Les anneaux $\mathbb{Z}_n$

Marc Lorenzi

22 décembre 2025

1 Congruences

1.1 Les sous-groupes de $\mathbb{Z}$

Pour tout $n \in \mathbb{Z}$, nous notons $n\mathbb{Z} = \{kn : k \in \mathbb{Z}\}$.

Proposition 1. *Pour tous $n, n' \in \mathbb{Z}$, $n\mathbb{Z} = n'\mathbb{Z}$ si et seulement si $n' = \pm n$.*

Démonstration. Soient $n, n' \in \mathbb{Z}$. Supposons $n\mathbb{Z} = n'\mathbb{Z}$. On a $n' = 1n' \in n'\mathbb{Z}$ donc $n' \in n\mathbb{Z}$ d'où n divise n'. De même, n' divise n donc $n' = \pm n$. Inversement, il est immédiat que $n\mathbb{Z} = (-n)\mathbb{Z}$. □

Proposition 2. *Les sous-groupes de $\mathbb{Z}$ sont les ensembles $n\mathbb{Z}$ où $n \in \mathbb{N}$.*

Démonstration. Soit $n \in \mathbb{N}$. Soit $G = n\mathbb{Z}$. On a $0 = 0n \in G$, donc G n'est pas vide. Soient $x, y \in G$. Soient $k, k' \in \mathbb{Z}$ tels que $x = nk$ et $y = n'k$. On a $x - y = n(k - k') \in G$.

Inversement, soit G un sous-groupe de $\mathbb{Z}$. Si $G = \{0\}$, alors $G = 0\mathbb{Z}$. Sinon, G contient un élément non nul et donc, par stabilité par passage à l'opposé, un élément $n > 0$. Prenons un tel n minimal. Comme G est un groupe, on a pour tout $k \in \mathbb{Z}$, $kn \in G$. Ainsi, $n\mathbb{Z} \subseteq G$. Soit enfin $a \in \mathbb{Z}$. Effectuons la division euclidienne de a par n : $a = kn + r$ où $k \in \mathbb{Z}$ et $r \in [\![0, n-1]\!]$. On a $r = a - kn \in G$. Comme $0 \leq r < n$, la minimalité de n entraîne $r = 0$. Ainsi, $a = nk$ donc $G \subseteq n\mathbb{Z}$. □

Remarque. En termes ensemblistes, nous avons $n\mathbb{Z} + n\mathbb{Z} = n\mathbb{Z} - n\mathbb{Z} = n\mathbb{Z}$. Remarquons également que les sous-groupes de $\mathbb{Z}$ étant stable par passage aux multiples, ce sont aussi les idéaux de l'anneau $\mathbb{Z}$.

1.2 Congruences

Définition 1. Soit $n \in \mathbb{N}$. Pour tous $a, b \in \mathbb{Z}$, a est *congru* à b *modulo* n lorsque $b - a \in n\mathbb{Z}$.

Lorsque a est congru à b modulo n, on note $a \equiv b \bmod n$. Sinon, on note $a \not\equiv b \bmod n$.

Remarque. Le cas $n = 0$ est à part. En effet, $a \equiv b \mod 0$ si et seulement si $a = b$. Dans la suite, nous nous occuperons uniquement du cas des entiers $n \in \mathbb{N}^*$.

Proposition 3. *Soit $n \in \mathbb{N}^*$. La relation de congruence modulo n est une relation d'équivalence. Elle possède n classes qui sont les classes de $0, 1, \ldots, n-1$.*

Démonstration. Soit $a \in \mathbb{Z}$. On a $a - a = 0 \in n\mathbb{Z}$ donc $a \equiv a \mod n$. la relation est réflexive.

Soient $a, b \in \mathbb{Z}$. Supposons $a \equiv b \mod n$. On a $(a - b) = -(b - a) \in n\mathbb{Z}$ donc $b \equiv a \mod n$. La relation est symétrique.

Soient $a, b, c \in \mathbb{Z}$. Supposons $a \equiv b \mod n$ et $b \equiv c \mod n$. On a $c - a = (c - b) + (b - a)$. Comme $n\mathbb{Z}$ est stable par addition, $c - a \in n\mathbb{Z}$ donc $a \equiv c \mod n$. La relation est transitive.

