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

120

Contexte : n désigne un entier naturel ≥ 2.

I - Structure de l'anneau $(\mathbb{Z}/n\mathbb{Z}, +, \cdot)$

def 1 : Soit $x, y \in \mathbb{Z}$. On dit que x est congru à y modulo n si $x - y$ est divisible par n. On note $x = y \bmod n$.

prop-def 2 : La relation de congruence est une relation d'équivalence. On note $\mathbb{Z}/n\mathbb{Z}$ l'ensemble des classes d'équivalences, et $\pi : \mathbb{Z} \twoheadrightarrow \mathbb{Z}/n\mathbb{Z}$ la projection canonique. On notera $\pi(x) = \bar{x}$ $\quad x \longmapsto x \bmod n$

ex 3 : $\mathbb{Z}/2\mathbb{Z} = \{0 \bmod 2 ; 1 \bmod 2\}$, constitué d'une classe d'entiers pairs, et une autre d'impairs.

def 4 : On définit l'addition et la multiplication sur $\mathbb{Z}/n\mathbb{Z}$ par :

$$+ : \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z} \longrightarrow \mathbb{Z}/n\mathbb{Z}, \quad (x \bmod n, y \bmod n) \longmapsto (x+y) \bmod n$$

$$\cdot : \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z} \longrightarrow \mathbb{Z}/n\mathbb{Z}, \quad (x \bmod n, y \bmod n) \longmapsto xy \bmod n$$

prop 5 : Muni de ces deux opérations $(\mathbb{Z}/n\mathbb{Z}, +, \cdot)$ est un anneau commutatif, unitaire à n éléments.

prop 6 : Les idéaux de $\mathbb{Z}/n\mathbb{Z}$ sont de la forme $\overline{\alpha}.\mathbb{Z}/n\mathbb{Z}$; avec $\overline{\alpha} \in \mathbb{Z}/n\mathbb{Z}$

prop 7 : Les propriétés suivantes sont équivalentes :
(1) p est premier.
(2) $(\mathbb{Z}/p\mathbb{Z}, +, \cdot)$ est un corps.
(3) $(\mathbb{Z}/p\mathbb{Z}, +, \cdot)$ est intègre.

app 8 : $(\mathbb{Z}/n\mathbb{Z}, +, \cdot)$ n'est pas un anneau principal.

prop 9 : Les morphismes d'anneaux de $\mathbb{Z}/m\mathbb{Z}$ vers $\mathbb{Z}/n\mathbb{Z}$ sont exactement de la forme $f : \mathbb{Z}/m\mathbb{Z} \longrightarrow \mathbb{Z}/n\mathbb{Z}$, $x \bmod m \longmapsto x \bmod n$ où $n \mid m$

th 10 : [Lemme Chinois]
Soient $n, m \geq 2$ deux entiers premiers entre eux. L'application $\varphi : \mathbb{Z}/mn\mathbb{Z} \longrightarrow \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$, $x \bmod mn \longmapsto (x \bmod m, x \bmod n)$ est un isomorphisme d'anneaux.

Cor 11 : Avec les mêmes hypothèses, f induit un isomorphisme de groupe $\tilde{f} : (\mathbb{Z}/mn\mathbb{Z})^\times \longrightarrow (\mathbb{Z}/m\mathbb{Z})^\times \times (\mathbb{Z}/n\mathbb{Z})^\times$, $x \bmod mn \longmapsto f(x \bmod mn)$

app 12 : Soit $n = p_1^{\alpha_1} \cdots p_r^{\alpha_r}$ une décomposition en produit de facteurs premiers, avec $\alpha_i \geq 1$ pour tout i.

$$\hat{f} : \mathbb{Z}/n\mathbb{Z} \longrightarrow \mathbb{Z}/p_1^{\alpha_1}\mathbb{Z} \times \cdots \times \mathbb{Z}/p_r^{\alpha_r}\mathbb{Z}$$
$$x \bmod n \longmapsto (x \bmod p_1^{\alpha_1}, \ldots, x \bmod p_r^{\alpha_r})$$

est un isomorphisme d'anneaux.

app 13 : [Cryptographie RSA]
Soient p, q deux nombres premiers distincts. On pose $n = pq$. Soient c, d deux nombres entiers, tels que $cd = 1 \bmod \varphi(n)$. Alors $\forall t \in \mathbb{Z} : t^{cd} = 1 \bmod n$.
On peut chiffrer un message via $g : \mathbb{Z}/n\mathbb{Z} \longrightarrow \mathbb{Z}/n\mathbb{Z}$, $t \longmapsto t^c$ et le déchiffrer via $h : \mathbb{Z}/n\mathbb{Z} \longrightarrow \mathbb{Z}/n\mathbb{Z}$, $t \longmapsto t^d$.

