Leçon 120 : Anneaux $\mathbf{Z}/n\mathbf{Z}$. Applications.

On rappelle que $\mathbf{Z}$ est un anneau euclidien. Ses seuls idéaux sont les $n\mathbf{Z}$ avec $n \in \mathbf{N}$. On dit que a est congru à b modulo n si n divise $a-b$. Cette relation est la relation d'équivalence associée à l'idéal $n\mathbf{Z}$. Elle est compatible avec l'addition et la multiplication dans $\mathbf{Z}$, ce qui munit l'ensemble quotient $\mathbf{Z}/n\mathbf{Z}$ d'une structure d'anneau.

1 Groupes cycliques

Définition 1. Un groupe G est dit cyclique s'il est fini et engendré par un seul élément.

Proposition 2. *Si G est cyclique de cardinal n, alors il est isomorphe au groupe $\mathbf{Z}/n\mathbf{Z}$*

Proposition 3. *Si G est de cardinal p premier, alors G est cyclique.*

Définition 4. On appelle fonction indicatrice d'Euler et on note $\varphi(n)$ le nombre d'entiers compris entre 1 et n qui sont premiers avec n.

Proposition 5. *Le groupe $\mathbf{Z}/n\mathbf{Z}$ possède $\varphi(n)$ générateurs.*

Proposition 6. *Pour tout d divisant n, le groupe $\mathbf{Z}/n\mathbf{Z}$ possède un unique sous-groupe d'ordre d, engendré par la classe de $\frac{n}{d}$.*

Remarque 7. Ce sont en fait des idéaux.

Proposition 8. *Pour tout $n \in \mathbf{N}^*$, on a $n = \sum_{d|n} \varphi(d)$.*

Théorème 9. *Soit K un corps et G un sous-groupe fini du groupe multiplicatif K^*. Alors G est cyclique.*

Exemple 10. Le groupe multiplicatif de $\mathbf{F}_p$ est cyclique, donc isomorphe à $\mathbf{Z}/(p-1)\mathbf{Z}$.

Proposition 11. *Soient $n, m \in \mathbf{N}^*$ et soit d leur PGCD. Alors il existe d morphismes entre les groupes $\mathbf{Z}/n\mathbf{Z}$ et $\mathbf{Z}/m\mathbf{Z}$. Ils sont de la forme $x[n] \mapsto ax[m]$ où a est un élément dont l'ordre dans $\mathbf{Z}/m\mathbf{Z}$ divise n et m.*

Corollaire 12. *Il y a $\varphi(n)$ automorphismes de $\mathbf{Z}/n\mathbf{Z}$. Ceux-ci sont de la forme $\overline{x} \mapsto \overline{kx}$ où k est premier avec n.*

2 Structure des groupes abéliens finis

Lemme 13. *Soit G un groupe abélien fini et soit H un sous-groupe de G. Alors tout morphisme de H dans $\mathbf{C}^*$ se prolonge en un morphisme de G dans $\mathbf{C}^*$.*

Lemme 14. *Soit G un groupe abélien fini et soit x un élément d'ordre maximal. Alors l'ordre de tout élément de G divise l'ordre de x.*

Théorème 15 (structure des groupes abéliens finis)**.** *Soit G un groupe abélien fini. Il existe des entiers $1 < d_k | \cdots | d_1$ tels que G soit isomorphe au produit $\mathbf{Z}/d_k\mathbf{Z} \times \cdots \times \mathbf{Z}/d_1\mathbf{Z}$. De plus, les entiers $d_k, \ldots, d_1$ sont uniques, on les appelles les invariants de G.*

Exemple 16. À isomorphisme près, il n'y a que 6 groupes abéliens d'ordre $600 = 2^3 \times 5^2 \times 3$. Ses invariants possibles sont : (600), (5;120), (2;300), (10;60), (2;2;150) et (2;10;30).

3 Anneaux $\mathbf{Z}/n\mathbf{Z}$

Définition 17. On note $(\mathbf{Z}/n\mathbf{Z})^*$ le groupe des éléments de $\mathbf{Z}/n\mathbf{Z}$ inversibles pour la multiplication.

