Leçon 120 : Anneaux Z/nZ. Applications.

1 Constructions et propriétés

1.1 Congruences

Théorème 1. *(Division euclidienne) Soient $a \in \mathbb{Z}$ et $b \in \mathbb{N}^*$, alors il existe un unique couple $(q, r) \in \mathbb{Z} \times \mathbb{N}$ tel que $a = bq + r$ avec $0 \leqslant r \leqslant b - 1$.*

Définition 2. Soit $n \in \mathbb{N}$ et $a, b \in \mathbb{Z}$. On dit que a est congru à b modulo n lorsque n divise $b - a$. On note alors $a \equiv b \mod (n)$

Proposition 3. *Cette relation de congruence modulo n est une relation d'équivalence sur $\mathbb{Z}$ et pour tout $a \in \mathbb{Z}$ on pose $\overline{a} = \{a + qn \mid q \in \mathbb{Z}\}$ sa classe d'équivalence.*

Définition 4. On pose $\mathbb{Z}/n\mathbb{Z}$ l'ensemble des classes d'équivalence modulo n. On désigne alors la surjection canonique $\pi_n : \mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$; $k \mapsto \overline{k}$.

Théorème 5. *Pour tout entier naturel non nul n, on a $\mathbb{Z}/n\mathbb{Z} = \{\overline{0}, \overline{1}, \ldots, \overline{n-1}\}$. Cet ensemble est de cardinal n et en bijection avec l'ensemble de tous les restes possibles dans la division euclidienne par n.*

Proposition 6. *Soient $a, b, c, d \in \mathbb{Z}$ tels que $a \equiv b \mod (n)$ et $c \equiv d \mod (n)$ alors $a + c \equiv b + d \mod (n)$ et $ac \equiv bd \mod (n)$.*

Théorème 7. *Pour $n \geqslant 2$, il existe une unique structure d'anneau commutatif unitaire sur $\mathbb{Z}/n\mathbb{Z}$ telle que la surjection canonique π_n soit un morphisme d'anneau.*

Théorème 8. *Pour tout $n \geqslant 2$, tous les sous groupes de $\mathbb{Z}/n\mathbb{Z}$ sont cyclique d'ordre qui divise n. Réciproquement pour tout diviseur d de n, il existe un unique sous groupe de $\mathbb{Z}/n\mathbb{Z}$ d'ordre d, c'est le groupe cyclique $H = \langle \overline{q} \rangle = \{\overline{0}, \overline{q}, \ldots, (d-1)\overline{q}\}$ avec $q = \frac{n}{d}$.*

1.2 Le groupe $(\mathbb{Z}/n\mathbb{Z})^\times$ et fonction indicatrice d'Euler

Exemple 9. Pour $n = 0$ on a $\mathbb{Z}^\times = \{-1, 1\}$ et pour $n = 1$ l'ensemble $\mathbb{Z}/\mathbb{Z} = \{\overline{0}\}$ n'est pas un anneau.

Théorème 10. *Soit $a \in \mathbb{Z}$, les propriétés suivantes sont équivalentes :*

1. *$\overline{a}$ est inversible dans $\mathbb{Z}/n\mathbb{Z}$,*
2. *a est premier avec n, $\overline{a}$ est générateur du groupe cyclique $(\mathbb{Z}/n\mathbb{Z}, +)$.*

Corollaire 11. *Ainsi les diviseurs de 0 de $\mathbb{Z}/n\mathbb{Z}$ sont les éléments ni nuls ni générateurs.*

Exemple 12. Les inversibles de $\mathbb{Z}/8\mathbb{Z}$ sont $\{\overline{1}, \overline{3}, \overline{5}, \overline{7}\}$ et les diviseurs de zéros sont $\{\overline{2}, \overline{4}, \overline{6}\}$.

Corollaire 13. *Soit G un groupe. Si G est monogène infini alors $G \cong \mathbb{Z}$. Si il est cyclique d'ordre n alors $G \cong \mathbb{Z}/n\mathbb{Z}$.*

Définition 14. On appelle fonction indicatrice d'Euler la fonction qui à tout $n \in \mathbb{N}^*$ associe le nombre $\varphi(n)$ d'entiers entre 1 et n qui sont premiers avec n.

Exemple 15. Si p premier alors $\varphi(p) = p - 1$.

