Chapitre 1

L'anneau $\mathbb{Z}$

1 La structure d'anneau de $\mathbb{Z}$

L'ensemble $\mathbb{Z}$ des entiers relatifs est muni d'une addition et d'une multiplication qui vérifient les propriétés suivantes :

1) L'addition est une *loi de composition interne* :

$$\forall (a,b) \in \mathbb{Z}^2 \ , \ a+b \in \mathbb{Z}$$

2) L'addition est *associative* :

$$\forall (a,b,c) \in \mathbb{Z}^3 \ , \ a+(b+c) = (a+b)+c$$

3) 0 est un *élément neutre* pour l'addition :

$$\forall a \in \mathbb{Z} \ , \ a+0 = 0+a = a$$

4) *Tout élément admet un opposé* pour l'addition :

$$\forall a \in \mathbb{Z} \ , \ a+(-a) = (-a)+a = 0$$

On résume les propriétés 1) à 4) en disant que $(\mathbb{Z},+)$ est un ***groupe***.

Qui plus est :

5) L'addition est *commutative* :

$$\forall (a,b) \in \mathbb{Z}^2 \ , \ a+b = b+a$$

En résumé, on dit que $(\mathbb{Z},+)$ est un groupe *commutatif* (ou *abélien*).

Pour ce qui est de la multiplication, elle possède les propriétés suivantes :

1) C'est une loi de composition interne : $\forall (a,b) \in \mathbb{Z}^2$, $a \cdot b \in \mathbb{Z}$

2) Elle est associative : $\forall (a,b,c) \in \mathbb{Z}^3$, $a \cdot (b \cdot c) = (a \cdot b) \cdot c$

3) Elle possède un élément neutre (l'entier 1) : $\forall a \in \mathbb{Z}$, $a \cdot 1 = 1 \cdot a = a$

4) Elle est *distributive par rapport à l'addition*, ce qui signifie que

$$\forall (a,b,c) \in \mathbb{Z}^3 \text{ , } a \cdot (b+c) = a \cdot b + a \cdot c.$$

On dit que $(\mathbb{Z}, +, \cdot)$ est un *anneau*.

2 Entiers relatifs et arithmétique

2.1 Division euclidienne

Théorème 1
Pour tout couple d'entiers naturels (a,b) avec $b \neq 0$, il existe un unique couple (q,r) d'entiers naturels tels que

$$\begin{cases} a = bq + r \\ 0 \leq r < b \end{cases} \tag{1.1}$$

Les entiers q et r sont respectivement le quotient et le reste de la division euclidienne de a par b.

Preuve. Pour l'existence, on considère l'ensemble $E = \{q \in \mathbb{N} \mid bq \leq a\}$; comme partie non vide et majorée de $\mathbb{N}$, il admet un plus grand élément q. On pose alors $r := a - bq$. Clairement, on a $0 \leq a - bq < b$, donc le couple (q,r) satisfait 1.1. Pour l'unicité, on suppose qu'il existe un autre couple (q',r') tel que

$$\begin{cases} a = bq' + r' \\ 0 \leq r' < b. \end{cases} \tag{1.2}$$

En particulier, $bq' = a - r' \leq a$, donc $q' \in E$, et par conséquent $q' \leq q = \max E$. Si q' était distinct de q, il serait au plus égal à $q-1$, et on aurait

$$r' = a - bq' \geq a - bq + b = r + b \geq b,$$

une contradiction. Donc $q' = q$ et par suite $r' = r$. □
La division euclidienne s'étend sans difficulté à l'ensemble $\mathbb{Z}$ des entiers relatifs :

Théorème 2
Pour tout couple d'entiers relatifs (a,b) avec $b \neq 0$, il existe un unique couple (q,r) d'entiers relatifs tels que

$$\begin{cases} a = bq + r \\ 0 \leq r < |b|. \end{cases} \tag{1.3}$$

2.2 Divisibilité

Définition 1
Soit a et b deux entiers relatifs, avec b non nul. On dit que "b divise a" ou que "a est un multiple de b" et on écrit "$b \mid a$" s' il existe $q \in \mathbb{Z}$ tel que $a = bq$.

Remarque : b divise a si et seulement si le reste de la division euclidienne de a par b est nul.

