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

Mohamed NASSIRI

$\mathbb{Z}/n\mathbb{Z}$ est un ensemble très intéressant : il peut être vu comme le groupe $(\mathbb{Z}/n\mathbb{Z}, +)$, comme l'anneau $(\mathbb{Z}/n\mathbb{Z}, +, \times)$ ou comme le corps $(\mathbb{Z}/p\mathbb{Z}, +, \times)$ pour p premier. C'est cette richesse qui fait également la complexité de l'étude de $\mathbb{Z}/n\mathbb{Z}$. Dans cette leçon, on souhaite étudier ces ensembles : ordre des éléments, générateurs, sous-groupes, idéaux, inversibles, automorphismes, etc. Bref de la bonne botanique !

Le point de départ des anneaux $\mathbb{Z}/n\mathbb{Z}$ est "l'arithmétique modulo" sur $\mathbb{Z}$. En donnant une structure algébrique à $\mathbb{Z}/n\mathbb{Z}$ cela va nous permettre de réaliser des opérations en restant dans $\mathbb{Z}/n\mathbb{Z}$. Ainsi, ces anneaux offrent un point de vue moderne de l'arithmétique issue de l'algèbre. On a, par exemple, l'équivalence suivante : $\bar{x} + \bar{y} = \bar{z} \Leftrightarrow x + y \equiv z \pmod{n}$. L'avantage de la première égalité peut se voir ainsi : par exemple dans $\mathbb{Z}/5\mathbb{Z}$, $\bar{2}$ et $\bar{7}$ sont le même nombre et ne sont plus congrus. Mais surtout, c'est une "vraie" égalité !

Quand l'anneau $\mathbb{Z}/p\mathbb{Z}$ est un corps, on a plusieurs résultats intéressants. Par exemple, on a deux résultats sur l'rréductibilité des polynômes : le critère d'Eisenstein et le critère de réduction. Mais également, l'étude des carrés de $\mathbb{Z}/p\mathbb{Z}$ va nous conduire au "théorème des deux carrés".

Références

[CAL] Éléments de théorie des groupes, Josette Calais
[PER] Cours d'Algèbre, Daniel Perrin
[MADag] Leçons d'Algèbre : Préparation à l'Oral de l'Agrégation, Karine Madère
[KM] Introduction à la théorie des nombres, Jean-Marie De Koninck et Armel Mercier
[ML3ag] Mathématiques Algèbre L3, Aviva Szpirglas

Développements

Théorème de Dirichlet (version faible)
Théorème des deux carrés

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

1.1 Présentation [CAL] p.94-95,99-100

Théorème 1 : $\forall n \in \mathbb{N}^*$, le groupe $(\mathbb{Z}/n\mathbb{Z}, +)$ est cyclique, d'ordre n.

Proposition 2 : Soient $n \in \mathbb{N}^*$ et π l'épimorphisme canonique $\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$. Pour tout sous-groupe K de $\mathbb{Z}/n\mathbb{Z}$, il existe un unique diviseur k de n, dans $\mathbb{N}^*$, tel que $\pi(K)$ engendre K et $ord(K) = \frac{n}{k}$.

Corollaire 3 : Le nombre de sous-groupes de $\mathbb{Z}/n\mathbb{Z}$, $n \in \mathbb{N}^*$, est égal au nombre de diviseurs de n dans $\mathbb{N}^*$.

Exemple 4 : Les diviseurs de 6, dans $\mathbb{N}$, $1, 2, 3$ et 6, on peut affirmer que $\mathbb{Z}/6\mathbb{Z}$ a quatre sous-groupes distincts :
$\langle\overline{1}\rangle = \mathbb{Z}/6\mathbb{Z}$, $\langle\overline{2}\rangle = \{\overline{2}, \overline{4}, \overline{0}\}$, $\langle\overline{3}\rangle = \{\overline{3}, \overline{0}\}$ et $\langle\overline{0}\rangle = \{\overline{0}\}$
Les sous-groupes $\langle\overline{4}\rangle$ et $\langle\overline{5}\rangle$ coïncident donc nécessairement avec l'un des quatre sous-groupes précédents.

1.2 Générateurs

Théorème 5 : Soit $k \in \mathbb{Z}$. k est premier avec $n \Leftrightarrow \overline{k}$ est générateur du groupe $\mathbb{Z}/n\mathbb{Z}$. **[PER] p.24**

Définition 6 : Soit $E(n) = \{k \in \mathbb{N} \mid 1 \leq k \leq n-1 \text{ et } (k, n) = 1\}$. On appelle fonction indicatrice d'Euler l'application $\varphi : \mathbb{N}^* \mapsto \mathbb{N}^*$ telle que :

$$\varphi(1) = 1, \text{ et } \varphi(n) = \text{card}(E(n)), \ \forall n > 1.$$

[CAL] p.104

Proposition 7 : Le nombre de générateurs du groupe $\mathbb{Z}/n\mathbb{Z}$ est $\varphi(n)$. **[CAL] p.104**

Exemple 8 : $\varphi(p) = p-1$, $\varphi(p^\alpha) = p^{\alpha-1}(p-1)$, $\alpha \in \mathbb{N}^*$. **[PER] p.24**

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

2.1 Présentation [MADag] p.44

Proposition 9 : La relation de congruence modulo n est une relation d'équivalence.