Théorème 16. *(Euler) Pour tout entier $a \in \mathbb{Z}$ premier avec n on a $a^{\varphi(n)} \equiv 1 \mod (n)$.*

Théorème 17. *(Fermat) Soit p premier, pour tout $a \in \mathbb{Z}$ premier avec p on a $a^{p-1} \equiv 1 \mod (p)$.*

Théorème 18. *Pour tout entier $n \geqslant 2$ on a $n = \sum_{d|n} \varphi(d)$.*

1.3 Anneau $\mathbb{Z}/n\mathbb{Z}$

Proposition 19. *Les idéaux de $\mathbb{Z}/n\mathbb{Z}$ sont les $d\mathbb{Z}/n\mathbb{Z}$ où $d|n$ et $d \notin \{1, n\}$. De plus $(d\mathbb{Z}/n\mathbb{Z}, +) \cong (\mathbb{Z}/\frac{n}{d}\mathbb{Z}, +)$.*

Corollaire 20. *L'anneau $\mathbb{Z}/n\mathbb{Z}$ est principal.*

Proposition 21. *L'ensemble des générateurs de $\mathbb{Z}/n\mathbb{Z}$ est $(\mathbb{Z}/n\mathbb{Z})^\times$.*

1.4 Cas des $\mathbb{Z}/p\mathbb{Z}$

Théorème 22. *Les assertions suivantes sont équivalentes :*

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

Corollaire 23. *Le groupe des inversible $(\mathbb{Z}/p\mathbb{Z})^\times \cong \mathbb{Z}/(p-1)\mathbb{Z}$ est donc cyclique.*

Exemple 24. Pour n non premier c'est totalement faux, par exemple $(\mathbb{Z}/8\mathbb{Z})^\times = \{\overline{1}, \overline{3}, \overline{5}, \overline{7}\}$ n'a que 4 éléments.

Corollaire 25. *Si $p \geqslant 2$ premier et G un p-groupe opérant sur un ensemble X fini, alors $|X^G| \equiv |X| \mod p$*

Corollaire 26. *Soit G un groupe fini qui opère sur lui même par conjugaison, en notant $\Omega(x_1), \ldots, \Omega(x_r)$ toutes les orbites 2 à 2 distinctes, on a :*

$$|G| = |Z(G)| + \sum_{\substack{i=1 \\ |\Omega(x_i)|\geqslant 2}}^{r} |\Omega(x_i)| = |Z(G)| + \sum_{\substack{i=1 \\ |\Omega(x_i)|\geqslant 2}}^{r} \frac{|G|}{|Stab(x_i)|}$$

Théorème 27. *Pour tout nombre premier p, le centre d'un p-groupe n'est pas réduit à $\{1\}$.*

Théorème 28. *Tout groupe d'ordre p^2 avec p premier est commutatif. Il est isomorphe soit à $\mathbb{Z}/p^2\mathbb{Z}$ soit à $\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$.*

Proposition 29. *Soit p premier impair, si G groupe d'ordre $2p$ alors G est isomorphe soit à $\mathbb{Z}/2p\mathbb{Z}$ soit à D_{2p}.*

2 Applications

2.1 Théorème des restes chinois

Lemme 30. *Soit $(n_1, \ldots, n_r) \in \mathbb{N}$ suite d'entiers strictement plus grand que 1. Si les n_i sont 2 à 2 premiers entre eux alors leur ppcm est $\prod_{i=1}^{r} n_i$. Sinon il est strictement inférieur.*

Théorème 31. *(Chinois) Soient $n_1, \ldots, n_r \in \mathbb{N}$ strictement plus grand que 1 et n leur produit. Les entiers $n_1, \ldots, n_r$ sont premiers entre eux si et seulement si les anneaux $\mathbb{Z}/n\mathbb{Z}$ et $\prod_{j=1}^{r} \mathbb{Z}/n_j\mathbb{Z}$ sont isomorphes. Dans ce cas, l'application ψ : $\begin{cases} \mathbb{Z}/n\mathbb{Z} \to \prod_{j=1}^{r} \mathbb{Z}/n_j\mathbb{Z} \\ \pi_n(k) \mapsto (\pi_1(k), \ldots, \pi_r(k)) \end{cases}$ est un isomorphisme d'anneaux dont l'inverse est : ψ^{-1} : $\begin{cases} \prod_{j=1}^{r} \mathbb{Z}/n_j\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z} \\ (\pi_1(a_1), \ldots, \pi_r(a_r)) \mapsto \pi_n\left(\sum_{i=1}^{r} a_i u_i \frac{n}{n_i}\right) \end{cases}$ où les $(u_1, \ldots, u_r)$ sont tels que $\sum_{j=1}^{r} u_j \frac{n}{n_j} = 1$*

2.2 Équations diophantiennes

Définition 32. On appelle équation diophantienne dans $\mathbb{Z}$ une équation de la forme $ax \equiv b \mod (n)$ avec $a \in \mathbb{N}^*$ et $b \in \mathbb{Z}$.

