Chapitre 6
L'anneau $\mathbb{Z}/n\mathbb{Z}$

1°) L'addition dans $\mathbb{Z}/n\mathbb{Z}$

Soit $n \in \mathbb{N}$. Quelques exemples permettent de se rendre compte que la relation de "congruence modulo n" est compatible avec l'addition :

Proposition : Soit $(a, b, c, d) \in \mathbb{Z}^4$ et $n \in \mathbb{N}$, on a :

$$((a \equiv b\ [n]) \text{ et } (c \equiv d\ [n])) \Longrightarrow a+c \equiv b+d\ [n].$$

Preuve : D'après les hypothèses, il existe deux entiers k et k' tels que

$$a = b + kn \quad \text{et} \quad c = d + k'n.$$

On a donc :

$$a + c = b + d + n.(k+k') \qquad \square$$

Cette proposition permet de définir une loi de composition interne dans $\mathbb{Z}/n\mathbb{Z}$, que l'on va appeler addition et noter $+$, comme pour $\mathbb{Z}$:

Définition : l'addition dans $\mathbb{Z}/n\mathbb{Z}$ est la loi

$$+ : \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z} \longrightarrow \mathbb{Z}/n\mathbb{Z}$$

$$(x, y) \longrightarrow x + y = \overline{a+b}$$

où $a \in \mathbb{Z}$ est un représentant de x et $b \in \mathbb{Z}$ est un représentant de y.

Remarque : Cette définition de $x+y$ semble dépendre du représentant choisi de x et de y.

Montrons que ce n'est pas le cas :

si $c \in \mathbb{Z}$ un autre représentant de x et $d \in \mathbb{Z}$ un autre représentant de y.

on a $\overline{a} = \overline{c} = x$, donc $a \equiv c \ [n]$.

$\overline{b} = \overline{d} = y$, donc $b \equiv d \ [n]$.

D'après le lemme ci-dessus,

$$a + b \equiv c + d \ [n]$$

donc $\overline{a+b} = \overline{c+d}$. La classe $x+y$ est donc bien définie. □

On écrit parfois, plus simplement :

$$\begin{aligned} + : \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z} &\longrightarrow \mathbb{Z}/n\mathbb{Z} \\ (\overline{a}, \overline{b}) &\longrightarrow \overline{a} + \overline{b} = \overline{a+b} \end{aligned}$$

Propriétés de l'addition dans $\mathbb{Z}/n\mathbb{Z}$:

L'addition dans $\mathbb{Z}/n\mathbb{Z}$ hérite de beaucoup de propriété de l'addition des entiers ; elle est :

Commutative :

Soit $x, y \in (\mathbb{Z}/n\mathbb{Z})^2$; soit a un représentant de x et b un représentant de y, on a :

$$x + y = \overline{a+b} = \overline{b+a} = y + x.$$

Associativité : Soit $x = \bar{a}$, $y = \bar{b}$, $z = \bar{c}$ trois classes de $\mathbb{Z}/n\mathbb{Z}$, on a :

$$\begin{aligned}(x+y)+z &= \overline{a+b} + \bar{c} \\ &= \overline{(a+b)+c} \\ &= \overline{a+(b+c)} \\ &= \bar{a} + \overline{b+c} \\ &= x + (y+z).\end{aligned}$$

$\bar{0}$ est un élément neutre :

Soit $x = \bar{a}$ un élément de $\mathbb{Z}/n\mathbb{Z}$.

$$x + \bar{0} = \overline{a+0} = \bar{a} = x$$

$$\bar{0} + x = \overline{0+a} = \bar{a} = x.$$

Tout élément $\bar{a}$ a un opposé : Soit $x = \bar{a} \in \mathbb{Z}/n\mathbb{Z}$

Posons $x' = \overline{-a}$, alors

$$x + x' = \overline{a-a} = \bar{0} = x' + x$$

On pose $-x = \overline{-a}$.

Tout ceci montre :

Proposition : $\mathbb{Z}/n\mathbb{Z}$ muni de l'addition est un groupe abélien, son élément neutre est $\bar{0}$.

2°) La multiplication dans $\mathbb{Z}/n\mathbb{Z}$.

Proposition : La multiplication dans $\mathbb{Z}$ est compatible avec la relation de congruence modulo n :

Soit $n \in \mathbb{Z}$, $(a, b, c, d) \in \mathbb{Z}^4$, si $a \equiv b\ [n]$ et $c \equiv d\ [n]$, alors

$$ac \equiv bd\ [n].$$

Preuve : Il existe $k, k' \in \mathbb{Z}$ tels que

$$a = b + kn \quad \text{et} \quad c = d + k'n.$$

alors

$$ac = (b + kn)(c + k'n)$$
$$= bc + n.(bk' + kc + kk'n).$$

□

Ceci permet de définir une loi de composition interne dans $\mathbb{Z}/n\mathbb{Z}$ que l'on appelle "multiplication" et que l'on note $\times$ ou $\cdot$ ou "sans symbole" selon le contexte.