Passons au décompte des classes. Soit $a \in \mathbb{Z}$. La division euclidienne de a par n donne $a = kn + r$ où $k \in \mathbb{Z}$ et $r \in [\![0, n-1]\!]$. De là, $a \in r + n\mathbb{Z}$. La relation de congruence modulo n possède donc au plus n classes, celles de $0, 1, \ldots, n-1$. Il reste à montrer que ces classes sont distinctes. Pour cela, donnons-nous $0 \leq i < j < n$. On a $0 < j - i < n$ donc $j - i \notin n\mathbb{Z}$. Dit autrement, les classe de i et de j sont distinctes. □

Nous noterons $\mathbb{Z}_n$ l'ensemble des classes pour la relation de congruence modulo n. Pour tout $a \in \mathbb{Z}$, la classe de a est

$$a + n\mathbb{Z} = \{a + kn : k \in \mathbb{Z}\}$$

La proposition précédente nous dit que pour tout $n \in \mathbb{N}^*$, $\mathbb{Z}_n$ est un ensemble fini de cardinal n, et

$$\mathbb{Z}_n = \{0 + n\mathbb{Z}, 1 + n\mathbb{Z}, \ldots, n - 1 + n\mathbb{Z}\}$$

1.3 Structure d'anneau sur $\mathbb{Z}_n$

Proposition 4. *Soient $a, b, a', b' \in \mathbb{Z}$. On suppose $a \equiv a' \mod n$ et $b \equiv b' \mod n$. On a alors $a + b \equiv a' + b' \mod n$ et $ab \equiv a'b' \mod n$.*

Démonstration.

$$(a' + b') - (a + b) = (a' - a) + (b' - b) \in n\mathbb{Z} + n\mathbb{Z} = n\mathbb{Z}$$

donc $a + b \equiv a' + b' \mod n$. De même,

$$a'b' - ab = (a' - a)b' + +a(b' - b) \in (n\mathbb{Z})\mathbb{Z} + \mathbb{Z}(n\mathbb{Z}) = \mathbb{Z}$$

donc $ab \equiv a'b' \mod n$. □

La propriété précédente permet de définir sur $\mathbb{Z}_n$ une addition et une multiplication en posant pour tous $a, b \in \mathbb{Z}$,

$$\begin{aligned} (a + n\mathbb{Z}) + (b + n\mathbb{Z}) &= a + b + n\mathbb{Z} \\ (a + n\mathbb{Z}) \times (b + n\mathbb{Z}) &= a \times b + n\mathbb{Z} \end{aligned}$$

Par la proposition **??**, ces opérations ne dépendent que des classes de a et b modulo n, et pas de a et b eux-mêmes.

Proposition 5. *$(\mathbb{Z}_n, +\times)$ est un anneau commutatif.*

Démonstration. Ce sont de simples vérifications. Par exemple, pour tous $a, b, c \in \mathbb{Z}$,

$$((a + n\mathbb{Z})(b + n\mathbb{Z}))(c + n\mathbb{Z}) = (ab + n\mathbb{Z})(c + n\mathbb{Z}) = (ab)c + n\mathbb{Z}$$

et

$$(a + n\mathbb{Z})((b + n\mathbb{Z})(c + n\mathbb{Z})) = (a + n\mathbb{Z})(bc + n\mathbb{Z}) = a(bc) + n\mathbb{Z}$$

Or, $(ab)c = a(bc)$ car la multiplication est associative dans $\mathbb{Z}$. La multiplication est donc associative dans $\mathbb{Z}_n$. Le neutre pour l'addition est $n\mathbb{Z}$, le neutre pour la multiplication est $1 + n\mathbb{Z}$. □

Remarque. On vérifie facilement que dans l'anneau $\mathbb{Z}_n$, il y a équivalence entre multiples et multiplications. Si $a, b \in \mathbb{Z}$, alors

$$(a + n\mathbb{Z})(b + n\mathbb{Z}) = a(b + n\mathbb{Z})$$

2 Le groupe additif $(\mathbb{Z}_n, +)$

Le groupe $(\mathbb{Z}_n, +)$ est un groupe cyclique, engendré entre autres par $1 + n\mathbb{Z}$.

