Leçon 120 : Anneaux Z/nZ. Applications.

RM
2022-2023

Soit $n \in \mathbb{N}^*$.

1 Structure de Z/nZ

1.1 Construction de l'anneau Z/nZ

Proposition 1 : Tout sous groupe (ou idéals) de $(\mathbb{Z}, +)$ est de la forme $m\mathbb{Z}$ ou $m \in \mathbb{N}$.

Définition 2 : Soient n un entier naturel et a, b deux entiers relatifs. On dit que a est congrus à b modulo n si n divise $b - a$. On note alors $a \equiv b \pmod{n}$.

Proposition 3 : On peut alors définir une relation d'équivalence sur $\mathbb{Z}$. L'ensemble des classes d'équivalences modulo n est noté $\mathbb{Z}/n\mathbb{Z}$. On note π_n la surjection canonique de $\mathbb{Z}$ sur $\mathbb{Z}/n\mathbb{Z}$.

Théorème 4 : On a $\mathbb{Z}/n\mathbb{Z} = \{\overline{0}, \overline{1}, ..., \overline{n-1}\}$ qui est un ensemble de cardinal n avec pour représentant des classes d'équivalences les entier $0, 1, ..., n-1$.

Théorème 5 : Pour $n \geq 2$, il existe une unique structure d'anneaux commutatif unitaire sur $\mathbb{Z}/n\mathbb{Z}$ telle que la surjection canonique π_n soit un morphisme d'anneaux.

Remarque 6 : Dans la pratique, ce théorème est fondamentale. Cela nous permet de dire que $\overline{a+b} = \overline{a} + \overline{b}$ et $\overline{ab} = \overline{a}\overline{b}$.

1.2 Le groupe (Z/nZ,+)

Définition 7 : On dit que G est monogène s'il existe un élément g de G tel que $G =< g >$. Si de plus G est fini, on dit alors qu'il est cyclique.

Exemple 8 : le groupe $(\mathbb{Z}, +)$ est monogène engendré par 1 et le groupe $\mathbb{Z}/n\mathbb{Z}$ est cyclique d'ordre n engendré par $\overline{1}$.

Théorème 9 : Tout groupe cyclique d'ordre n est isomorphe à $(\mathbb{Z}/n\mathbb{Z}, +)$.

Exemple 10 : Le groupe multiplicatif $\mathbb{U}_n$ des racines n-ièmes de l'unité est cyclique d'ordre n, isomorphe à $\mathbb{Z}/n\mathbb{Z}$ par l'application $\overline{k} \mapsto e^{\frac{2ik\pi}{n}}$.

Théorème 11 : Pour $n \geq 2$, tous les sous-groupes de $\mathbb{Z}/n\mathbb{Z}$ sont cycliques 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 $H =< \overline{q} >$ où $q = n/d$. Ce sous groupe est aussi l'ensemble des éléments de G dont l'ordre divise d et ses générateurs sont tous les éléments d'ordre d de $\mathbb{Z}/n\mathbb{Z}$.

Proposition 12 : Les générateurs de $\mathbb{Z}/n\mathbb{Z}$ sont les nombres $\overline{k}$ tels que k soit premier avec n.
Exemple 13 : Dans $\mathbb{Z}/8\mathbb{Z}$, les générateurs du groupe sont alors $\overline{1}, \overline{3}, \overline{5}, \overline{7}$.

1.3 Le groupe multiplicatif

Définition 14 : Pour $n \geq 2$, on note $(\mathbb{Z}/n\mathbb{Z})^\times$ le groupe multiplicatif des éléments inversibles de $\mathbb{Z}/n\mathbb{Z}$.

Définition 15 : On appelle fonction indicatrice d'Euler la fonction qui associe a tout entier naturel non nul n, le nombre $\varphi(n)$ d'entiers compris entre 1 et n qui sont premiers à n (avec $\varphi(1) = 1$).

Exemple 16 : Si $p \geq 2$ est un nombre premier, on a $\varphi(p) = p - 1$.