Définition : La multiplication dans $\mathbb{Z}/n\mathbb{Z}$ est la loi :

$$\begin{array}{rcl} \times : \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z} & \longrightarrow & \mathbb{Z}/n\mathbb{Z} \\ (x, y) & \longrightarrow & x \times y = \overline{ab} \end{array}$$

où $\bar{a} = x$, $a \in \mathbb{Z}$

$\bar{b} = y$, $b \in \mathbb{Z}$.

Remarque : Là encore, la proposition ci-dessus montre que $x \times y$ ne dépend pas du choix des représentants a et b de x et y.

Propriétés de la multiplication de $\mathbb{Z}/n\mathbb{Z}$:

La multiplication est :

associative,

commutative

possède un élément neutre $\overline{1}$.

est distributive sur l'addition.

On montrera tout cela en exercice.

Autrement dit :

Proposition : $(\mathbb{Z}/n\mathbb{Z}, +, \times)$ est un anneau commutatif.

Voici d'autres exemples d'anneaux :

$(\mathbb{R}, +, \times)$, $(\mathbb{Q}, +, \times)$, $(\mathbb{C}, +, \times)$

(où tout élément non nul possède un inverse pour $\times$).

$(\mathbb{Z}, +, \times)$

$(\mathcal{M}_n(\mathbb{R}), +, \times)$ (non commutatif).

3°) Inversibles de $\mathbb{Z}/n\mathbb{Z}$, le groupe $(\mathbb{Z}/n\mathbb{Z})^\times$.

Ecrivons la table de multiplication de $\mathbb{Z}/6\mathbb{Z}$:

	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$
$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$
$\bar{1}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$
$\bar{2}$	$\bar{0}$	$\bar{2}$	$\bar{4}$	$\bar{0}$	$\bar{2}$	$\bar{4}$
$\bar{3}$	$\bar{0}$	$\bar{3}$	$\bar{0}$	$\bar{3}$	$\bar{0}$	$\bar{3}$
$\bar{4}$	$\bar{0}$	$\bar{4}$	$\bar{2}$	$\bar{0}$	$\bar{4}$	$\bar{2}$
$\bar{5}$	$\bar{0}$	$\bar{5}$	$\bar{4}$	$\bar{3}$	$\bar{2}$	$\bar{1}$

On observe que le produit de certains éléments non nuls ($\bar{2}$ et $\bar{3}$ par exemple) peut être nul : l'anneau $\mathbb{Z}/n\mathbb{Z}$ n'est pas toujours intègre.

On observe par ailleurs qu'il existe des éléments ($\bar{3}$ par exemple) qui ne donnent jamais "$\bar{1}$" après multiplication par un autre nombre de $\mathbb{Z}/n\mathbb{Z}$. On

dit qu'ils ne sont pas inversibles.

Définition: Un élément $x \in \mathbb{Z}/n\mathbb{Z}$ est dit **inversible** s'il existe $y \in \mathbb{Z}/n\mathbb{Z}$ tel que

$$xy = yx = \overline{1}.$$

Exemples:

Dans $\mathbb{Z}/6\mathbb{Z}$, $\overline{1}$ et $\overline{5}$ sont inversibles; $\overline{0}, \overline{2}, \overline{3}, \overline{4}$ ne sont pas inversibles.

Si $x \in \mathbb{Z}/n\mathbb{Z}$ est inversible, il existe un unique $y \in \mathbb{Z}/n\mathbb{Z}$ tel que $xy = \overline{1}$.

(preuve: Si $xy = \overline{1}$ et $xy' = \overline{1} = y'x$, on multiplie la première égalité à gauche pour obtenir:

$(y'x)y = y' \Rightarrow y = y'$).

L'unique y tel que $xy = yx = \overline{1}$ est appelé l'inverse de x. On le note parfois y^{-1} mais pas $1/y$ qui

fait trop référence aux fractions dans $\mathbb{Q}$ et créerait trop de confusions.

Notation : L'ensemble des éléments inversibles de $\mathbb{Z}/n\mathbb{Z}$ est noté $(\mathbb{Z}/n\mathbb{Z})^\times$.

Le produit de deux inversibles est un inversible et $(\mathbb{Z}/n\mathbb{Z})^\times$ est un groupe pour la multiplication, dont l'élément neutre est $\bar{1}$.

Exemples :

$(\mathbb{Z}/2\mathbb{Z})^\times = \{\bar{1}\}$

$(\mathbb{Z}/6\mathbb{Z})^\times = \{\bar{1}, \bar{5}\}$.

Proposition : Soit $n \in \mathbb{N}^*$, $a \in \mathbb{Z}$.
$\bar{a}$ est inversible dans $\mathbb{Z}/n\mathbb{Z}$ ssi $\text{pgcd}(a, n) = 1$.

Preuve :

supposons $\bar{a}$ inversible.

Soit $\bar{b}$ sont inverse. On a : $\bar{a}.\bar{b} = \bar{1}$,

donc $ab \equiv 1 \ [n]$.