2.1 Les sous-groupes de $\mathbb{Z}_n$

Proposition 6. *Les sous-groupes de $\mathbb{Z}_n$ sont cycliques.*

Démonstration. Soit G un sous-groupe de $\mathbb{Z}_n$. Si $G = \{n\mathbb{Z}\}$, alors $G =< n\mathbb{Z} >$. Supposons que $G \neq \{n\mathbb{Z}\}$. Prenons $m \in [\![1, n-1]\!]$ minimal tel que $m+n\mathbb{Z} \in G$. Montrons que $G =< m+n\mathbb{Z} >$. Par stabilité de G par passage aux multiples, $< m + n\mathbb{Z} > \subseteq G$. Inversement, soit $x \in G$. Soit $a \in \mathbb{Z}$ tel que $x\overline{a}$. Effectuons la division euclidienne de a par m : $a = qm + r$ où $q \in \mathbb{Z}$ et $r \in [\![0, n-1]\!]$. En passant aux classes, il vient

$$r + n\mathbb{Z} = (x + n\mathbb{Z}) - q(m + n\mathbb{Z}) \in G$$

Par minimalité de m, on a donc $r = 0$, d'où $x = q(m+n\mathbb{Z}) \in < m+n\mathbb{Z} >$. Ainsi, $G \subseteq < m+n\mathbb{Z} >$. □

Proposition 7. *Pour tout $m \in \mathbb{Z}$, $< m + n\mathbb{Z} >=< m \wedge n + n\mathbb{Z} >$.*

Démonstration. Soit $m \in \mathbb{Z}$. Notons $\delta = m \wedge n$. Il existe $u, v \in \mathbb{Z}$ tels que $um + vn = \delta$. En passant aux classes,

$$\delta + n\mathbb{Z} = u(m + n\mathbb{Z}) + vn\mathbb{Z} = u(m + n\mathbb{Z}) \in < m + n\mathbb{Z} >$$

De là, $< \delta + n\mathbb{Z} > \subseteq < m + n\mathbb{Z} >$. Inversement, soit $x \in < m + n\mathbb{Z} >$. Soit $k \in \mathbb{Z}$ tel que $x = k(m + n\mathbb{Z})$. Comme δ divise m, il existe $c \in \mathbb{Z}$ tel que $m = c\delta$. De là,

$$x = k(m + n\mathbb{Z}) = k(c\delta + n\mathbb{Z}) = kc(\delta + n\mathbb{Z}) \in < \delta + n\mathbb{Z} >$$

Ainsi, $< m + n\mathbb{Z} > \subseteq < \delta + n\mathbb{Z} >$. □

Corollaire 8. *Pour tout $m \in \mathbb{Z}$, $| < m + n\mathbb{Z} > | = n/(m \wedge n)$.*

Démonstration. Soit $m \in \mathbb{Z}$. Soit $G =< m + n\mathbb{Z} >$. Soit $\delta = m \wedge n$. On a $G =< \delta + n\mathbb{Z} >$. Posons $n = d\delta$. On a alors facilement

$$G = \{n\mathbb{Z}, \delta + n\mathbb{Z}, \ldots, (d-1)\delta + n\mathbb{Z}\}$$

Ainsi, le cardinal de G est $d = n/\delta$. □

Corollaire 9. *Le cardinal des sous-groupes de $\mathbb{Z}_n$ divise n.*

Démonstration. Conséquence immédiate de la proposition précédente. □

Proposition 10. *Pour tout diviseur d de n, $\mathbb{Z}_n$ possède un et un seul sous-groupe de cardinal d, qui est $< n/d + n\mathbb{Z} >$.*

Démonstration. Soit d un diviseur de n. Clairement, $< n/d + n\mathbb{Z} >$ est un sous-groupe de $\mathbb{Z}_n$ de cardinal d. Inversement, soit $G =< m + n\mathbb{Z} >$ un sous-groupe de $\mathbb{Z}_n$ de cardinal d. En posant $\delta = m \wedge n$, on a aussi $G =< \delta + n\mathbb{Z} >$. En posant $n = d'\delta$, la preuve de la proposition précédente nous dit que

$$G = \{n\mathbb{Z}, \delta + n\mathbb{Z}, (d'-1)\delta + n\mathbb{Z}\}$$

est de cardinal d'. Ainsi, $d' = d$, puis $\delta = n/d$ et enfin $G =< \delta + n\mathbb{Z} >=< n/d + n\mathbb{Z} >$. □

Notation. Pour tout diviseur d de n, nous noterons G_d l'unique sous-groupe de $n\mathbb{Z}$ de cardinal d.