II - Structures de groupes sous-jacentes :

II - 1 Structure du groupe $(\mathbb{Z}/n\mathbb{Z}, +)$:

prop 13 : $(\mathbb{Z}/n\mathbb{Z}, +)$ est un groupe cyclique de cardinal n, dont $\overline{1}$ est un générateur. En particulier $(\mathbb{Z}/n\mathbb{Z}, +)$ est abélien.

th 14 : Tout groupe monogène G est soit isomorphe à $\mathbb{Z}$, soit isomorphe à $\mathbb{Z}/n\mathbb{Z}$, avec $n = |G|$.

ex 15 : $U_n := \{ e^{\frac{2ik\pi}{n}} ; k \in [\![0, n-1]\!] \} \cong (\mathbb{Z}/n\mathbb{Z}, +)$

def 15: On définit la fonction indicatrice d'Euler par $\varphi(n) := |(\mathbb{Z}/n\mathbb{Z})^\times|$

prop 16: Soit $x \in \mathbb{Z}$. Les propriétés suivantes sont équivalentes. (1) $\bar{x}$ est un générateur de $(\mathbb{Z}/n\mathbb{Z}, +)$
(2) $\text{pgcd}(x, n) = 1$.
(3) $\bar{x}$ est inversible pour la loi $\times$; ie $\bar{x} \in (\mathbb{Z}/n\mathbb{Z})^\times$

ex 17: Les générateurs de $(\mathbb{Z}/8\mathbb{Z} ; +)$ sont $\{\bar{1}, \bar{3}, \bar{5}, \bar{7}\}$.

prop 18: Pour chaque entier $d \geq 1$ divisant n, il existe un unique sous-groupe de $\mathbb{Z}/n\mathbb{Z}$ d'ordre d. C'est le sous groupe $\langle \frac{n}{d} \bmod n \rangle$.

app 19: $n = \sum_{d/n} \varphi(d)$

app 20: [Classification des groupes d'ordre pq]
Soit G un groupe d'ordre pq, avec $p < q$ deux nombres premiers. • si $p \nmid q-1$ alors $G \cong \mathbb{Z}/pq\mathbb{Z}$,
• si $p \mid q-1$ alors $G \cong \mathbb{Z}/q\mathbb{Z} \rtimes_\varphi \mathbb{Z}/p\mathbb{Z}$

app 21: [Structure des groupes abéliens finis]
Soit G un groupe abélien fini d'ordre $n \geq 2$. Il existe $p_1 | \dots | p_r$ uniques tels que $G \cong \mathbb{Z}/p_1\mathbb{Z} \times \dots \times \mathbb{Z}/p_r\mathbb{Z}$

DEV 1

prop 22: $\text{Aut}(\mathbb{Z}/n\mathbb{Z}) \longrightarrow (\mathbb{Z}/n\mathbb{Z})^\times$, $u \longmapsto u(1)$ est un isomorphisme de groupes.

II-2 Structure de $(\mathbb{Z}/n\mathbb{Z})^\times$

th 23: Soit $n = p_1^{\alpha_1} \dots p_r^{\alpha_r}$ une décomposition en produit de facteurs premiers. $(\mathbb{Z}/n\mathbb{Z})^\times \cong (\mathbb{Z}/p_1^{\alpha_1}\mathbb{Z})^\times \times \dots \times (\mathbb{Z}/p_r^{\alpha_r}\mathbb{Z})^\times$ via l'isomorphisme utilisé th 10.
donc $\varphi(n) = \varphi(p_1^{\alpha_1}) \dots \varphi(p_r^{\alpha_r})$.