Théorème 17 : Soit a un entier relatif. Les propriétés suivantes sont équivalentes :
1) $\overline{a}$ est inversible dans $\mathbb{Z}/n\mathbb{Z}$.
2) a est premier avec n.
3) $\overline{a}$ est un générateur du groupe cyclique $(\mathbb{Z}/n\mathbb{Z}, +)$.

Remarque 18 : On en déduit que $\varphi(n)$ est le nombre de générateurs du groupe cyclique $(\mathbb{Z}/n\mathbb{Z}, +)$ ou encore le nombre d'éléments inversibles de $\mathbb{Z}/n\mathbb{Z}$.

Théorème 19 : Si $d|n$, on a alors $\varphi(d)$ éléments d'ordre d dans $\mathbb{Z}/n\mathbb{Z}$.

Corollaire 20 : On a alors pour $n \geq 2$ que $n = \sum_{d|n} \varphi(d)$.

1.4 Théorème chinois

Remarque 21 : Le théorème chinois nous permet alors de résoudre certains systèmes de congruences. Il nous garantit alors une de l'existence d'une solution et même son unicité dans $\mathbb{Z}/n\mathbb{Z}$. On alors que toutes solutions sont de la $x_0 + kn$ ou x_0 est une solution particulière.

Exemple 22 : On considère le système suivant

$$\begin{cases} k \equiv 2 \pmod{4} \\ k \equiv 3 \pmod{5} \\ k \equiv 1 \pmod{9} \end{cases}.$$

On a alors comme solution $k = 118 + 180q$ ou $q \in \mathbb{Z}$.

Remarque 23 : Dans la pratique, pour trouver la solution de ce système, on pose $x = x_1 + 4x_2 + x_320$ et on cherche x_1, x_2, x_3 pour avoir une solution particulière.

Théorème (Chinois) 24 : Soient $(n_j)_{1\leq j\leq r}$ une suite de $r \geq 2$ entiers naturels distincts de 0 et 1, et $n = \prod_{j=1}^{r} n_j$. Les entiers $n_1, .., n_r$ sont deux à deux 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

$$\begin{array}{rccc} \psi : & \mathbb{Z}/n\mathbb{Z} & \to & \prod_{j=1}^{r} \mathbb{Z}/n_j\mathbb{Z} \\ & \pi_n(k) & \mapsto & (\pi_1(k), ..., \pi_r(k)) \end{array} .$$

est un isomorphisme.

Dev 1

Application (Calcul de $\varphi(n)$) 25 : Si $n \geq 2$ a pour décomposition en facteurs premiers $n = \prod_{i=1}^{r} p_i^{\alpha_i}$ avec $2 \leq p_1 < ... < p_r$ premiers et les α_i entiers naturels non nuls, on a alors :

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

Remarque 26 : On dispose même de l'application inverse de ψ, qui est

$$\begin{array}{rccc} \psi^{-1} : & \prod_{j=1}^{r} \mathbb{Z}/n_j\mathbb{Z} & \to & \mathbb{Z}/n\mathbb{Z} \\ & (\pi_1(a_1), ..., \pi_r(a_r)) & \mapsto & \pi_n\left(\sum_{i=1}^{r} a_i u_i \frac{n}{n_i}\right) \end{array} .$$

2 Arithmétique dans Z

2.1 Test de primalité

Théorème (d'Euler) 27 : Pour tout entier relatif a premier avec n, on a $a^{\varphi(n)} \equiv 1 \pmod{n}$.

Théorème (Fermat) 28 : Soit p un entier naturel premier. Pour tout entier relatif a premier avec p, on a $a^{p-1} \equiv 1 \pmod{p}$ et pour tout entier relatif a, on a $a^p \equiv a \pmod{p}$.

Théorème (Wilson) 29 : Un entier $p \geq 2$ est un nombre premier si et seulement si $(p-1)! \equiv -1 \pmod{p}$.

Remarque 30 : C'est un résultat théorique, car dans la pratique, le calcul est tellement couteux en temps que l'on ne peut pas l'utiliser pour déterminer si un grands nombre est premier ou pas.