2.2 Générateurs

Proposition 11. *Les générateurs de $\mathbb{Z}_n$ sont les classes $a + n\mathbb{Z}$ où $a \in [\![1, n]\!]$ est premier avec n.*

Démonstration. Soit $a \in [\![1, n]\!]$. Par le corollaire ?, $| < a + n\mathbb{Z} > | = n/(a \wedge n)$. La classe $a + n\mathbb{Z}$ engendre $\mathbb{Z}_n$ si et seulement si $n/(a \wedge n) = n$, c'est à dire $a \wedge n = 1$. □

Définition 2. La *fonction indicatrice d'Euler* est la fonction $\varphi : \mathbb{N}^* \longrightarrow \mathbb{N}^*$ définie, pour tout $n \in \mathbb{N}^*$, par

$$\varphi(n) = |\{a \in [\![1, n]\!] : a \wedge n = 1\}|$$

Le groupe $(\mathbb{Z}_n, +)$ possède donc $\varphi(n)$ générateurs.

Proposition 12. *Pour tout diviseur d de n, les groupe $(G_d, +)$ est $(\mathbb{Z}_d, +)$ sont isomorphes.*

Démonstration. Soit d un diviseur de n. Rappelons que $G_d =< n/d+n\mathbb{Z} >$. Soit $f : G_d \longrightarrow d\mathbb{Z}$ définie pour tout $k \in \mathbb{Z}$ par

$$f(kn/d + n\mathbb{Z}) = k + d\mathbb{Z}$$

Il s'agit tout d'abord de vérifier que la fonction f est bien définie. Soient $k, k' \in \mathbb{Z}$. Supposons que $kn/d + n\mathbb{Z} = k'n/d + n\mathbb{Z}$. Il existe $k'' \in \mathbb{Z}$ tel que

$$k'\frac{n}{d} = k\frac{n}{d} + k''n$$

De là,

$$k' = k + k''d$$

et donc $k + d\mathbb{Z} = k' + d\mathbb{Z}$.

Soient $k, k' \in \mathbb{Z}$. On a

$$\begin{aligned} f((kn/d + n\mathbb{Z}) + (k'n/d + n\mathbb{Z})) &= f((k + k')n/d + n\mathbb{Z}) \\ &= (k + k') + d\mathbb{Z} \\ &= f(kn/d + n\mathbb{Z}) + f(k'n/d + n\mathbb{Z}) \end{aligned}$$

Ainsi, f est un morphisme de groupes.

Soit $k \in \mathbb{Z}$. Supposons que $kn/d + d\mathbb{Z} \in \ker f$. On a donc $k + d\mathbb{Z} = d\mathbb{Z}$ c'est à dire $k \in d\mathbb{Z}$. De là, $kn/d + d\mathbb{Z} \in n\mathbb{Z}$. Ainsi, $\ker f = n\mathbb{Z}$ donc f est injectif. Enfin, $|G_d| = |d\mathbb{Z}| = d$, donc f est un isomorphisme. □

Remarque. L'isomorphisme réciproque de f est la fonction $f^{-1} : \mathbb{Z}_d \longrightarrow G_d$ définie pour tout $k \in \mathbb{Z}$ par

$$f^{-1}(k + d\mathbb{Z}) = kn/d + n\mathbb{Z}$$

Corollaire 13. *Pour tout diviseur d de n, le groupe G_d possède $\varphi(d)$ générateurs. Ces générateurs sont les $kn/d + d\mathbb{Z}$ où $k \in [\![1, d]\!]$ est premier avec d.*

Démonstration. Soit d un diviseur de n. L'isomorphisme f établit une bijection entre les générateurs de G_d et les générateurs de $\mathbb{Z}_d$. Ces derniers sont les $k + d\mathbb{Z}$ où $k \in [\![1, d]\!]$ est premier avec d. □

Proposition 14.

$$\sum_{d|n} \varphi(d) = n$$

Démonstration. Pour tout diviseur d de n, soit A_d l'ensemble des générateurs de G_d. Les A_d sont disjoints deux à deux et de cardinal $\varphi(d)$. De plus, pour tout $x \in \mathbb{Z}_n$, le sous-groupe $< x >$ de $\mathbb{Z}_n$ est de la forme G_d où d divise n, et donc $x \in A_d$. Ainsi, on a l'union disjointe

$$\mathbb{Z}_n = \bigcup_{d|n} A_d$$

De là,

$$|\mathbb{Z}_n| = \sum_{d|n} |A_d|$$

d'où le résultat. □

3 Les inversibles de $\mathbb{Z}_n$

L'ensemble $\mathbb{Z}_n^\times$ des éléments inversibles de $\mathbb{Z}_n$ est un groupe pour la multiplication.

