120

(120) Anneaux $\mathbb{Z}/n\mathbb{Z}$. Applications

I/ Structure de groupe

- Groupe cyclique : générateurs de $\mathbb{Z}/n\mathbb{Z}$, indicatrice d'Euler
  Tout groupe cyclique à n éléments est isomorphe à $(\mathbb{Z}/n\mathbb{Z}, +)$. (Demazure)
  ex : racines de l'unité
- Sous-groupes de $\mathbb{Z}/n\mathbb{Z}$ (Combes)
  → ils sont cycliques
- Morphisme de groupes de $\mathbb{Z}/n\mathbb{Z}$ dans $\mathbb{Z}/m\mathbb{Z}$ (pas de réf)
  d'abord dans le cas où $m = n$.

II/ Structure d'anneau

- Structure multiplicative : $\mathbb{Z}/n\mathbb{Z}$ est un anneau
  Divisibilité pour 0, 1, 11, éléments nilpotents
  - Lemme chinois (Combes) + ex de résolution d'équations
    texemple : $x^2 + x + 1 = 0$ dans $\mathbb{Z}/91\mathbb{Z}$.
    → calcul de l'inverse de l'isomorphisme par Bézout étendu.
- Groupe des inversibles : théorème de Fermat, nombre de Carmichael fournissent un contre-ex. (Demazure)
  Condition pour que $\mathbb{Z}/n\mathbb{Z}$ soit un corps
  Nombre d'inversibles, indicatrice d'Euler (Combes)
  Application du lemme chinois au groupe $(\mathbb{Z}/n\mathbb{Z})^*$
  $\varphi(n) = \prod_{i=1}^{r} \varphi(p_i^{\alpha_i})$

III/ Applications

- Automorphismes de $\mathbb{Z}/n\mathbb{Z}$ et groupes d'ordre pq (Perrin)
  $\mathrm{Aut}(\mathbb{Z}/n\mathbb{Z}) \simeq (\mathbb{Z}/n\mathbb{Z})^*$
  Caractérisation de $(\mathbb{Z}/p^\alpha\mathbb{Z})^*$.
  Appl : Thm 7.13 sur les groupes d'ordre pq, $p < q$ premiers.
- Théorème d'Euler et cryptographie RSA (Demazure)
  Proposition et théorème d'Euler
  Appl : cryptographie RSA.
- Corps $\mathbb{Z}/p\mathbb{Z}$ et arithmétique
  - $(\mathbb{Z}/p\mathbb{Z})^*$ cyclique (FGN)
  - Tests de primalités : Wilson (Gourdon), Rabin-Miller (Demazure)
  - Critère d'Eisenstein pour $\mathbb{Z}[X]$, avec application.
  - Carrés dans $\mathbb{Z}/p\mathbb{Z}$, -1 est un carré ssi $p = 2$ (Gourdon)
    Thm des deux carrés (Gourdon, Perrin)
  - Progression arithmétique de Dirichlet (FGN)
    version faible : nbr premiers $\equiv 1 \pmod n$ → infinité.