Application (Chiffrement RSA) 31 : Ce chiffrement permet l'échange un échange de message sécuriser. Un utilisateur choisis 2 nombres premiers assez grand p, q et on pose $n = pq$. On a alors $\varphi(n) = (p-1)(q-1)$ et on choisit un entier relatif e premier avec $\varphi(n)$ de sorte qu'il existe $d \in \mathbb{Z}$ tel que $ed \equiv 1 \pmod{\varphi(n)}$.
L'utilisateur envoie alors la clé publique (n, e), et le gens peuvent encoder leur message $m \in \mathbb{Z}$ en envoyant $M \equiv m^e \pmod{n}$. L'utilisateur décode alors le message en calculant $M^d \equiv$ qui vérifie $M^d \equiv m^{ed} \equiv m \pmod{n}$ et retrouve le message d'origine. La sécurité de RSA vient qu'il est très difficile de trouver d sans connaitre p et q, et ils sont eux même difficile à trouver car il est difficile de factoriser n.

Définition 32 : Un entier $n \geq 2$ est appelé nombre de Carmichael si n n'est pas premier et $\forall a \in \mathbb{Z}, a^n \equiv a \pmod{n}$.

Remarque 33 : L'idée est ici d'étudier les nombres qui vérifie le critère de Fermat sans être premier.

Exemple 34 : 561 est le plus petit nombre de Carmichael

2.2 Équation de Fermat

On s'intéresse à l'équation de Fermat $x^n = y^n + z^n$.

Développement 35 : Soit p un nombre premier de Sophie Germain, c'est-à-dire un nombre premier impair tel que $q = 2p+1$ soit premier. Alors il n'existe pas de triplet $(x, y, z) \in \mathbb{Z}^3$ tel que $xyz \not\equiv 0[p]$ et $x^p + y^p + z^p = 0$.

Dev 2

Théorème (de Fermat) 36 : Il n'existe pas de nombre entiers strictement positifs x, y, z solution de l'équation de Fermat pour $n > 2$.

3 Application à l'irréductibilité des polynômes

3.1 Irréductibilité et construction des corps finis

Définition 37 : Un polynôme $P \in \mathbb{K}[X]$ non nulle est dit irréductible s'il est non constant et n'est divisible que par les constantes non nulles ou les polynômes λP avec $\lambda \in \mathbb{K}^*$.

Exemple 38 : • Un polynôme de degré 1 est irréductible. Si le corps $\mathbb{K}$ est algébriquement clos, les polynômes de degré 1 sont alors les seuls polynômes irréductibles.

• Un polynôme de degré 2 est réductible dans $\mathbb{K}[X]$ si et seulement si il admet une racine double ou deux racines simples dans $\mathbb{K}$.

• $P(X) = X^2 - 2$ est réductible dans $\mathbb{R}[X]$ mais pas sur $\mathbb{Q}[X]$.

• Un polynôme de degré $1, 2, 3$ est réductible dans $\mathbb{K}[X]$ si et seulement si il admet au moins une racine dans $\mathbb{K}$.

Théorème 39 : On a que $\mathbb{K}[X]/(P)$ est un corps si et seulement si le polynôme P est irréductible.

Exemple 40 : On a que $\mathbb{R}[X]/(X^2+1)$ est un corps, qui est isomorphe à $\mathbb{C}$.

Définition 41 : On note $\mathcal{U}_n(p)$ l'ensemble de tous les polynômes unitaires irréductibles de degré n dans $\mathbb{F}_p[X]$ et $I_n(p)$ le cardinal de $\mathcal{U}_n(p)$. On pose le polynôme $P_n(X) = X^{p^n} - X \in \mathbb{F}_p[X]$.

Exemple 42 : Comme tous les polynômes $P(X) = X - \lambda$ sont irréductible pour $\lambda \in \mathbb{F}_p$, on a $I_1(p) = p$.

Remarque 43 : Si $P \in \mathcal{U}_n(p)$, on a donc que $\mathbb{F}_p[X]/(P)$ est un corps fini de cardinal p^n. On peut le voir comme une extension de corps de $\mathbb{F}_p$ de degré n avec comme base $(\overline{X}^k)_{0 \leq k \leq n-1}$.
De cette manière, on peut associer l'existence de corps finis à l'existence de polynômes irréductibles.