2.3 PGCD, PPCM

Définition 2

1) *Le PGCD de deux entiers relatifs a et b non tous les deux nuls est l'entier d défini par :*

$$d := \max \{k \in \mathbb{N}^* \mid k \text{ divise } a \text{ et } b\}$$

2) *Le PPCM de deux entiers relatifs a et b non nuls est l'entier m défini par :*

$$m := \min \{k \in \mathbb{N}^* \mid k \text{ est un multiple commun à } a \text{ et } b\}$$

2.4 Sous groupes de $\mathbb{Z}$ et théorème de Bézout

Définition 3
Un sous-groupe *de $\mathbb{Z}$ est une partie non vide et "stable par addition et soustraction". Plus précisément, $F \subset \mathbb{Z}$ est un sous-groupe si*

1) *$F \neq \emptyset$,*

2) *pour tout élément x de F et tout élément y de F, la différence $x - y$ appartient à F.*

Remarques : si F est un sous-groupe de $\mathbb{Z}$ alors

1) 0 appartient à F.

2) Si $x \in F$ alors $-x \in F$.

3) Plus généralement, si $x \in F$ alors $kx \in F$ pour tout $k \in \mathbb{Z}$.

Notation : si a est un entier (quelconque), on note $a\mathbb{Z}$ l'ensemble de ses multiples. Autrement dit

$$a\mathbb{Z} = \{am, m \in \mathbb{Z}\} = \{n \in \mathbb{Z} \mid \exists m \in \mathbb{Z}, n = am\}.$$

De même, si a et b sont deux entiers, on définit

$$a\mathbb{Z} + b\mathbb{Z} = \{ax + by, x, y \in \mathbb{Z}\} = \{n \in \mathbb{Z} \mid \exists x, y \in \mathbb{Z} \in \mathbb{Z}, n = ax + by\}.$$

Proposition 1

1) *Pour tout entier a, l'ensemble $a\mathbb{Z}$ est un sous-groupe de $\mathbb{Z}$.*

2) *Si a et b sont des entiers, on a l'équivalence : $a\mathbb{Z} \subset b\mathbb{Z} \Leftrightarrow b$ divise a.*

3) *Si a et b sont des entiers, l'ensemble $a\mathbb{Z} + b\mathbb{Z}$ est un sous-groupe de $\mathbb{Z}$.*

Théorème 3
Soit F un sous-groupe de $\mathbb{Z}$. Alors, il existe un unique entier naturel g tel que $F = g\mathbb{Z}$.

Preuve. Si $F = \{0\}$ alors $g = 0$ convient. Sinon, F contient un élément non nul x, ainsi que son opposé $-x$, donc il contient un élément strictement positif. Par conséquent, l'ensemble $F_+ = \{x \in F \mid x > 0\} \subset \mathbb{N}$ est non vide. Il admet donc, comme toute partie non vide de $\mathbb{N}$, un plus petit élément noté g. Clairement, g appartient à F, ainsi que tous ses multiples, donc $g\mathbb{Z} \subset F$. Inversement, si a est un élément (quelconque) de F, on peut effectuer la division euclidienne de a par g :

$$a = gq + r\ , \ \text{ avec } q, r \in \mathbb{Z} \text{ et } 0 \leq r < g.$$

On en déduit que $r = a - qg$ appartient à F, comme différence de deux éléments de F. S'il était > 0, cela contredirait la définition de g, donc $r = 0$, ce qui signifie que $a \in g\mathbb{Z}$. □

Corollaire 1
Soient a et b deux entiers non tous les deux nuls. On note d leur PGCD et m leur PPCM.

