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

Pandou

23 avril 2022

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

1.1 Construction et propriétés

Définition 1. *Soit $n \geqslant 2$, on définit une relation d'équivalence sur $\mathbb{Z}$ en posant $a \equiv b \mod (n) \iff n|(a-b)$. Alors, l'ensemble $\mathbb{Z}/n\mathbb{Z}$ est le quotient $\mathbb{Z}/\equiv$.*

Théorème 2 (Division euclidienne)**.** *Soit $a, n \in \mathbb{Z}$, $b \neq 0$, alors il existe un unique couple (q, r) tel que*

$$a = nq + r \qquad et \qquad 0 \leqslant r \leqslant n-1$$

Corollaire 3. *$\{0, 1, ..., n-1\}$ forme un système de représentants de $\mathbb{Z}/n\mathbb{Z}$.*

Corollaire 4. *L'addition est compatible avec la relation $\equiv$ et donc induit une loi de groupe sur $\mathbb{Z}/n\mathbb{Z}$.*

Proposition 5. *$\mathbb{Z}/n\mathbb{Z}$ est cyclique, engendré par 1.*

Théorème 6. *Soit $n \geqslant 2$, tout groupe cyclique non trivial d'ordre n est isomorphe à $\mathbb{Z}/n\mathbb{Z}$.*

Remarque 7 : Parfois, pour insister sur la structure de groupe, on pourra préférer l'utilisation du groupe cyclique $\mathbb{U}_n = \{z \in \mathbb{C}, z^n = 1\}$.

Corollaire 8. *Tout sous-groupe d'un groupe cyclique est cyclique.*

DEVELOPPEMENT 1

Application 9 : Soit p un nombre premier impair, $n \geqslant 1$ et $q = p^n$. Alors,

$$SO_2(\mathbb{F}_q) \simeq \begin{cases} \mathbb{Z}/(q-1)\mathbb{Z} & \text{si } -1 \text{ n'est pas un carré dans } \mathbb{F}_q^* \\ \mathbb{Z}/(q+1)\mathbb{Z} & \text{sinon} \end{cases}$$

Proposition 10. *Les sous-groupes de $\mathbb{Z}/n\mathbb{Z}$ sont exactement les sous-groupes d'ordre d engendré par $\frac{n}{d}$ pour d divisant n.*

1.2 Ordre et générateurs

Proposition 11. *L'ordre de k dans $\mathbb{Z}/n\mathbb{Z}$ est $\dfrac{n}{\text{pgcd}(k,n)}$.*

Corollaire 12. *k est un générateur de $\mathbb{Z}/n\mathbb{Z}$ si, et seulement si, $k \wedge n = 1$.*

Exemple 13 : Les générateurs de $\mathbb{Z}/4\mathbb{Z}$ sont 1 et 3.

Définition 14. *On définit l'indicatrice d'Euler par* $\varphi(n) = \text{Card}\big(\{k \in [\![1, n]\!], k \wedge n = 1\}\big)$.

Proposition 15. *Soit p un nombre premier et $n \geqslant 1$, alors*

$$\varphi(p^n) = p^{n-1}(p-1)$$

Proposition 16.

$$n = \sum_{d|n} \varphi(d)$$

Corollaire 17. *Soit K un corps, alors tout sous-groupe fini de K^* est cyclique.*

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

2.1 Généralités

Proposition 18. *La multiplication sur $\mathbb{Z}$ est compatible avec la relation de congruence, donc elle induit sur $\mathbb{Z}/n\mathbb{Z}$ une structure d'anneaux.*

Remarque 19 : $n\mathbb{Z}$ est un idéal de $\mathbb{Z}$. La définition précédente de $\mathbb{Z}/n\mathbb{Z}$ coincide avec le quotient de $\mathbb{Z}$ par l'idéal $n\mathbb{Z}$.

Proposition 20 (Relation de Bézout)**.** *Soit a, b deux entiers. Alors, a et b sont premiers entre si, et seulement s'il existe $u, v \in \mathbb{Z}$ tels que $au + bv = 1$.*

Corollaire 21. *$k \in \mathbb{Z}/n\mathbb{Z}$ est inversible si, et seulement si, $k \wedge n = 1$.*

Remarque 22 : $\varphi(n)$ est donc aussi le nombre d'inversibles de $\mathbb{Z}/n\mathbb{Z}$: autrement dit, c'est l'ordre du groupe $(\mathbb{Z}/n\mathbb{Z})^\times$.

