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

1. Étude de sa structure

1.1. Structure de groupes

1. Définition. Soit $n \in \mathbf{N}^*$ un entier non nul. Deux entiers $a, b \in \mathbf{Z}$ sont *congrus modulo* n si $a - b \in n\mathbf{Z}$. Dans ce cas, on note $a \equiv b \mod n$.
2. Proposition. La relation de congruence modulo n est une relation d'équivalence sur l'ensemble $\mathbf{Z}$. On note $\mathbf{Z}/n\mathbf{Z}$ l'ensemble de ses classes d'équivalences. Pour un entier $k \in \mathbf{Z}$, on note $\overline{k} \in \mathbf{Z}/n\mathbf{Z}$ sa classe d'équivalence modulo n.
3. Exemple. Modulo 2, on a $\overline{1} = \{\dots, -1, 1, 3, 5, \dots\} = 1 + 2\mathbf{Z}$.
4. Proposition. L'application

$$\left|\begin{array}{l}\mathbf{Z}/n\mathbf{Z} \times \mathbf{Z}/n\mathbf{Z} \longrightarrow \mathbf{Z}/n\mathbf{Z}, \\ \qquad (\overline{a}, \overline{b}) \longmapsto \overline{a} + \overline{b} \coloneqq \overline{a+b}\end{array}\right.$$

est bien définie et muni l'ensemble $\mathbf{Z}/n\mathbf{Z}$ d'une structure de groupe abélien.
5. Exemple. Dans le groupe $\mathbf{Z}/3\mathbf{Z}$, on a $\overline{2} + \overline{5} = \overline{7} = \overline{1}$.
6. Proposition. Un élément $\overline{k} \in \mathbf{Z}/n\mathbf{Z}$ engendre le groupe $\mathbf{Z}/n\mathbf{Z}$ si et seulement si les entiers n et k sont premiers entre eux. En particulier, le groupe $\mathbf{Z}/n\mathbf{Z}$ est cyclique.
7. Théorème. Tout groupe cyclique d'ordre n est isomorphe au groupe $\mathbf{Z}/n\mathbf{Z}$.
8. Théorème. Soit G un groupe abélien fini. Alors il existe un unique entier $s \geqslant 0$ et des uniques entiers $d_1, \dots, d_s \in \mathbf{N}^*$ tels que

$$G \simeq \mathbf{Z}/d_1\mathbf{Z} \times \cdots \times \mathbf{Z}/d_s\mathbf{Z} \qquad \text{et} \qquad d_1 \mid \cdots \mid d_s.$$

1.2. Structure d'anneaux

9. Proposition. L'application

$$\left|\begin{array}{l}\mathbf{Z}/n\mathbf{Z} \times \mathbf{Z}/n\mathbf{Z} \longrightarrow \mathbf{Z}/n\mathbf{Z}, \\ \qquad (\overline{a}, \overline{b}) \longmapsto \overline{a} \times \overline{b} \coloneqq \overline{a \times b}\end{array}\right.$$

est bien définie et muni l'ensemble $\mathbf{Z}/n\mathbf{Z}$ d'anneaux commutatif unitaire.
10. Exemple. Modulo 7, on a $\overline{2} \times \overline{5} = \overline{10} = \overline{3}$.
11. Proposition. Les idéaux de l'anneau $\mathbf{Z}/n\mathbf{Z}$ sont de la forme $d\mathbf{Z}/n\mathbf{Z}$ avec $d \mid n$.
12. Proposition. Un élément $\overline{k} \in \mathbf{Z}/n\mathbf{Z}$ est inversible si et seulement si les entiers n et k sont premiers entre eux.
13. Corollaire. Les points suivants sont équivalents :
- l'anneau $\mathbf{Z}/n\mathbf{Z}$ est un corps ;
- il est intègre ;
- l'entier n est premier.

14. Notation. Pour un nombre premier p, on note le corps $\mathbf{F}_p \coloneqq \mathbf{Z}/p\mathbf{Z}$ à p éléments.
15. Proposition. On a $\mathrm{Aut}(\mathbf{Z}/n\mathbf{Z}) \simeq (\mathbf{Z}/n\mathbf{Z})^\times$.
16. Proposition. Pour tout nombre premier p, on a $(\mathbf{Z}/p\mathbf{Z})^\times \simeq \mathbf{Z}/(p-1)\mathbf{Z}$.
17. Définition. La *fonction indicatrice d'Euler* est l'application

$$\varphi\colon \left|\begin{array}{l}\mathbf{N}^* \longrightarrow \mathbf{N}^*, \\ \quad n \longmapsto |(\mathbf{Z}/n\mathbf{Z})^\times| = |\{k \in [\![0, n-1]\!] \mid n \wedge k = 1\}|.\end{array}\right.$$

