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

1 Le groupe $\mathbb{Z}/n\mathbb{Z}$

1.1 Étude algébrique

Définition 1. Soient $n \in \mathbb{N}^*, x, y \in \mathbb{Z}$. On dit qu'ils sont congrus modulo n si $x - y \in n\mathbb{Z}$, et on note $x \equiv y[n]$.

Proposition 2. $n\mathbb{Z}$ est un sous-groupe de $\mathbb{Z}$, distingué car $\mathbb{Z}$ abélien, c'est donc un groupe.

***Exemple* 3.** *$\mathbb{Z}/2\mathbb{Z} = \{\overline{0}, \overline{1}\}$ où $\overline{0}$ est la classe des entiers pairs et $\overline{1}$ la classe des entiers impairs.*

Théorème 4. À isomorphisme près, $\mathbb{Z}/n\mathbb{Z}$ est le seul groupe cyclique d'ordre n.

Proposition 5. Pour tout d diviseur de n, $\mathbb{Z}/n\mathbb{Z}$ possède un unique sous-groupe d'ordre d, engendré par $\overline{(\frac{n}{d})}$.

***Exemple* 6.** *Le sous-groupe d'ordre 2 de $\mathbb{Z}/4\mathbb{Z}$ est $2\mathbb{Z}/4\mathbb{Z} = \{\overline{0}, \overline{2}\}$.*

Définition 7. Pour $n \in \mathbb{N}^*$, on appelle indicatrice d'Euler de n, et on note $\varphi(n)$, le nombre de générateurs de $\mathbb{Z}/n\mathbb{Z}$.

Proposition 8. Pour tout $\overline{k} \in \mathbb{Z}/n\mathbb{Z}, \overline{k}$ engendre $\mathbb{Z}/n\mathbb{Z}$ si et seulement si $k \wedge n = 1$.

***Application* 9.** *Si p premier, $\varphi(p) = p - 1$ et $\varphi(p^\alpha) = p^{\alpha-1}(p-1)$.*

***Exemple* 10.** *Les générateurs de $\mathbb{Z}/6\mathbb{Z}$ sont $\overline{1}, \overline{5}$, et $\varphi(6) = 2$.*

Proposition 11. Pour tout $n \in \mathbb{N}^*$, on a $n = \sum_{d|n} \varphi(d)$.

Proposition 12. Il y a exactement $n \wedge m$ morphismes de $\mathbb{Z}/n\mathbb{Z}$ dans $\mathbb{Z}/m\mathbb{Z}$.

1.2 Produits directs

Théorème 13 (chinois)**.** Soient $m, n \in \mathbb{N}^*$. $\mathbb{Z}/mn\mathbb{Z}$ est isomorphe à $\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ si et seulement si $m \wedge n = 1$.

Théorème 14. Soit G un groupe abélien fini.
Alors il existe une unique suite d'entiers naturels $d_1, \cdots, d_k$ tels que G soit isomorphe à $\mathbb{Z}/d_1\mathbb{Z} \times \cdots \times \mathbb{Z}/d_k\mathbb{Z}$ et $\forall i \in [\![1, k-1]\!], d_i | d_{i+1}$.

***Exemple* 15.** *$\mathbb{Z}/36\mathbb{Z} \times \mathbb{Z}/15\mathbb{Z}$ est isomorphe à $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z} \times \mathbb{Z}/30\mathbb{Z}$.*

***Application* 16.** *À isomorphisme près, il existe 5 groupes abéliens d'ordre 48.*

2 L'anneau $\mathbb{Z}/n\mathbb{Z}$

Proposition 17. $n\mathbb{Z}$ est un idéal de $\mathbb{Z}$, $\mathbb{Z}/n\mathbb{Z}$ possède donc une structure d'anneau quotient. L'isomorphisme de groupes donné par le lemme chinois est en fait un isomorphisme d'anneaux.

2.1 Éléments inversibles

Proposition 18. $\overline{k}$ est inversible dans $\mathbb{Z}/n\mathbb{Z}$ si et seulement si $k \wedge n = 1$.

Corollaire 19. On a $|(\mathbb{Z}/n\mathbb{Z})^*| = \varphi(n)$.

Théorème 20 (Euler)**.** On a, pour tout $a \in \mathbb{Z}, a^{\varphi(n)} \equiv 1[n]$.

Corollaire 21 (Fermat)**.** Si p nombre premier, pour tout $a \in \mathbb{Z}, a^p \equiv a[p]$.