Proposition 15. *Soit $a \in \mathbb{Z}$. On a $a + n\mathbb{Z} \in \mathbb{Z}_n^\times$ si et seulement si $a \wedge n = 1$.*

Démonstration. Supposons $a+n\mathbb{Z}$ inversible. Il existe $b \in \mathbb{Z}$ tel que $(a+n\mathbb{Z})(b+n\mathbb{Z}) = 1+n\mathbb{Z}$, ou encore $ab \equiv 1 \bmod n$. Il existe donc $v \in \mathbb{Z}$ tel que $ab - nv = 1$. Par le théorème de Bézout, $a \wedge n = 1$.

Inversement, supposons $a \wedge n = 1$. Par le théorème de Bézout, il existe $b, v \in \mathbb{Z}$ tels que $ab - nv = 1$. En passant aux classes, $(a + n\mathbb{Z})(b + n\mathbb{Z}) = 1 + n\mathbb{Z}$, donc $a \in \mathbb{Z}_n^\times$ et son inverse est $b + n\mathbb{Z}$. □

Le cardinal de $\mathbb{Z}_n^\times$ est donc $\varphi(n)$.

Proposition 16. *Si n est premier, alors $\mathbb{Z}_n$ est un corps. Sinon, $\mathbb{Z}_n$ n'est pas intègre.*

Démonstration. Supposons n premier. On a $|\mathbb{Z}_n^\times| = \varphi(n) = n - 1$, donc $\mathbb{Z}_n^\times = \mathbb{Z}_n \setminus \{n\mathbb{Z}\}$. Ainsi, $\mathbb{Z}_n$ est un corps.

Supposons $n = ab$ composé, où $a, b \neq 1, n$. En passant aux classes,

$$(a + n\mathbb{Z})(b + n\mathbb{Z}) = n\mathbb{Z}$$

Or, $a + n\mathbb{Z} \neq n\mathbb{Z}$ et $b + n\mathbb{Z} \neq n\mathbb{Z}$. Ainsi, $a + n\mathbb{Z}$ est un diviseur de zéro non nul dans l'anneau $n\mathbb{Z}$. □

La structure du groupe multiplicatif $\mathbb{Z}_n^\times$ est beaucoup plus subtile à étudier que celle du groupe additif $(\mathbb{Z}_n, +)$. Nous réservons cette étude à un autre article. Nous y démontrerons entre autres les résultats suivants.

• Si $n = p_1^{\alpha_1} \dots p_r^{\alpha_r}$ où les p_i sont des nombres premiers distincts et les α_i des entiers naturels non nuls, alors

$$\mathbb{Z}_n^\times \simeq \prod_{i=1}^{r} \mathbb{Z}_{p_i^{\alpha_i}}^\times$$

• Pour tout nombre premier impair p et tout entier naturel non nul α, le groupe $\mathbb{Z}_{p^\alpha}^\times$ est cyclique, isomorphe au groupe additif $\mathbb{Z}_{\varphi(p^\alpha}$, de cardinal $\varphi(p^\alpha) = p^{\alpha-1}(p-1)$ ·

• $\mathbb{Z}_2^\times$ et $\mathbb{Z}_4^\times$ sont de cardinal 1. Pour tout $\alpha \geq 3$, $\mathbb{Z}_{2^\alpha}$ n'est pas cyclique. C'est un groupe de cardinal $2^{\alpha-1}$ et on a l'isomorphisme

$$\mathbb{Z}_{2^\alpha}^\times \simeq \mathbb{Z}_{2^{\alpha-2}} \times \mathbb{Z}_2$$

• Le groupe $\mathbb{Z}_n^\times$ est cyclique si et seulement si $n = 4$ ou $n = p^\alpha$ ou $n = 2p^\alpha$, où p est un nombre premier impair et $\alpha \in \mathbb{N}$.