-b)$
- Notation : $a \equiv b \bmod n$
- Rmq : c'est une relation d'équivalence
- Def : l'ensemble des classes d'équivalence est noté $\mathbb{Z}/n\mathbb{Z}$ ou $\mathbb{Z}/n$, la classe de $k \in \mathbb{Z}$ est notée $k \bmod n$ ou $\overline{k}$ lorsqu'il n'y a pas d'ambiguïté sur $n$
- Thm : il existe une unique structure d'anneau commutatif unitaire sur $\mathbb{Z}/n\mathbb{Z}$ telle que la surjection canonique $\pi_n : \mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ soit un morphisme d'anneaux

## 1.2. Structure et éléments remarquables [Berhuy, Perrin]

- Prop : pour $a \in \mathbb{Z}$, s'équivalent :
  - $\overline{a}$ est inversible dans $\mathbb{Z}/n\mathbb{Z}$ ssi $a$ et $n$ sont premiers entre eux
  - $\overline{a}$ est un diviseur de zéro ssi $n$ ne divise pas $a$ et $n$ et $a$ ne sont pas premiers entre eux
  - $\overline{a}$ est nilpotent ssi tout diviseur premier de $n$ divise également $a$
- Cor : si $n = p_1^{\alpha_1} \cdots p_r^{\alpha_r}$ (décomposition en produit de facteurs premiers), alors $\sqrt{n\mathbb{Z}} = p_1 \cdots p_r \mathbb{Z}$
- Thm : les idéaux de $\mathbb{Z}/n\mathbb{Z}$ sont les images par $\pi_n$ des idéaux de $\mathbb{Z}$ contenant $n$
- Thm : $\mathbb{Z}/n\mathbb{Z}$ possède $2^{\omega(n)}$ idempotents, où $\omega(n)$ est le nombre de diviseurs premiers de $n$
- Thm de structure des groupes abéliens finis (admis)

## 1.3. Théorème chinois [Berhuy, Caldero-Peronnier]

- Thm : si $m_1, \dots, m_r \in \mathbb{N}^*$ sont premiers entre eux deux à deux, alors l'application $\mathbb{Z} \to \mathbb{Z}/m_1 \times \cdots \times \mathbb{Z}/m_r$ définie par $a \longmapsto (a \bmod m_1, \dots, a \bmod m_r)$ est un morphisme d'anneaux surjectif de noyau $m_1 \cdots m_r\mathbb{Z}$, induisant un isomorphisme d'anneaux $\mathbb{Z}/m_1 \cdots m_r \cong \mathbb{Z}/m_1 \times \cdots \times \mathbb{Z}/m_r$
- Cor : si $n = p_1^{\alpha_1} \cdots p_r^{\alpha_r}$ (décomposition en produit de facteurs premiers), alors le morphisme ci-dessus induit un isomorphisme d'anneaux $\mathbb{Z}/n \cong \mathbb{Z}/p_1^{\alpha_1} \times \cdots \times \mathbb{Z}/p_r^{\alpha_r}$
- App : résolution de systèmes de congruences du type $x \equiv a \bmod m$, $x \equiv b \bmod n$
- Rmq :
  - pas toujours de solution si $m$ et $n$ ne sont pas premiers entre eux
  - si $a \bmod \delta = b \bmod \delta$ où $\delta = \operatorname{pgcd}(m, n)$, alors :
    - $x_0 = \frac{1}{\delta}(avn + bum)$ est solution, où $u, v \in \mathbb{Z}$ sont tels que $au + bv = \delta$
    - l'ensemble des solutions est $\{x_0 + k\mu \mid k \in \mathbb{Z}\}$, où $\mu = \operatorname{ppcm}(m, n)$
- Ex : résolution de $x \equiv 3 \bmod 21$, $x \equiv 10 \bmod 35$ dans $\mathbb{Z}$

# 2. Le groupe $(\mathbb{Z}/n\mathbb{Z})^\times$

## 2.1. Indicatrice d'Euler [Perrin, Rombaldi]

- Def : $\varphi(n) = |\{k \in \{1, \dots, n\} \mid \operatorname{pgcd}(k, n) = 1\}|$
- Prop : si $p$ est premier, alors :
  - $\varphi(p) = p - 1$
  - $\varphi(p^\alpha) = p^{\alpha-1}(p-1)$ pour tout $\alpha \in \mathbb{N}^*$
- Prop : $\varphi(n) = |(\mathbb{Z}/n\mathbb{Z})^\times|$
- Thm (Euler) : si $a \in \mathbb{Z}$ est premier avec $n$, alors $a^{\varphi(n)} \equiv 1 \bmod n$
- Cor (Fermat) : si $p$ est un nombre premier ne divisant pas $a \in \mathbb{Z}$, alors $a^{p-1} \equiv 1 \bmod p$

## 2.2. Structure de $(\mathbb{Z}/n\mathbb{Z})^\times$ [Berhuy, Perrin]

- Prop : si $p$ est un nombre premier, alors $\mathbb{F}_p^\times \cong \mathbb{Z}/(p-1)$
- Prop : si $n = p_1^{\alpha_1} \cdots p_r^{\alpha_r}$ (décomposition en produit de facteurs premiers), alors $(\mathbb{Z}/n)^\times \cong (\mathbb{Z}/p_1^{\alpha_1})^\times \times \cdots \times (\mathbb{Z}/p_r^{\alpha_r})^\times$
- Cor : $\varphi$ est multiplicative
- Cor : $\varphi(n) = n\prod_{i=1}^r (1 - 1/p_i)$
- Thm : $n = \sum_{d|n} \varphi(d)$
- Cor : $\varphi(n) = \sum_{d|n} d\mu(n/d)$ où $\mu$ est la fonction de Möbius
- Prop : si $p$ est un nombre premier impair et $\alpha \in \mathbb{N}_{\geq 2}$, alors $(\mathbb{Z}/p^\alpha)^\times \cong \mathbb{Z}/p^{\alpha-1}(p-1)$
- Prop :