18. Proposition. On a

$$n = \sum_{d \mid n} \varphi(d).$$

19. Proposition. Soit $a \in \mathbf{Z}^*$ un entier premier avec l'entier n. Alors

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

20. Proposition. Pour tout nombre premier p et tout entier $\alpha \in \mathbf{N}^*$, on a

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

En particulier, pour tout entier $a \in \mathbf{Z}^*$ qui n'est pas divisible par le nombre p, on a

$$a^{p-1} \equiv 1 \mod p.$$

21. Théorème *(Wilson)*. Un entier $p \geqslant 2$ est premier si et seulement si

$$(p-1)! \equiv -1 \mod p.$$

2. Applications à l'arithmétique

2.1. Équations diophantiennes et théorème des restes chinois

22. Théorème. Soient $a, b, n \in \mathbf{Z}$ trois entiers avec $n \neq 0$. Alors l'équation

$$ax \equiv b \mod n$$

admet des solutions si et seulement si $d \coloneqq \mathrm{pgcd}(a, n) \mid b$. Dans ce cas, les solutions sont de la forme $x_0 + n/d \times k$ avec $k \in \mathbf{Z}$ pour une solution particulière $x_0 \in \mathbf{Z}$.
23. Exemple. L'équation $3x \equiv 2 \mod 6$ admet des solutions.
24. Théorème *(Germain)*. Soit $p \geqslant 3$ un nombre premier tel que le nombre $2p+1$ soit premier. Alors il n'existe pas de triplet $(x, y, z) \in \mathbf{Z}^3$ tel que

$$xyz \not\equiv 0 \mod p \qquad \text{et} \qquad x^p + y^p + z^p = 0.$$

25. Théorème *(des restes chinois)*. Soient A un anneau unitaire et $I_1, \dots, I_n \subset A$ des idéaux deux à deux étrangers ($I_i + I_j = A$ si $i \neq j$). Alors l'application

$$\left|\begin{array}{l}A \longrightarrow A/I_1 \times \cdots \times A/I_n, \\ x \longmapsto (x \mod I_1, \dots, x \mod I_n)\end{array}\right.$$

est un morphisme d'anneaux surjectif de noyau $I_1 \cap \cdots \cap I_n = I_1 \cdots I_n$. En particulier, il induit un isomorphisme d'anneaux

$$A/I_1 \cdots I_n \longrightarrow A/I_1 \times \cdots \times A/I_n.$$

26. Corollaire *(des restes chinois dans $\mathbf{Z}$)*. Soient $m_1, \dots, m_n \in \mathbf{N}^*$ des entiers deux à deux premiers entre eux et $v_1, \dots, v_n \in \mathbf{Z}$ d'autres entiers. Alors il existe une unique solution $x \in [\![0, m_1 \cdots m_n - 1]\!]$ du système

$$\forall i \in [\![1, r]\!], \qquad x \equiv v_i \mod m_i. \tag{1}$$

27. Proposition *(interpolation de Lagrange)*. En reprenant les notations précédentes, pour tout indice $i \in [\![1, r]\!]$, il existe un entier $N_i \in [\![0, m_i - 1]\!]$ tel que $N_i M_i \equiv 1$

mod m_i avec $M_i = m_1 \cdots m_r/m_i$. Alors l'unique solution du système (1) est l'entier

$$\sum_{i=1}^{n} v_i N_i M_i.$$

28. Exemple. On souhaite résoudre le système

$$\begin{cases} x \equiv 0 & \mod 2, \\ x \equiv 2 & \mod 3, \\ x \equiv -2 & \mod 7. \end{cases}$$

On calcul d'abord $M \coloneqq 2 \times 3 \times 7 = 42$. Les entiers 2, 3 et 7 étant premiers, ce système admet une unique solution dans l'intervalle $[\![0, 41]\!]$.

- L'élément $M_1 \coloneqq M/2 = 21 \equiv 1$ est d'inverse $N_1 = 1$ dans $\mathbf{Z}/2\mathbf{Z}$.
- L'élément $M_2 \coloneqq M/3 = 14 \equiv -1$ est d'inverse $N_2 = -1$ dans $\mathbf{Z}/3\mathbf{Z}$.
- L'élément $M_3 \coloneqq M/7 = 6 \equiv -1$ est d'inverse $N_2 = -1$ dans $\mathbf{Z}/7\mathbf{Z}$.