Il existe donc $k \in \mathbb{Z}$ tel que

$$ba + kn = 1.$$

D'après le théorème de Bezout, $a \wedge n = 1$.

supposons que $a \wedge n = 1$.

D'après le théorème de Bezout, il existe $u, v \in \mathbb{Z}$ tels que :

$$ua + vn = 1$$

ce qui implique :

$$\bar{u}\bar{a} + \bar{v}\underbrace{\bar{n}}_{\bar{0}} = \bar{1}$$

$$\Rightarrow \bar{u}\bar{a} = \bar{1}$$

donc $\bar{a}$ est inversible, et son inverse est $\bar{u}$. □

Remarque: Cette preuve fournit aussi une méthode pour calculer l'inverse d'un élément de $\mathbb{Z}/n\mathbb{Z}$, à l'aide de l'algorithme d'Euclide augmenté qui permet de trouver les coefficients de Bezout.

Définition: Un corps est un anneau dont tous les éléments non nuls sont inversibles.

Propriété : $\mathbb{Z}/n\mathbb{Z}$ est un corps ssi n est premier.

Preuve :

Supposons que n est premier :

Soit $\bar{a} \in \mathbb{Z}/n\mathbb{Z}$.

Si $a \wedge n \neq 1$, alors $a \wedge n = n$ et n divise a, donc $\bar{a} = \bar{0}$.

D'après la propriété ci-dessus, si $\bar{a} \neq \bar{0}$, $a \wedge n = 1$ et $\bar{a}$ est

inversible.

Supposons que $\mathbb{Z}/n\mathbb{Z}$ est un corps.

Si n n'est pas premier, écrivons $n = ab$ avec $1 < a, b < n$.

Alors $a \wedge n = a \neq 1$, donc $\bar{a}$ n'est pas inversible et $\bar{a} \neq \bar{0}$ ce qui contredit l'hypothèse. □

Notation: Soit p un nombre premier.

L'anneau $\mathbb{Z}/p\mathbb{Z}$ est souvent noté $\mathbb{F}_p$.

Le terme mathématique anglais "Field" signifie "corps" (au sens mathématique !).

4°/ Le petit théorème de Fermat.

Théorème (version 1): Soit p un nombre premier

$$\forall x \in \mathbb{Z}/p\mathbb{Z}, \quad x^p = x.$$

Avant de démontrer ce résultat, donnons en des énoncés équivalents:

Théorème (version 2): Soit p un nombre premier et $x \in \mathbb{Z}/p\mathbb{Z}$

Si $x \neq \bar{0}$, alors $x^{p-1} = \bar{1}$.

Théorème (version 3): Soit p un nombre premier et $a \in \mathbb{Z}$, alors:

$$a^p \equiv a \ [p].$$

Théorème (version 4): Soit p un nombre premier et $a \in \mathbb{Z}$, alors:

Si $p \nmid a$, $\quad a^{p-1} \equiv 1 \ [p]$

Exercice : démontrer que ces quatre énoncés sont équivalents.

Avant de démontrer le petit théorème de Fermat, nous prouvons une propriété fondamentale des corps $\mathbb{F}_p$:

Proposition : Soit p premier et $x, y \in \mathbb{F}_p$. Alors :

$$(x+y)^p = x^p + y^p .$$

Preuve : Soient $a, b \in \mathbb{Z}$ des représentants de x et y : $x = \bar{a}$ et $y = \bar{b}$.

On a :

$$(x+y)^p = (\bar{a} + \bar{b})^p$$

$$= (a+b)^p .$$

$$= \sum_{k=0}^{p} \binom{p}{k} a^k b^{p-k}$$

$$= \sum_{k=0}^{p} \overline{\binom{p}{k}} \bar{a}^k \bar{b}^{p-k}$$

$$= x^p + \sum_{k=1}^{p-1} \overline{\binom{p}{k}} x^k y^{p-k} + y^p$$

Mais on a vu dans le chapitre sur le lemme de Gauss que $\overline{\binom{p}{k}} = \bar{0}$ si $0 < k < p$.

donc $(x+y)^p = x^p + y^p$. □

Remarque : Ce résultat est faux si p n'est pas premier.

Par exemple dans $\mathbb{Z}/4\mathbb{Z}$:

$(\bar{1}+\bar{1})^4 = \bar{2}^4 = \overline{16} = \bar{0} \neq \bar{1}^4 + \bar{1}^4$.

Preuve du petit théorème de Fermat :

Soit $a \in \mathbb{N}$, on va montrer par récurrence sur a que $\bar{a}^p = \bar{a}$.

- Si $a = 0$, c'est évident,
- Si le résultat est vrai pour a, on a :

$$\overline{a+1}^p = \bar{a}^p + \bar{1}^p \quad \text{(propriété ci-dessus)}$$
$$= \bar{a} + \bar{1} \quad \text{(récurrence)}$$
$$= \overline{a+1}.$$

□