  - $(\mathbb{Z}/2)^\times = \{1\}$
  - $(\mathbb{Z}/4)^\times \cong \mathbb{Z}/2$
  - $(\mathbb{Z}/2^\alpha)^\times \cong \mathbb{Z}/2 \times \mathbb{Z}/2^{\alpha-2}$ pour tout $\alpha \in \mathbb{N}_{\geq 2}$
- Thm : $(\mathbb{Z}/n\mathbb{Z})^\times$ est cyclique ssi :
  - $n = 4$
  - il existe $p$ premier impair et $\alpha \in \mathbb{N}^*$ tels que $n = p^\alpha$ ou $n = 2p^\alpha$

# 3. Cas où $n$ est premier

- Prop : s'équivalent :
  - $n$ est premier
  - $\mathbb{Z}/n\mathbb{Z}$ est intègre
  - $\mathbb{Z}/n\mathbb{Z}$ est un corps
- Notation : $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ pour $p$ premier

## 3.1. Polynômes à coefficients entiers [Berhuy, Perrin]

- Def : contenu $c(f)$ pour $f \in \mathbb{Z}[X]$
- Def : on dit que $f \in \mathbb{Z}[X]$ est primitif lorsque $c(f) = 1$
- Prop : si $f \in \mathbb{Z}[X]$ est primitif non constant et $p$ est un nombre premier, tels que :
  - le coefficient dominant de $f$ ne soit pas divisible par $p$
  - la réduction modulo $p$ de $f$ soit irréductible sur $\mathbb{F}_p$
  alors $f$ est irréductible sur $\mathbb{Z}$
- Thm (Eisenstein) : si $f = \sum a_k X^k \in \mathbb{Z}[X]$ et $p$ est un nombre premier, tels que :
  - $p$ ne divise pas $a_n$
  - $p$ divise $a_0, a_1, \ldots, a_{n-1}$
  - $p^2$ ne divise pas $a_0$
  alors $f$ est irréductible sur $\mathbb{Q}$ (et même sur $\mathbb{Z}$ si $f$ est primitif)
- App : $X^n - 2$ est irréductible sur $\mathbb{Q}$ pour tout $n \in \mathbb{N}^*$

## 3.2. Symboles de Legendre et de Jacobi [Berhuy, Gozard]

- Notation : $\mathbb{F}_p^{\times[2]} = \{x^2 \mid x \in \mathbb{F}_p^\times\}$
- Lemme : si $p$ est premier impair, alors $\mathbb{F}_p^\times / \mathbb{F}_p^{\times[2]}$ est un groupe d'ordre $2$
- Lemme : si $p$ est premier impair, alors $\mathbb{F}_p^{\times[2]} = \{x \in \mathbb{F}_p^\times \mid x^{(p-1)/2} = 1\}$

### 3.2.1. Symbole de Legendre

- Def : symbole de Legendre $\left(\frac{\cdot}{p}\right)$ pour $p$ premier impair

- Ex : $\left(\frac{5}{7}\right) = -1$
- Prop : pour tout $a \in \mathbb{Z}$, $\left(\frac{a}{p}\right) = a^{(p-1)/2}$
- Prop : le symbole de Legendre est un morphisme de groupes $\mathbb{F}_p^\times \to \{-1, 1\}$
- Prop :
  - $\left(\frac{-1}{p}\right) = (-1)^{(p-1)/2} = \begin{cases} 1 & \text{si } p \equiv 1 \bmod 4 \\ -1 & \text{si } p \equiv 3 \bmod 4 \end{cases}$
  - $\left(\frac{2}{p}\right) = (-1)^{(p^2-1)/8} = \begin{cases} 1 & \text{si } p \equiv \pm 1 \bmod 8 \\ -1 & \text{si } p \equiv \pm 3 \bmod 8 \end{cases}$
- Thm : loi de réciprocité quadratique

## 3.2.2. Symbole de Jacobi

- Def : symbole de Jacobi $\left(\frac{\cdot}{N}\right)$ pour $N \in \mathbb{N}_{\geq 2}$ impair
- Prop : pour tous $a, b \in \mathbb{Z}$, $\left(\frac{ab}{N}\right) = \left(\frac{a}{N}\right)\left(\frac{b}{N}\right)$
- Rmq :
  - si $\left(\frac{a}{N}\right) = -1$, alors $a$ n'est pas un carré modulo $N$
  - si $\left(\frac{a}{N}\right) = 1$, alors $a$ n'est pas nécessairement un carré modulo $N$ (par exemple avec $a = -1$ et $N = 21$)
- Prop :
  - $\left(\frac{-1}{N}\right) = (-1)^{(N-1)/2} = \begin{cases} 1 & \text{si } N \equiv 1 \bmod 4 \\ -1 & \text{si } N \equiv 3 \bmod 4 \end{cases}$
  - $\left(\frac{2}{N}\right) = (-1)^{(N^2-1)/8} = \begin{cases} 1 & \text{si } N \equiv \pm 1 \bmod 8 \\ -1 & \text{si } N \equiv \pm 3 \bmod 8 \end{cases}$
- Thm : loi de réciprocité quadratique pour le symbole de Jacobi