Proposition 18. *Un entier est inversible modulo n si et seulement si il est premier avec n.*

Corollaire 19. *Le cardinal de* $(\mathbf{Z}/n\mathbf{Z})^*$ *vaut* $\varphi(n)$.

Proposition 20. *Les trois assertions suivantes sont équivalentes :*

1. $\mathbf{Z}/n\mathbf{Z}$ *est un anneau intègre.*
2. $\mathbf{Z}/n\mathbf{Z}$ *est un corps.*
3. n *est premier.*

Corollaire 21. *Les idéaux maximaux de* $\mathbf{Z}/n\mathbf{Z}$ *sont les* $\overline{p}(\mathbf{Z}/n\mathbf{Z})$ *où* p *est un nombre premier divisant* n.

Exemple 22.

1. **Petit théorème de Fermat :** Soient $a \in \mathbf{Z}$ et p un nombre premier, alors $a^p \equiv a \mod p$.
2. **Théorème d'Euler :** Plus généralement si $n \in \mathbf{N}^*$ et si a est premier avec n, on a $a^{\varphi(n)} \equiv 1 \mod n$.
3. **Théorème de Wilson :** Un nombre p est premier si et seulement si $(p-1)! \equiv -1 \mod p$.

Théorème 23 (lemme chinois)**.** *Soient* n *et* m *premiers entre eux. Alors les anneaux* $(\mathbf{Z}/nm\mathbf{Z})$ *et* $(\mathbf{Z}/n\mathbf{Z} \times \mathbf{Z}/m\mathbf{Z})$ *sont isomorphes.*

Remarque 24.
— La réciproque est vraie.
— Par récurrence, le résultat se généralise pour des entiers $n_1, \ldots, n_k$ premiers entre eux deux à deux.

Exemple 25. On considère le système de congruences suivant :

$$\begin{cases} x \equiv 2 \mod 4 \\ x \equiv 3 \mod 5 \\ x \equiv 1 \mod 9 \end{cases}$$

Les solutions de ce systèmes sont les $x_k = 118 + 180k$, $k \in \mathbf{Z}$.

Corollaire 26. *Soient* n *et* m *deux entiers. Soit* d *leur PGCD et soit* μ *leur PPCM. Alors les anneaux* $(\mathbf{Z}/n\mathbf{Z} \times \mathbf{Z}/m\mathbf{Z})$ *et* $(\mathbf{Z}/d\mathbf{Z} \times \mathbf{Z}/\mu\mathbf{Z})$ *sont isomorphes.*

Corollaire 27. *Soit* n *un entier, que l'on décompose en produit de facteurs premiers* $n = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$. *Alors :*

$$\varphi(n) = \prod_{i=1}^{k} \varphi\left(p_i^{\alpha_i}\right) = n \prod_{i=1}^{k} \left(1 - \frac{1}{p_i}\right)$$

4 Structure de $(\mathbf{Z}/n\mathbf{Z})^*$

Lemme 28. *Soit* p *un nombre premier impair et soit* $k \in \mathbf{N}^*$. *Alors on a* $(1+p)^{p^k} = 1 + \lambda p^{k+1}$ *avec* $\lambda \in \mathbf{N}^*$ *non divisible par* p.

Théorème 29 (structure de $(\mathbf{Z}/p^\alpha\mathbf{Z})^*$)**.** *Soit* p *un nombre premier impair et soit* α *un entier* $\geqslant 2$. *Alors les groupes* $(\mathbf{Z}/p^\alpha\mathbf{Z})^*$ *et* $\mathbf{Z}/\varphi(p^\alpha)\mathbf{Z}$ *sont isomorphes.*

Lemme 30. *Soit* $k \in \mathbf{N}^*$, *on a* $(5)^{2^k} = 1 + \lambda 2^{k+2}$ *avec* λ *impair.*

Théorème 31 (structure de $(\mathbf{Z}/2^\alpha\mathbf{Z})^*$)**.** *On a* $(\mathbf{Z}/2\mathbf{Z})^* = \{1\}$, $(\mathbf{Z}/4\mathbf{Z})^* = \{\pm 1\} \cong \mathbf{Z}/2\mathbf{Z}$. *Pour* $\alpha \geqslant 3$ *on a* $(\mathbf{Z}/2^\alpha\mathbf{Z})^* \cong \mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/2^{\alpha-2}\mathbf{Z}$.