Définition 10 : Une classe d'équivalence de la relation de congruence modulo n est appelée classe

de congruence modulo n.
L'ensemble des classes de congruence modulo n est noté $\mathbb{Z}/n\mathbb{Z}$.
Soit $k \in \mathbb{Z}$. La classe de congruence modulo n de k est notée $\underline{k}$.

Proposition 11 : Soit α une classe de congruence modulo n. Alors l'ensemble $\alpha \cap [\![0; n-1]\!]$ est un singleton.

Définition 12 : On définit une multiplication sur $\mathbb{Z}/n\mathbb{Z}$ en posant, $\forall (x,y) \in \mathbb{Z}^2$, $\overline{x}.\overline{y} = \overline{xy}$.

Théorème 13 : $(\mathbb{Z}/n\mathbb{Z}, +, .)$ est un anneau commutatif.
De plus, la surjection canonique

$$s : \mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}, \ k \mapsto \overline{k}$$

est un homomorphisme d'anneaux de noyau $n\mathbb{Z}$.
Enfin, l'anneau $\mathbb{Z}/n\mathbb{Z}$ est de cardinal n.

2.2 $(\mathbb{Z}/n\mathbb{Z})^*$ et Aut$(\mathbb{Z}/n\mathbb{Z})$

Définition 14 : $\overline{k} \in (\mathbb{Z}/n\mathbb{Z})^* \Leftrightarrow \exists \lambda \in \mathbb{Z}, \ \overline{\lambda k} = \overline{1}$. **[PER] p.24**

Théorème 15 : (*à rapprocher du théorème 5*) k est premier avec $n \Leftrightarrow \overline{k}$ est générateur du groupe $\mathbb{Z}/n\mathbb{Z} \Leftrightarrow \overline{k} \in (\mathbb{Z}/n\mathbb{Z})^*$ **[PER] p.24**

Théorème 16 : $(\mathbb{Z}/n\mathbb{Z})^*$ est un groupe multiplicatif abélien, d'ordre $\varphi(n)$. **[CAL] p.105**

Corollaire 17 : Théorème d'Euler
Soit $(a,m) = 1$, alors $a^{\Phi(m)} \equiv 1 \pmod{m}$ **[KM] p.43**

Corollaire 18 : Petit théorème de Fermat
Soit p un nombre premier et soit a un entier positif tel que $p \nmid a$. Alors $a^{p-1} \equiv 1 \pmod{p}$. De plus, $\forall a \in \mathbb{N}$, on a $a^p \equiv a \pmod{p}$. **[KM] p.43**

Proposition 19 : On a un isomorphisme Aut$(\mathbb{Z}/n\mathbb{Z}) \approx (\mathbb{Z}/n\mathbb{Z})^*$. En particulier, Aut$(\mathbb{Z}/n\mathbb{Z})$ est un groupe abélien, de cardinal $\varphi(n)$. **[PER] p.24**

Proposition 20 (admis) : Soit n un entier, $n = p_1^{a_1} p_2^{a_2} ... p_r^{a_r}$, avec les p_i premiers distincts et les a_i sont des entiers strictement positifs.
1) On a un isomorphisme d'anneaux

$$\mathbb{Z}/n\mathbb{Z} \approx \prod_{i=1}^{r} \mathbb{Z}/p_i^{a_i}\mathbb{Z},$$

2) On a un isomorphisme de groupes

$$(\mathbb{Z}/n\mathbb{Z})^* \approx \prod_{i=1}^{r} (\mathbb{Z}/p_i^{a_i}\mathbb{Z})^*,$$

3) On a

$$\varphi(n) = \prod_{i=1}^{r} (\varphi(p_i^{a_i}) = n \prod_{i=1}^{r} (1 - 1/p_i)$$

Lemme 21 : Si p est un nombre premier, on a un isomorphisme $(\mathbb{Z}/p\mathbb{Z})^* \approx \mathbb{Z}/(p-1)\mathbb{Z}$.