Corollaire 23 (Petit théorème de Fermat)**.** *Si $a \wedge n = 1$, alors*

$$a^{\varphi(n)} = 1 \mod (n)$$

En particulier, si p est premier et a n'est pas multiple de p, alors

$$a^{p-1} = 1 \mod (p)$$

Théorème 24 (Restes chinois)**.** *Soit $a, b \geqslant 2$ deux entiers premiers entre eux, alors le morphisme d'anneaux*

$$\mathbb{Z}/ab\mathbb{Z} \longrightarrow (\mathbb{Z}/a\mathbb{Z}) \times (\mathbb{Z}/b\mathbb{Z})$$

est un isomorphisme.
En particulier, on a

$$(\mathbb{Z}/ab\mathbb{Z})^\times \simeq (\mathbb{Z}/a\mathbb{Z})^\times \times (\mathbb{Z}/b\mathbb{Z})^\times$$

Corollaire 25. *Si a et b sont premiers entre eux, on a*

$$\varphi(ab) = \varphi(a)\varphi(b)$$

En particulier, si $n = \prod_{i=1}^{m} p_i^{\alpha_i}$ est la décomposition en facteurs premiers de n, alors

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

2.2 Le corps $\mathbb{F}_p$

Proposition 26. *$\mathbb{Z}/n\mathbb{Z}$ est un corps si, et seulement si n est premier. Dans ce cas, on notera $\mathbb{F}_p$ le corps $\mathbb{Z}/p\mathbb{Z}$.*

Proposition 27. *$(\mathbb{Z}/p\mathbb{Z})^\times$ est un groupe cyclique d'ordre $p - 1$.*

Application 28 : p est premier si, et seulement si, $(p-1)! = -1 \mod (p)$.

2.3 Automorphisme et groupe multiplicatif

Proposition 29.

$$\mathrm{Aut}(\mathbb{Z}/n\mathbb{Z}) \simeq (\mathbb{Z}/n\mathbb{Z})^\times$$

DEVELOPPEMENT 2

Lemme 30. *Si $p \geqslant 3$ est premier et $k \geqslant 1$, alors*

$$(1+p)^{p^k} = 1 + \lambda p^{k+1}$$

où $\lambda \wedge p = 1$.

Théorème 31. *Soit $p \geqslant 3$ premier et $k \geqslant 1$, alors*

$$(\mathbb{Z}/p^k\mathbb{Z})^\times \simeq \mathbb{Z}/\big(p^{k-1}(p-1)\big)\mathbb{Z}$$

Lemme 32. *Soit $k \geqslant 1$, alors*

$$5^{2^k} = 1 + \lambda 2^{k+2}$$

avec k impair.

Théorème 33. *Soit $k \geqslant 3$, alors*

$$(\mathbb{Z}/2^k\mathbb{Z})^\times \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2^{k-2}\mathbb{Z}$$

De plus, on a

$$(\mathbb{Z}/2\mathbb{Z})^\times = 1 \qquad \text{et} \qquad (\mathbb{Z}/4\mathbb{Z})^\times \simeq \mathbb{Z}/2\mathbb{Z}$$

Corollaire 34. *On en déduit en particulier que $\mathrm{Aut}(\mathbb{Z}/n\mathbb{Z})$ est cyclique si, et seulement si, $n \in \{2, 4, p^k, 2p^k\}$ avec p premier impair et $k \geqslant 1$.*

3 Quelques applications

3.1 Groupes abéliens

Définition 35. *Soit G un groupe abélien, un caractère de G est un morphisme de groupes $\chi : G \longrightarrow \mathbb{C}^\times$. Le groupe des caractères de G est le dual de G, noté $\widehat{G}$.*

Proposition 36.

$$\widehat{\mathbb{Z}/n\mathbb{Z}} \simeq \mathbb{Z}/n\mathbb{Z}$$

Lemme 37. *Soit G un groupe abélien fini et H un sous-groupe de G, alors le morphisme de groupes*

$$\rho_H : \chi \in \widehat{G} \longmapsto \chi_{|H} \in \widehat{H}$$

est surjectif.

Théorème 38 (Structure des groupes abéliens finis)**.** *Soit G un groupe abélien fini, alors il existe $d_1, ..., d_r \geqslant 1$ tels que $d_1|...|d_r$ et*

$$G \simeq \mathbb{Z}/d_1\mathbb{Z} \times ... \times \mathbb{Z}/d_r\mathbb{Z}$$

De plus, la suite $(d_1, ..., d_r)$ est unique et ne dépend que de la classe d'isomorphisme de G appelée invariants de G.