Exemple 32. Soit G un groupe d'ordre pq avec p et q deux nombres premiers tels que $p < q$ et $p \nmid (q-1)$. Alors G est cyclique.

5 Arithmétique et théorème des deux carrés

Exemple 33. On considère l'équation diophantienne $3x^2 - 35y^2 = a$ avec a un entier compris entre 1 et 20. Cette équation n'a des solutions que pour $a \in \{3; 7; 12; 13\}$.

Proposition 34. *Soient p et q premiers distincts et soit $n = pq$. Soient e et d deux entiers tels que $ed \equiv 1 \mod \varphi(n)$. Alors pour tout $M \in \mathbf{Z}$, on a $M^{de} \equiv M \mod n$.*

Exemple 35. Principe du chiffrement RSA.

— On choisit p et q deux nombres premiers distincts et on calcule leur produit n.
— On choisit e premier avec $\varphi(n) = (p-1)(q-1)$.
— On calcule d, inverse de e modulo $\varphi(n)$.

Les nombres (n, e) sont la *clef publique* et le nombre d est la *clef privée*. Le message à envoyer est représenté par un élément M de $\mathbf{Z}/n\mathbf{Z}$. Le message chiffré est alors $C = M^e$. Pour déchiffrer le message, on utilise la proposition précédente : $C^d \equiv M \mod n$.

Théorème 36. *Soit p premier impair. Un élément $x \neq 0$ est un carré dans $\mathbf{F}_p^*$ si et seulement si $x^{\frac{p-1}{2}} = 1$.*

Définition 37. On appelle entiers de Gauss l'ensemble des nombres complexes de la forme $a + \mathrm{i}b$, avec a et b des entiers relatifs. Cet ensemble est noté $\mathbf{Z}[\mathrm{i}]$.

Proposition 38. *L'ensemble $\mathbf{Z}[\mathrm{i}]$ est un anneau euclidien pour la norme $N(z) = |z|^2$. Un élément est inversible si et seulement si il est de norme 1. Les unités de $\mathbf{Z}[\mathrm{i}]$ sont donc $1, -1, \mathrm{i}$ et $-\mathrm{i}$.*

Proposition 39. *La norme N est multiplicative. Par conséquent, l'ensemble des éléments de $\mathbf{Z}$ qui sont somme de deux carrés est stable par produit.*

Théorème 40 (théorème des deux carrés de Fermat, cas premier)**.** *Soit p un nombre premier impair. Alors p est la somme de deux carrés si et seulement si $p \equiv 1 \mod 4$.*

Théorème 41 (théorème des deux carrés de Fermat, cas général)**.** *Soit n un entier supérieur ou égal à 2, que l'on décompose en produit de facteurs premiers $n = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$. Alors n est la somme de deux carrés si et seulement si pour tout p_i congru à 3 modulo 4, on a α_i pair.*

Exemple 42. Soit p un nombre premier. Alors l'équation diophantienne $x^2 + y^2 = pz^2$ n'a pas de solutions si $p \equiv 3 \mod 4$.

Développements

1. Structure des groupes abéliens finis. **[15]**
2. Structure de $(\mathbf{Z}/p^\alpha\mathbf{Z})^*$, p premier impair. **[29]**

Références

— COMBES, *Algèbre et géométrie.*
— GOURDON, *Les maths en tête, algèbre.*
— PERRIN, *Cours d'algèbre.*
— PERRIN, *Mathématiques d'école.*
— PEYRÉ, *L'algèbre discrète de la transformée de Fourier.*