***Contre-exemple* 22.** *Nombres de Carmichael.*

***Application* 23** (Cryptage RSA)**.** *Soient p, q deux nombres premiers distincts. Soit $n = pq$, soient c, d tels que $cd \equiv 1[\varphi(n)]$. Les applications $\mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ définies par $c : \overline{x} \mapsto \overline{x}^c$ et $d : \overline{x} \mapsto \overline{x}^d$ sont respectivement appelées fonction de chiffrement et de déchiffrement. On a $c \circ d = d \circ c = \mathrm{Id}_{\mathbb{Z}/n\mathbb{Z}}$. On peut ainsi transmettre des messages cryptés à l'aide de la clé publique (n, c) et de la clé privée d.*

Proposition 24. Si $p \geq 3$ premier, alors $(\mathbb{Z}/p^\alpha\mathbb{Z})^*$ est isomorphe à $\mathbb{Z}/p^{\alpha-1}(p-1)\mathbb{Z}$. Si $\alpha \geq 3, (\mathbb{Z}/2^\alpha\mathbb{Z})^*$ est isomorphe à $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2^{\alpha-2}\mathbb{Z}$.

Proposition 25. Pour tout $n \in \mathbb{N}^*$, $\mathrm{Aut}(\mathbb{Z}/n\mathbb{Z})$ et $(\mathbb{Z}/n\mathbb{Z})^*$ sont isomorphes.

2.2 Éléments nilpotents et idempotents

Proposition 26. Soit $n = p_1^{\alpha_1} \cdots p_r^{\alpha_r} \in \mathbb{N}$. $\overline{x} \in \mathbb{Z}/n\mathbb{Z}$ est nilpotent si et seulement si $x \in p_1 \cdots p_r\mathbb{Z}$.

Proposition 27. $\overline{x} \in \mathbb{Z}/n\mathbb{Z}$ est idempotent si et seulement si, pour tout $i \in [\![1, r]\!], x \equiv 0[p_i^{\alpha_i}]$ ou $x \equiv 1[p_i^{\alpha_i}]$.

Corollaire 28. Il y a donc exactement 2^r éléments idempotents.

***Exemple* 29.** *Les idempotents de $\mathbb{Z}/12\mathbb{Z}$ sont $0, 1, 4, 9$.*

3 Le corps $\mathbb{Z}/p\mathbb{Z}$

3.1 Généralités

Proposition 30. $\mathbb{Z}/p\mathbb{Z}$ est un corps si et seulement si p est premier. On le note alors $\mathbb{F}_p$.

Théorème 31 (Wilson)**.** Soit $p \geq 2$. p est premier si et seulement si $(p-1)! \equiv -1[p]$.

Lemme 32. $\mathbb{F}_p$ est de caractéristique p.

***Application* 33.** *Tout corps fini K de caractéristique p est un $\mathbb{F}_p$-espace vectoriel. Si on note r sa dimension, il est de cardinal $q = p^r$. Le groupe additif de K est alors isomorphe à $(\mathbb{Z}/p\mathbb{Z})^r$, et son groupe multiplicatif à $\mathbb{Z}/(p^r-1)\mathbb{Z}$.*

3.2 Éléments carrés

Définition 34. Soit p nombre premier. Pour $a \in \mathbb{F}_p$, on définit le symbole de Legendre par $\left(\frac{a}{p}\right) = 0$ si $a = 0$, 1 si a est un carré dans $\mathbb{F}_p^*$ et -1 sinon.

Proposition 35. On a, pour $a \in \mathbb{F}_p$, $\left(\frac{a}{p}\right) = a^{\frac{p-1}{2}}$. En particulier, le symbole de Legendre est multiplicatif.

Corollaire 36. Il y a donc $\frac{p+1}{2}$ carrés dans $\mathbb{F}_p$.

Corollaire 37. -1 est un carré dans $\mathbb{F}_p$ si et seulement si $p \equiv 1[4]$.

Théorème 38 (Frobenius-Zolotarev)**.** Supposons $p \geq 3$, soit $u \in GL_n(\mathbb{F}_p)$. On a $\varepsilon(u) = \left(\frac{\det(u)}{p}\right)$.

Théorème 39 (Réciprocité quadratique)**.** Soient p, q nombres premiers impairs distincts. On a $\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}$.