Finalement, l'unique solution est $0 \times 21 \times 1 + 2 \times 14 \times (-1) - 2 \times 6 \times (-1) = -16$.

29. Corollaire. Soient $m, n \in \mathbf{N}^*$ deux entiers premiers entre eux. Alors il existe un isomorphisme

$$(\mathbf{Z}/mn\mathbf{Z})^\times \simeq (\mathbf{Z}/m\mathbf{Z})^\times \times (\mathbf{Z}/n\mathbf{Z})^\times.$$

En particulier, on peut écrire $\varphi(mn) = \varphi(m)\varphi(n)$.

30. Proposition. Soit $n \geqslant 2$ un entier et $n = p_1^{\alpha_1} \dots p_k^{\alpha_k}$ sa décomposition en facteurs premiers. Alors

$$\varphi(n) = p_1^{\alpha_1 - 1} \cdots p_1^{\alpha_k - 1}(p_1 - 1) \cdots (p_k - 1).$$

2.2. Carrés dans les corps finis

31. Définition. Un élément x d'un corps K est un *carré* s'il existe un élément $y \in K$ tel que $x = y^2$. On note $K^2 \subset K$ l'ensemble des carrés et on pose $K^{\times 2} \coloneqq K^2 \cap K^\times$.

32. Proposition. Soit q une puissance d'un nombre premier p.

- Si $p = 2$, alors $\mathbf{F}_q^{\times 2} = \mathbf{F}_q$.
- Si $p > 2$, alors $|\mathbf{F}_q^2| = (q+1)/2$ et $|\mathbf{F}_q^{\times 2}| = (q-1)/2$.

33. Exemple. Les carrés dans $\mathbf{F}_9$ sont 0, 1, 4, 9 et 7.

34. Proposition. On suppose que $p > 2$. Pour $x \in \mathbf{F}_q$, on a

$$x \in \mathbf{F}_q^{\times 2} \iff x^{(q-1)/2} = 1.$$

35. Exemple. L'élément 2 est un carré dans $\mathbf{F}_7$ puisque $2^{(7-1)/2} = 2^3 = 1$, mais les éléments -1 et 3 n'en sont pas.

36. Définition. Soient p un nombre premier impair. Pour tout élément $a \in \mathbf{F}_p^\times$, son *symbole de Legendre* est l'entier

$$\left(\frac{a}{p}\right) \coloneqq a^{(p-1)/2} = \begin{cases} 1 & \text{si } a \in \mathbf{F}_p^{\times 2}, \\ -1 & \text{si } a \in \mathbf{F}_p^\times \setminus \mathbf{F}_p^{\times 2}. \end{cases}$$

37. Exemple. En reprenant l'exemple précédent, on a $(\frac{2}{7}) = 1$ et $(\frac{-1}{7}) = (\frac{3}{7}) = -1$.

38. Lemme. Pour tout élément $a \in \mathbf{F}_p^\times$, on a

$$|\{x \in \mathbf{F}_p \mid ax^2 = 1\}| = 1 + \left(\frac{a}{p}\right).$$

39. Théorème *(loi de réciprocité quadratique)*. Soient p et q deux nombres premiers impairs. Alors

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{(p-1)/2 \times (q-1)/2}.$$

40. Proposition *(lois spéciales)*. Pour tout nombre premier impair, on a

$$\left(\frac{-1}{p}\right) = (-1)^{(p-1)/2} \qquad \text{et} \qquad \left(\frac{2}{p}\right) = (-1)^{(p^2-1)/8}.$$

Autrement dit,

- l'entier -1 est un carré modulo p si et seulement si $p \equiv 1 \mod 4$;
- l'entier 2 est un carré modulo p si et seulement si $p \equiv \pm 1 \mod 8$;

41. Théorème. L'application $a \in \mathbf{F}_p^\times \longmapsto (\frac{a}{p}) \in \{\pm 1\}$ est un morphisme de groupes.

42. Exemple. Avec les trois derniers points, on trouve

$$\left(\frac{14}{23}\right) = \left(\frac{2}{23}\right)\left(\frac{7}{23}\right) = \left(\frac{7}{23}\right) = -\left(\frac{23}{7}\right) = -\left(\frac{2}{7}\right) = -1.$$

Par conséquent, l'entier 14 n'est pas un carré modulo 23, c'est-à-dire l'équation $x^2 = 14$ dans $\mathbf{Z}/23\mathbf{Z}$ n'admet pas de solution.