Lemme 44 : Tout diviseur irréductible de P_n dans $\mathbb{F}_p[X]$ est de degré divisant n. Réciproquement, pour tout diviseur d de n, tout polynôme $P \in \mathcal{U}_d(p)$ divise P_n.

Théorème 45 : Le polynôme P_n est sans facteur carré dans $\mathbb{F}_p[X]$ et on a la décomposition en facteur irréductible, $P_n(X) = X^{p^n} - X = \prod_{d|n} \prod P \in \mathcal{U}_d(p) P$.

Remarque 46 : On peut alors compter le nombre de polynôme irréductible dans $\mathbb{F}_p[X]$. Par exemple, le nombre de polynômes irréductible de degré 2 dans $\mathbb{F}_2[X]$ est de 1, et c'est $X^2 + X + 1$.

Développement 47 : Pour tout entier naturel non nul n, on a $nI_n(p) = \sum_{d|n} \mu(d) p^{n/d}$.

Corollaire 48 : Il existe des polynômes irréductibles de degré n dans $\mathbb{F}_p[X]$.

Théorème 49 : A un isomorphisme près, il n'existe qu'un seul corps à p^n éléments, c'est le corps $\mathbb{F}_{p^n} = \mathbb{F}_p[X]/(P)$ où $P \in \mathcal{U}_n(p)$.

3.2 Polynôme cyclotomique

Définition 50 : Soit $\mathbb{K}$ un corps et $n \in \mathbb{N}^*$. On pose $\mu_n(\mathbb{K}) = \{\zeta \in \mathbb{K} | \zeta^n = 1\}$ l'ensemble des racines n-èmes de l'unité et $K_n = D_{\mathbb{K}}(X^n - 1)$. On pose de plus $\mu_n^*(\mathbb{K}_n) = \{\zeta \in \mathbb{K}_n | \zeta^n = 1 \text{ et } \zeta^d \neq 1 \text{ pour } d < n\}$ l'ensemble des racines primitives n-èmes de l'unité.

Proposition 51 : On a $|\mu_n^*(\mathbb{K}_n)| = \varphi(n)$ et si $\zeta \in \mu_n^*(\mathbb{K}_n)$, alors ζ^m l'est aussi si et seulement si $m \wedge n = 1$.

Définition 52 : On définit le n-ème polynôme cyclotomique $\Phi_{n,\mathbb{K}} \in \mathbb{K}_n[X]$ est donné par la formule :

$$\Phi_{n,\mathbb{K}}(X) = \prod_{\zeta \in \mu_n^*(\mathbb{K}_n)} (X - \zeta).$$

Remarque 53 : Sur $\mathbb{Q}$, comme le corps de décomposition de $X^n - 1$ est $\mathbb{C}$, on a les racines n-èmes de l'unité "classiques".

Proposition 54 : On a que $X^n - 1 = \prod_{d|n} \Phi_d(X)$.

Exemple 55 : On a $\Phi_1(X) = X - 1$, $Phi_2(X) = X + 1$, $\Phi_3(X) = X^2 + X + 1$, $\Phi_p(X) = X^{p-1} + ... + X + 1$ pour p premier.

Proposition 56 : On a $\Phi_{n,\mathbb{Q}}(X) \in \mathbb{Z}[X]$.

Développement 57 : $\Phi_n(X)$ est irréductible sur $\mathbb{Z}[X]$ (et donc dans $\mathbb{Q}[X]$).

Application 58 : Soit K une extension finie de $\mathbb{Q}$. Il y a alors un nombre fini de racines de l'unité dans $\mathbb{K}$.

Corollaire 59 : Si ζ est une racine primitive n-ème de l'unité dans un corps de caractéristique nulle, alors son polynôme minimal sur $\mathbb{Q}$ est Φ_n, et donc on a $[\mathbb{Q}(\zeta) : \mathbb{Q}] = \varphi(n)$.

Références :

1. Algèbre Gourdon
2. Algèbre et géométrie Rombaldi
3. Cours d'algèbre Perrin