Théorème 33. *L'équation diophantienne $ax \equiv b \mod (n)$ admet des solutions entières si et seulement $\delta = pgcd(a, n)$ divise b. Dans ce cas, en notant $a = \delta a'$, $b = \delta b'$ et $n = \delta n'$, l'ensemble des solutions est alors $S = \{b'x'_0 + kn' \mid k \in \mathbb{Z}\}$ où x'_0 est une solution de $a'x \equiv 1 \mod (n')$.*

Corollaire 34. *Pour un système d'équations diophantiennes $k \equiv a_j \mod (n_j)$ pour $1 \leqslant j \leqslant r$.. Lorsque les $n_1, \ldots, n_r$ sont deux à deux premiers entre eux, cela revient à trouver l'antécédent dans $\mathbb{Z}/n\mathbb{Z}$ de $(\pi_1(a_1), \ldots, \pi_r(a_r))$ par l'isomorphisme ψ défini dans le théorème Chinois. Cet antécédent est $\overline{k_0}$ où $k_0 = \sum_{i=1}^{r} a_i u_i m_i$. Les autres solutions sont donc les $k = k_0 + qn$ avec $q \in \mathbb{Z}$.*

Exemple 35. Les solutions du système $\begin{cases} k \equiv 2 \mod (4) \\ k \equiv 3 \mod (5) \\ k \equiv 1 \mod (9) \end{cases}$ sont les $k = 118 + 180q$ avec $q \in \mathbb{Z}$.

2.3 Polynômes cyclotomiques

Définition 36. Une racine n-ième primitive de l'unité de $\mathbb{K}$ est un élément $\zeta \in \mathbb{K}$ tel que $\zeta^n = 1$ et $\zeta^d \neq 1$ pour tout $d < n$. C'est un générateur de $\mu_n(\mathbb{K})$ de sorte qu'il y ait $\varphi(n)$ racines primitives de l'unité, leur ensemble est noté $\mu_n^*(\mathbb{K})$.

Définition 37. Le n-ième polynôme cyclotomique de $\mathbb{K}$ est $\Phi_n(X) \prod_{\zeta \in \mu_n^*(\mathbb{K})} (X - \zeta)$.

Remarque 38. Si $\zeta \in \mu_n^*(\mathbb{K})$ alors les ζ^d avec $pgcd(d, n) = 1$.
Le polynôme $\Phi_n(X)$ est unitaire de degré $\varphi(n)$.

Proposition 39. *On a* $X^n - 1 = \prod_{d|n} \Phi_d(X)$.

Proposition 40. *Dans* $\mathbb{Q}$ *on a* $\Phi_n(X) \in \mathbb{Z}[X]$.

Théorème 41. *Le polynôme cyclotomique* $\Phi_n(X)$ *est irréductible sur* $\mathbb{Z}$ *donc sur* $\mathbb{Q}$.

Dev 1 : Classification des groupes d'ordre p^2 25, 26,27 et 28
Dev 2 : Théorème des restes chinois 31 et 35
Dev 3 : Polynômes cyclotomiques irréductibles 40 et 41

Références

[BER18] Grégory BERHUY : Algèbre le grand combat. Calvage et Mounet, 2018.

[ROM17] JeanÉtienne ROMBALDI : Mathématiques pour l'Agrégation : Algèbre géométrie. De Boeck Superieur, 2017.

RAPPORT DU JURY :
Il est attendu de construire rapidement Z/nZ, puis d'en décrire les éléments inversibles, les diviseurs de zéro et les idéaux. Ensuite, le cas où l'entier n est un nombre premier doit être étudié. La fonction indicatrice d'Euler ainsi que le théorème chinois et sa réciproque sont incontournables. Il est naturel de s'intéresser à la résolution des systèmes de congruences. Les applications sont très nombreuses. Les candidates et candidats peuvent, par exemple, choisir de s'intéresser à la résolution d'équations diophantiennes (par réduction modulo n bien choisi) ou bien au cryptosystème RSA. Si des applications en sont proposées, l'étude des morphismes de groupes de Z/nZ dans Z/mZ ou le morphisme de Frobenius peuvent figurer dans la leçon.
Pour aller plus loin, les candidates et candidats peuvent poursuivre en donnant une généralisation du théorème chinois lorsque deux éléments ne sont pas premiers entre eux, s'intéresser au calcul effectif des racines carrées dans Z/nZ, au logarithme discret, ou à la transformée de Fourier rapide.