Exemple 39 : Un groupe d'ordre p^2 est toujours abélien et isomorphe à $\mathbb{Z}/p^2\mathbb{Z}$ ou à $(\mathbb{Z}/p\mathbb{Z})^2$.

Corollaire 40. *Si G est un groupe abélien fini, alors $G \simeq \widehat{G}$.*

Remarque 41 : Si G n'est pas abélien, alors le résultat précédent n'est plus nécessairement vrai, par exemple les seuls morphismes $\mathfrak{S}_n \longrightarrow \mathbb{C}^*$ sont l'identité et la signature. (Il faut en fait changer la définition de $\widehat{G}$ pour un groupe non abélien).

3.2 Arithmétique

Définition 42 (Chiffrement RSA)**.** *Soit p et q deux nombres premiers distincts et $n = pq$. Soit c et d tels que $cd = 1 \mod (\varphi(n))$. Le couple (n, c) est la clé publique et d la clé secrète. La fonction $g : t \in \mathbb{Z}/n\mathbb{Z} \longmapsto t^c$ est appelée fonction de chiffrement et la fonction $f : t \in \mathbb{Z}/n\mathbb{Z} \longmapsto t^d$ est appelée fonction clé de déchiffrement.*

Théorème 43. *Soit (n, c) une clé publique et d la clé secrète. Alors,*

$$f \circ g = \mathrm{Id}_{\mathbb{Z}/n\mathbb{Z}}$$

Interprétation 44 : Il est difficile de calculer d en ne connaissant que la clé publique (n, c). La méthode naïve consiste à factoriser n pour trouver p et q, ce qui est particulièrement difficile aujourd'hui avec p et q qui ont 150 chiffres.
Le chiffrement est public, aux yeux de tous, mais le déchiffrement n'est accessible qu'à la personne qui dispose de la clé de déchiffrement.

Définition 45. *Un nombre de Carmichael est un entier n qui n'est pas premier mais tel que $a^{n-1} = \mod (n)$ pour tout entier a.*

Remarque 46 : Les nombres de Carmichael sont les nombres qui passent à travers le critère de primalité qu'on pourrait imaginer du petit théorème de Fermat.

Théorème 47. *Un entier n est un nombre de Carmichael si, et seulement s'il existe des nombres premiers distincts $p_1, ..., p_k$ tels que $n = p_1...p_k$ tel que $\forall i, p_i - 1|n - 1$.*

Corollaire 48. *Un nombre de Carmichael a au moins 3 facteurs premiers.*

Exemple 49 : Le plus petit nombre de Carmichael est $561 = 3 \times 11 \times 17$.
On sait aussi (mais je ne sais pas le démontrer) qu'il existe une infinité de nombres de Carmichael.

3.3 Critère d'irréductibilité de polynômes

Théorème 50 (Critère d'Eisenstein)**.** *Soit $P(X) = a_nX^n + ... + a_0 \in \mathbb{Q}[X]$. On suppose qu'il existe un nombre premier p tel que*

- *p divise tous les a_i avec $i \leqslant n - 1$.*
- *p ne divise pas a_n.*
- *p^2 ne divise pas a_0.*

Alors, P est irréductible dans $\mathbb{Q}[X]$.

Exemple 51 : Soit p un nombre premier, alors $\Phi_p(X) = X^{p-1} + ... + X + 1$ est irréductible dans $\mathbb{Q}[X]$.

Théorème 52. *Soit $P = a_nX^n + ... + a_0 \in \mathbb{Z}[X]$ et p un nombre premier tel que $a_n \neq 0 \mod (p)$. Si $\overline{P}$ est irréductible dans $\mathbb{F}_p$, alors P est irréductible sur $\mathbb{Q}$.*

Application 53 : $X^p - X - 1$ est irréductible sur $\mathbb{Z}$.

Remarque 54 : La réciproque est fausse : $X^4 + 1$ est irréductible sur $\mathbb{Z}$, mais réductible dans tous les $\mathbb{F}_p$.

Références :

- Arnaudiès, Fraysse. Algèbre (Tome 1).
- Gourdon, Algèbre.
- Perrin, Cours d'algèbre.
- Risler, Algèbre pour la L3.