***Exemple* 40.** *65 est un carré dans $\mathbb{F}_{29}$.*

4 Applications

4.1 Critères de divisibilité

Proposition 41. Soit $x = \sum_{j=0}^{k} a_j 10^j \in \mathbb{N}$. On a :

- $x \equiv \alpha_0 + \cdots + \alpha_k[3]$ et $x \equiv \alpha_0 + \cdots + \alpha_k[9]$.
- $x \equiv \alpha_0[2]$ et $x \equiv a_0[5]$.
- $x \equiv \alpha_0 - \alpha_1 + \cdots + (-1)^k \alpha_k[11]$.

4.2 Équations diophantiennes

Définition 42. On appelle équation diophantienne une équation de la forme $P(x_1, \cdots, x_n) = 0$, où $P \in \mathbb{Z}[X_1, \cdots, X_n]$ et dont les solutions recherchées sont entières.

Proposition 43. Soient $a \geq 2, b \in \mathbb{Z}^*, c \in \mathbb{Z}$. L'équation diophantienne $ax + by = c$ est équivalente à l'équation $\overline{b}\overline{y} = \overline{c}$ dans $\mathbb{Z}/a\mathbb{Z}$. Cette équation a des solutions si et seulement si $a \wedge b = 1$ ou si $c \in (a \wedge b)\mathbb{Z}$.

***Exemple* 44.** *Les solutions de $522x+2214y = 36$ sont $\{(34+123k, -8-29k), k \in \mathbb{Z}\}$.*

Proposition 45. $(x, y, z) \in (\mathbb{N}^*)^3$ est solution de $x^2 + y^2 = z^2$ si et seulement si il existe $d, u, v \in \mathbb{N}$ avec $u \wedge v = 1$ tels que (x, y, z) ou $(y, x, z) = (d(u^2-v^2), 2duv, d(u^2+v^2))$.

***Application* 46.** *Les équations diophantiennes $x^4 + y^4 = z^2$ et $x^4 + y^4 = z^4$ n'ont pas de solution non triviale.*

Théorème 47. Soit $\Sigma = \{n \in \mathbb{N}, \exists (a, b) \in \mathbb{N}^2, n = a^2 + b^2\}$. Soit $p \geq 3$ premier. Alors $p \in \Sigma \Leftrightarrow p \equiv 1 \mod 4$.

Corollaire 48. Soit $n \geq 2$, de décomposition en facteurs premiers $n = \prod_{p \in \mathcal{P}} p^{v_p(n)}$. Alors $n \in \Sigma \Leftrightarrow v_p(n)$ pair pour tout $p \equiv 3 \mod 4$.

4.3 Irréductibilité des polynômes dans $\mathbb{Z}[X]$

Théorème 49 (Eisenstein)**.** Soit $P = \sum_{k=0}^{n} a_k X^k \in \mathbb{Z}[X]$. S'il existe p premier tel que $p \nmid a_n$, $p | a_k$ pour tout $0 \leq k \leq n-1$ et $p^2 \nmid a_0$, alors P est irréductible dans $\mathbb{Q}[X]$, et dans $\mathbb{Z}[X]$ si son contenu est 1.

Théorème 50 (Réduction modulo p)**.** Soit $P \in \mathbb{Z}[X]$, soit p premier, on note $\overline{P}$ le polynôme obtenu en réduisant modulo p les coefficients de P. Si $\deg(\overline{P}) = \deg(P)$ et $\overline{P}$ irréductible dans $\mathbb{F}_p[X]$, alors P irréductible dans $\mathbb{Q}[X]$.

***Exemple* 51.** *$3X^3 + 17X - 11$ est irréductible dans $\mathbb{Z}[X]$ et dans $\mathbb{Q}[X]$.*

***Contre-exemple* 52.** *X^4+1 est réductible dans $\mathbb{F}_p[X]$ pour tout p premier, mais irréductible dans $\mathbb{Z}[X]$ et $\mathbb{Q}[X]$.*

Définition 53. Soit $n \in \mathbb{N}^*$, soit $\omega = e^{2i\pi/n}$. On définit $\Phi_n = \prod_{\substack{k \leq n \\ k \wedge n = 1}} (X - \omega^k)$.

Proposition 54. $\Phi_n \in \mathbb{Z}[X]$ est irréductible dans $\mathbb{Q}[X]$.

Développements

— Loi de réciprocité quadratique.
— Théorème des deux carrés.

Références

[1] F. Combes, Algèbre et géométrie, Bréal.

[2] X. Gourdon, Les maths en tête - Algèbre, Ellipses.

[3] D. Perrin, Cours d'algèbre, Ellipses.