3 Le corps $\mathbb{Z}/p\mathbb{Z}$

3.1 Présentation

Proposition 22 : Soit $p \in \mathbb{N}$, $p \geq 2$. Les assertions suivantes sont équivalentes :
(i) p est un nombre premier
(ii) $\mathbb{Z}/p\mathbb{Z}$ est un anneau intègre
(iii) $\mathbb{Z}/p\mathbb{Z}$ est un corps

Application 23 : Théorème de Wilson :
Soit $m \in \mathbb{N}^*$. Alors

$$m \text{ est premier} \Leftrightarrow (m-1)! \equiv -1 \pmod{m}$$

[KM] p.45

Application 24 : Caractéristique d'un corps K
Soit $\varphi : \mathbb{Z} \mapsto K$ le morphisme d'anneaux défini par $\varphi(n) = n.1 = 1 + ... + 1$.
Le nombre p, générateur de Kerφ, est appelé la caractéristique du corps K. La caractéristique d'un corps est donc 0 ou un nombre premier. On le note car(K). **[PER] p.72**

3.2 Carrés de $\mathbb{Z}/p\mathbb{Z}$ [PER] p.56 → 58, 74-75

Définition 25 : $\mathbb{F}_p := \mathbb{Z}/p\mathbb{Z}$, $\mathbb{F}_p^2 := \{x \in \mathbb{F}_p \mid \exists y \in \mathbb{F}_p, \ x = y^2\}$ et $\mathbb{F}_p^{*2} := \mathbb{F}_p^2 \cap \mathbb{F}_p^*$

Proposition 26 : 1) Pour $p = 2$, $\mathbb{F}_p^2 = \mathbb{F}_p$
2) Pour $p > 2$, $|\mathbb{F}_p^2| = \frac{p+1}{2}$ et $|\mathbb{F}_p^{*2}| = \frac{p-1}{2}$

Proposition 27 : Pour $p > 2$, on a :

$$x \in \mathbb{F}_p^{*2} \Leftrightarrow x^{\frac{p-1}{2}} = 1$$

Corollaire 28 : Soit $p > 2$. Alors $-1 \in \mathbb{F}_p^{*2} \Leftrightarrow p = 2$ ou $p \equiv 1 \pmod{4}$

Définition 29 : On pose $\Sigma = \{n \in \mathbb{N} \mid n = a^2 + b^2 = n\}$

♠ **Théorème 30 :** Théorème des deux carrés ♠
$p \in \Sigma \Leftrightarrow p = 2$ ou $p \equiv 1 \pmod{4}$

4 Applications

4.1 Irréductibilité des polynômes

♠ **Théorème 31 :** Critère d'Eisenstein ♠
Soit $P = a_n X^n + ... + a_1 X + a_0 \in \mathbb{Z}[X]$ et p un nombre premier. On suppose que :

$$(i) \ p \nmid a_n \ , \ (ii) \ p \mid a_0, ..., a_{n-1} \ , \text{et} \ (iii) \ p^2 \nmid a_0$$

Alors P est irréductible dans $\mathbb{Q}[X]$.
Si $c(P) = 1$, alors P est irréductible dans $\mathbb{Z}[X]$. **[FGNag1] p.145**

Exemple 32 : 1) $\forall p$ premier, $X^n - p$ est irréductible dans $\mathbb{Q}[X]$ et $\mathbb{Z}[X]$.
2) $\Phi_5(X) = X^4 + X^3 + X^2 + X + 1$ est irréductible dans $\mathbb{Z}[X]$. **[ML3ag] p.549**

Théorème 33 : Critère de réduction modulo p : Soit p un nombre premier.

Soit $P = a_nX^n + ... + a_1X + a_0 \in \mathbb{Z}$[X] et $\overline{P} = \overline{a_n}X^n + ... + \overline{a_1}X + \overline{a_0}$, où $\overline{a_i}$ est la classe des a_i dans $\mathbb{Z}/p\mathbb{Z}$
vc Alors si $\overline{P}$ est irréductible sur $\mathbb{F}_p$, P est irréductible sur $\mathbb{Z}$.
Si $c(P) = 1$, alors P est irréductible dans $\mathbb{Z}$[X]. **[ML3ag] p.550**

Exemple 34 : $P(X) = X^3 + 462X^2 + 2433X - 67691$ est irréductible dans $\mathbb{Z}$[X] **[PER] p.77**

2

4.2 Théorème de Dirichlet (version faible)

♠ **Théorème 35 :** Théorème de Dirichlet (version faible) : ♠
a) $\Phi_n(X)$ désigne le n-ième polynôme cyclotomique. Si un nombre premier p divise $\Phi_n(a)$ pour un certain $a \in \mathbb{N}$, mais aucun des $\Phi_d(a)$ où $d \mid n$, $d < n$, alors $p \equiv 1 \pmod{n}$
b) Il existe une infinité de nombres premiers de la forme $1 + \lambda n$, $\lambda \in \mathbb{N}^*$. **[GOZ] p.84**