3. Polynôme irréductibles et réduction

3.1. Critères d'irréductibilité

43. Théorème *(critère d'Eisenstein)*. Soit $P \coloneqq a_n X^n + \cdots + a_0 \in \mathbf{Z}[X]$ un polynôme à coefficients entiers. Soit p un nombre premier tel que

- $p \nmid a_n$;
- $p \mid a_i$ pour $i \in [\![0, n-1]\!]$;
- $p^2 \nmid a_0$.

Alors le polynôme P est irréductible dans $\mathbf{Q}[X]$. En particulier, s'il est primitif, alors il est irréductible dans $\mathbf{Z}[X]$.

44. Exemple. Le polynôme $X^n - 2$ est irréductible dans $\mathbf{Z}[X]$ en appliquant le critère avec $p = 2$.

45. Théorème. Soit $P \coloneqq a_n X^n + \cdots + a_0 \in \mathbf{Z}[X]$ un polynôme à coefficients entiers. On suppose que $p \nmid a_n$ et que le polynôme $\overline{P}$ est irréductible dans $\mathbf{F}_p[X]$. Alors le polynôme P est irréductible dans $\mathbf{Q}[X]$.

46. Exemple. Le polynôme $X^3 + 462X^2 + 2433X - 6791$ est irréductible sur $\mathbf{Z}$ puisque sa projection $X^3 + X - 1$ dans $\mathbf{F}_2[X]$ est irréductible dans $\mathbf{F}_2[X]$.

3.2. Polynômes cyclotomiques

47. Notation. On considère un corps K de caractéristique $p \geqslant 0$ et un entier $n > 0$. On suppose que $p \nmid n$.

48. Définition. Une *racine n-ième de l'unité* est un élément $\xi \in K$ tel que $\xi^n = 1$. Elle est *primitive* si $\xi^d \neq 1$ pour $d < n$. On note $\mu_n(K)$ (resp. $\mu_n^\times(K)$) les ensembles de racines n-ième (resp. primitives).

49. Définition. Soit K_n un corps de décomposition du polynôme $X^n - 1$ sur K. Le

n-ième polynôme cyclotomique est le polynôme

$$\Phi_{n,K} \coloneqq \prod_{\xi \in \mu_n^\times(K_n)} (X - \xi) \in K_n[X].$$

50. Remarque. Le polynôme $\Phi_{n,K}$ est unitaire de degré $\varphi(n) = |(\mathbf{Z}/n\mathbf{Z})^\times|$.

51. Proposition. On a

$$X^n - 1 = \prod_{d|n} \Phi_{d,K}.$$

52. Exemple. On peut calculer $\Phi_{1,\mathbf{Q}} = X - 1$, $\Phi_{2,\mathbf{Q}} = X + 1$ et $\Phi_{3,\mathbf{Q}} = X^2 + X + 1$.

53. Proposition. On a $\Phi_n \coloneqq \Phi_{n,\mathbf{Q}} \in \mathbf{Z}[X]$. Soit $\sigma\colon \mathbf{Z} \longrightarrow K$ l'unique morphisme d'anneaux que l'on étend en un morphisme d'anneaux $\sigma\colon \mathbf{Z}[X] \longrightarrow K[X]$ en envoyant l'indéterminée X sur elle-même. Alors $\Phi_{n,K} = \sigma(\Phi_{n,\mathbf{Q}})$.

54. Remarque. On particulier, le polynôme $\Phi_{n,\mathbf{F}_p}$ s'obtient en réduisant modulo p le polynôme $\Phi_{n,\mathbf{Q}}$.

55. Théorème. Le polynôme $\Phi_n \coloneqq \Phi_{n,\mathbf{Q}}$ est irréductible sur $\mathbf{Z}$ et donc sur $\mathbf{Q}$.

56. Corollaire. Soit $\xi \in \mu_n^\times(\mathbf{C})$. Alors son polynôme minimal sur $\mathbf{Q}$ est le polynôme Φ_n. En particulier, on a $[\mathbf{Q}(\zeta) : \mathbf{Q}] = \varphi(n)$.

— D2 —

[1] Josette Calais. *Éléments de théorie des groupes*. 3e édition. Presses Universitaires de France, 1998.
[2] Serge Francinou, Hervé Gianella et Serge Nicolas. *Algèbre 1*. Cassini, 2001.
[3] Xavier Gourdon. *Algèbre*. 2e édition. Ellipses, 2009.
[4] Daniel Perrin. *Cours d'algèbre*. Ellipses, 1996.