prop 24: Soit p un nombre premier, $\alpha \geq 1$ entier :
• $\varphi(p) = p-1$; $\varphi(p^\alpha) = p^{\alpha-1}(p-1)$

ex 25: • $\varphi(2) = 1$ donc $(\mathbb{Z}/2\mathbb{Z})^\times \cong \{\bar{0}\}$
• $\varphi(4) = 2$, donc $(\mathbb{Z}/4\mathbb{Z})^\times \cong \mathbb{Z}/2\mathbb{Z}$

th 26: Soit $p \geq 3$ un nombre premier, alors
• $(\mathbb{Z}/p^\alpha\mathbb{Z})^\times \cong \mathbb{Z}/p^{\alpha-1}(p-1)\mathbb{Z}$; en particulier $(\mathbb{Z}/p^\alpha\mathbb{Z})^\times$ est cyclique.
• Si $\alpha \geq 3$: $(\mathbb{Z}/2^\alpha\mathbb{Z})^\times \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2^{\alpha-2}\mathbb{Z}$

DEV 1

ex 27: $(\mathbb{Z}/60\mathbb{Z})^\times \cong (\mathbb{Z}/2^2\mathbb{Z})^\times \times (\mathbb{Z}/3\mathbb{Z})^\times \times (\mathbb{Z}/5\mathbb{Z})^\times$
$\cong (\mathbb{Z}/2\mathbb{Z})^2 \times \mathbb{Z}/4\mathbb{Z}$.

Cor 28: [Petit théorème de Fermat]
$\forall a \in (\mathbb{Z}/p\mathbb{Z})^\times$: $a^{p-1} = 1 \bmod p$, où p est un nombre premier.

app 29: [Théorème de Wilson]
Soit $p \geq 2$. p est premier si et seulement si $(p-1)! \equiv -1 \bmod p$

app 30: [Test de Pocklington-Lehmer]
Soit $n \geq 2$ un entier impair, on note $n-1 = \prod_{i \in I} p_i^{\alpha_i}$ la décomposition en produit de facteurs premiers alors :
n est premier si et seulement si $\forall i \in I$ $\exists a_i \in (\mathbb{Z}/n\mathbb{Z})^\times$ tel que $a_i^{n-1} = 1$ et $\text{pgcd}(a_i^{\frac{n-1}{p_i}} - 1 ; n) = 1$

III - Le cas $n = p$ premier : On notera $\mathbb{F}_p := \mathbb{Z}/p\mathbb{Z}$, (corps)

III - 1 Etude des carrés dans $\mathbb{F}_p$

Soit p premier impair.

def 31 : On dit que $a \in \mathbb{F}_p^*$ est un carré s'il existe $u \in \mathbb{F}_p^*$ tel que $u^2 = a$, un tel u est appelé racine carrée de a. On note $\mathbb{F}_p^{*2}$ l'ensemble des carrés.

th 32 : (1) L'ensemble des carrés de $\mathbb{F}_p^*$ est un sous groupe multiplicatif cyclique à $\frac{p-1}{2}$ éléments.

(2) Pour tout $x \in \mathbb{F}_p^*$: x est un carré ssi $x^{\frac{p-1}{2}} = 1 \bmod p$

x n'est pas un carré ssi $x^{\frac{p-1}{2}} = -1 \bmod p$.

def 33 : On définit le symbole de Legendre, ($a \in \mathbb{Z}$)

$$\left(\frac{a}{p}\right) = \begin{cases} 0 & \text{si } p \mid a \\ 1 & p \nmid a \text{ et } a \text{ est un carré dans } \mathbb{F}_p^* \\ -1 & p \nmid a \text{ et } a \text{ n'est pas un carré dans } \mathbb{F}_p^* \end{cases}$$

prop 34 : $\forall a, b \in \mathbb{Z}$: $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$

th 35 : (1) -1 est un carré dans $\mathbb{F}_p^*$ ssi $p = 1 \bmod 4$

(2) 2 est un carré dans $\mathbb{F}_p^*$ ssi $p = \pm 1 \bmod 8$.

th 36 : [Loi de réciprocité quadratique]

Soient p, q deux nombres premiers impairs, on a :

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

ex 37 : $\left(\frac{665}{97}\right) = -1$

III - 2 Polynômes dans $\mathbb{F}_p[X]$

def 38 : Soit k un corps, $n \geq 1$, $P_n := X^n - 1$ et K_n le corps de décomposition de P_n sur k, $\mu_n(K_n)$ est l'ensemble des racines n-ièmes primitives ie générateur de μ_n