Questions

Exercice : 1) Dans le théorème des restes chinois, on a un isomorphisme (pour p et q premiers entre eux) :

$$\Phi : \mathbb{Z}/pq\mathbb{Z} \xrightarrow{\sim} \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/q\mathbb{Z}$$

Donner l'application réciproque de Φ.
2) Utiliser cette application pour résoudre le système :

$$(S) \begin{cases} x \equiv 5 \pmod{13} \\ x \equiv 2 \pmod{7} \end{cases}$$

Solution : 1) Posons l'application réciproque

$$\Psi : \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/q\mathbb{Z} \to \mathbb{Z}/pq\mathbb{Z}$$

Comme c'est un morphisme, on a juste besoin de connaître l'image de $(0,1)$ et de $(1,0)$. En effet, pour tout $(a,b) \in \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/q\mathbb{Z}$, on a $\Psi(a,b) = a\Psi(1,0) + b\Psi(0,1)$.
Comme p et q sont premiers entre eux, d'après le lemme de Bézout, il existe $u, v \in \mathbb{Z}$ tel que $up + vq = 1$.
En prenant,

$$\begin{aligned} \Psi : \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/q\mathbb{Z} &\to \mathbb{Z}/pq\mathbb{Z} \\ (1,0) &\mapsto vq \\ (0,1) &\mapsto up \end{aligned}$$

2) Remarquons pour commencer que 13 et 7 sont premiers entre eux et que l'on a l'équivalence suivante :

$$x \text{ est solution de } (S) \Leftrightarrow x = \Psi(5,2)$$

Comme 13 et 7 sont premiers entre eux, et que l'on a la relation de Bézout $1 = 2 \times 7 + (-1) \times 13$. On a donc :

$$\Psi : \mathbb{Z}/13\mathbb{Z} \times \mathbb{Z}/7\mathbb{Z} \to \mathbb{Z}/91\mathbb{Z}$$

On a donc $\Psi(1,0) = 2 \times 7 = 14$ et $\Psi(0,1) = (-1) \times 13 = -13$. Par conséquent, $x = \Psi(5,2) = 5\Psi(1,0) + 2\Psi(0,1) = 5 \times 14 + 2 \times (-13) = 44 \pmod{91}$

Exercice : Que peut-on dire du nombre de morphismes d'anneaux entre $\mathbb{Z}/n\mathbb{Z}$ et $\mathbb{Z}/m\mathbb{Z}$ pour $(m,n) \in \mathbb{N}^{*2}$ fixés ?

Solution : Posons $\Theta : \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/m\mathbb{Z}$. Le morphisme d'anneaux Θ vérifie $\Theta(0) = 0$ et $\Theta(1) = 1$.
Nous noterons $\tilde{x}$ et $\overline{x}$ respectivement les classes de $x \in \mathbb{Z}$ dans $\mathbb{Z}/n\mathbb{Z}$ et respectivement dans $\mathbb{Z}/m\mathbb{Z}$.
On a donc :

$$0 = \Theta(0) = \Theta(\tilde{n}) = \Theta(\underbrace{1 + ... + 1}_{n \text{ fois}}) = \underbrace{\Theta(1) + ... + \Theta(1)}_{n \text{ fois}} = n.\Theta(1) = n.\overline{1} = \overline{n}$$

Ainsi, $n = 0 \in \mathbb{Z}/m\mathbb{Z}$, c'est-à-dire m divise n.
De plus, le morphisme est unique car $\Theta(\tilde{x}) = \overline{x}$ pour tout $\tilde{x} \in \mathbb{Z}/n\mathbb{Z}$.
En effet,

$$\overline{x} = \underbrace{1 + ... + 1}_{x \text{ fois}} = \underbrace{\Theta(1) + ... + \Theta(1)}_{x \text{ fois}} = \Theta(\underbrace{1 + ... + 1}_{x \text{ fois}}) = \Theta(\tilde{x})$$

Exercice : A quelle(s) condition(s) $\mathbb{Z}/n\mathbb{Z}$ n'admet pas d'éléments nilpotents ?

Solution : $\mathbb{Z}/n\mathbb{Z}$ n'admet pas d'éléments nilpotents si les facteurs premiers de n sont d'exposants 1.
Procédons par contraposée.
Ainsi, il existe donc un nombre premier p tel que p^2 divise n. L'élement $\frac{n}{p}$ est nilpotent (d'indice 2).
En effet, il existe $k \in \mathbb{N}$ tel que $n = kp^2$.

$$\left(\frac{n}{p}\right)^2 = (kp)^2 = k.kp^2 = k.n \equiv 0 \pmod{n}$$