On définit le n-ième polynôme cyclotomique $\Phi_{n,k} \in K_n[X]$

$$\Phi_{n,k}(X) := \prod_{\zeta \in \mu_n'(K_n)} (X - \zeta)$$

prop 39 : Soit $\pi : \mathbb{Z}[X] \longrightarrow \mathbb{F}_p[X]$, $\sum a_i X^i \longmapsto \sum \overline{a_i} X^i$, on a : $\Phi_{n,\mathbb{F}_p} = \pi(\Phi_{n,\mathbb{Q}})$

Rq 40 : ($\Phi_{n,\mathbb{Q}} \in \mathbb{Z}[X]$)

app 41 : [Théorème de Dirichlet faible]

Soit $n \geq 2$. Il existe une infinité de nombres premiers p tels que $p = 1 \bmod n$.

app 42 : Soit $a > 0$. L'équation $x^2 = a$ admet une solution dans $\mathbb{Z}$ ssi elle admet une solution dans $\mathbb{F}_p$, $\forall p \geq 2$.

th 40 : Les propriétés suivantes sont équivalentes : ($n \geq 2$)

(1) Il existe p premier tel que $\gcd(n, p) = 1$ et $\Phi_{n,\mathbb{F}_p}$ est irréductible sur $\mathbb{F}_p$.

(2) $(\mathbb{Z}/n\mathbb{Z})^\times$ est cyclique.

(3) $n \in \{1, 2, 4, q^\alpha, 2q^\alpha\}$; avec q premier impair.

ex 41 : $\Phi_8 = X^4 + 1$ est irréductible sur tout corps.

th 42 : [Polynôme irréductible sur $\mathbb{F}_p$]

Il y a $I(n,p) = \frac{1}{n}\sum_{d \mid n} \mu\left(\frac{n}{d}\right) p^d$ polynômes irréductibles, unitaires de degré n dans $\mathbb{F}_p$. (μ désigne la fonction de Möbius)

IV - Application à la résolution d'équations diophantiennes :

ex 43 : (S) : $\begin{cases} 2x + 6y = 1 \bmod 35 \\ 3x + 14y = 9 \bmod 35 \end{cases}$ Les solutions de (S) sont de la forme $(3 + 14k + 35l, 5 + 7k)$ avec $k, l \in \mathbb{Z}$.

th 44 : [Sophie Germain]

Soit p un nombre premier tel que $2p+1$ soit premier. Il n'existe pas de triplet $(x, y, z) \in \mathbb{Z}^3$ tel que $xyz \neq 0 \bmod p$ et $x^p + y^p + z^p = 0$ (dans $\mathbb{Z}$)

th 45 : [Théorème des deux carrés] Soit p un nombre premier ≥ 2 on a équivalence entre (1) p est somme de deux carrés dans $\mathbb{Z}$

(2) $p = 2$ ou $p \equiv 1 \bmod 4$.

DEV (2)

Plan :

I - Structure de l'anneau $(\mathbb{Z}/n\mathbb{Z}, +, \cdot)$

II - Structures de groupes sous jacentes.
- II.1 Structure du groupe $(\mathbb{Z}/n\mathbb{Z}, +)$
- II.2 Structure du groupe $((\mathbb{Z}/n\mathbb{Z})^\times, \cdot)$

III - Le cas $n = p$, premier.
- III-1 Etude des carrés dans $\mathbb{F}_p$.
- III-2 Polynôme dans $\mathbb{F}_p[X]$

IV - Applications à la résolutions d'équation diophantiennes.

Références : Arithmétique [F. Liret], Dunod.
- Algèbre et géométrie, [F. Combes], Bréal.
- Cours d'algèbre [D. Perrin] ← (développement théorème de Dirichlet faible)
- les maths en tête [X. Gourdon] (développement étude de $\mathrm{Aut}(\mathbb{Z}/n\mathbb{Z})$)
- Oraux X-ENS, algèbre 1 [Francinou, Gianella, Nicolas] ← ~~(développement Sophie-Germain)~~

On aurait pu ajouter :
- l'étude des nilpotents, idempotents de l'anneau $(\mathbb{Z}/n\mathbb{Z}, +, \cdot)$
- les générateurs de $(\mathbb{Z}/n\mathbb{Z})^\times$
- l'étude des carrés dans $(\mathbb{Z}/n\mathbb{Z}, +, \cdot)$
- les polynômes sur $(\mathbb{Z}/n\mathbb{Z}, +, \cdot)$