1) *$a\mathbb{Z} + b\mathbb{Z} = d\mathbb{Z}$ et $a\mathbb{Z} \cap b\mathbb{Z} = m\mathbb{Z}$.*

2) *(Théorème de Bézout) Si $\mathrm{PGCD}(a, b) = d$ alors il existe deux entiers u et v tels que*

$$au + bv = d.$$

3) *Le PGCD de a et b est le "plus grand diviseur commun" à a et b au sens de la relation d'ordre usuelle sur $\mathbb{Z}$, mais également au sens de la relation de divisibilité.*

4) *Le PPCM de a et b est le "plus petit multiple commun" à a et b au sens de la relation d'ordre usuelle sur $\mathbb{Z}$ et au sens de la relation de divisibilité.*

Remarque : on peut donc définir le PGCD (resp. le PPCM) de deux entiers a et b comme le générateur positif du sous-groupe $a\mathbb{Z} + b\mathbb{Z}$ (resp. $a\mathbb{Z} \cap b\mathbb{Z}$). Si l'on adopte ce point de vue il n'y a plus lieu de conserver la restriction à *"a et b non tous les deux nuls"* dans la définition du PGCD et du PPCM, et on peut donc éventuellement poser $\mathrm{PGCD}(0, 0) = \mathrm{PPCM}(0, 0) = 0$.

2.5 Algorithme d'Euclide

Proposition 2
Soient a et b deux entiers, avec $b \neq 0$. Si r est le reste de la division euclidienne de a par b alors

$$\mathrm{PGCD}(a, b) = \mathrm{PGCD}(b, r).$$

Voici le principe de l'algorithme d'Euclide : soient a et b deux entiers positifs ; on pose $r_0 = a$ et $r_1 = b$, puis pour $k \geq 1$, **tant que** $r_k > 0$, on définit r_{k+1} comme le reste de la division euclidienne de r_{k-1} par r_k. En particulier, on a $r_{k+1} < r_k$ si r_k est non nul. La suite ainsi construite est donc strictement décroissante, ce qui garantit que l'algorithme s'arrête. On vérifie alors, en utilisant la Proposition 2, que le dernier terme non nul de la suite est le PGCD de a et b.

Entrées : a,b entiers naturels
Sorties : PGCD de a et b
tant que $b > 0$ **faire**
    $r \leftarrow a\%b$ `/* reste de la division euclidienne de` a `par` b `*/`
    $a \leftarrow b$
    $b \leftarrow r$
fin
retourner a

Algorithme 1 : Algorithme d'Euclide

Voici maintenant une variante de l'algorithme d'Euclide qui permet de déterminer le PGCD de deux entiers a et b ainsi que deux entiers u et v tels que $au + bv = \mathrm{PGCD}(a, b)$. Cette variante est généralement appelée *algorithme d'Euclide étendu*.
On définit récursivement des entiers u_k et v_k de la façon suivante : on pose $u_0 = 1$, $v_0 = 0$, $u_1 = 0$, $v_1 = 1$ et pour $k \geq 1$

$$\begin{cases} u_{k+1} = u_{k-1} - u_k q_k \\ v_{k+1} = v_{k-1} - v_k q_k \end{cases}$$

On vérifie alors par récurrence sur k, que les entiers u_k et v_k ainsi définis vérifient la relation

$$r_k = au_k + bv_k$$

pour tout $k \geq 0$. En particulier, si n est l'indice du dernier reste non nul, on obtient

$$d = r_n = au_n + bv_n.$$

Entrées : a,b entiers naturels
Sorties : $d = \text{PGCD}(a,b)$ et $(u,v) \in \mathbb{Z}^2$ tel que $d = au + bv$
$u \leftarrow 1$
$v \leftarrow 0$
$s \leftarrow 0$
$t \leftarrow 1$
tant que $b > 0$ **faire**
  $q \leftarrow a/b$ `/* quotient de la division euclidienne de` a `par` b `*/`
  $r \leftarrow a\%b$ `/* reste de la division euclidienne de` a `par` b `*/`
  $a \leftarrow b$
  $b \leftarrow r$
  $X \leftarrow s$
  $s \leftarrow u - qs$
  $u \leftarrow X$
  $X \leftarrow t$
  $t \leftarrow v - qt$
  $v \leftarrow X$
fin
retourner a, u, v

Algorithme 2 : Algorithme d'Euclide étendu

Remarque : l'algorithme précédent fournit une preuve *constructive* du théorème de Bézout, à l'inverse de l'approche par les sous-groupes (§2.4) qui prouve l'existence d'une relation de Bézout mais ne donne aucun moyen d'en déterminer une.

2.6 Compléments

Dans ce paragraphe, on notera $a \wedge b$ le PGCD de deux entiers a et b, et $a \vee b$ leur PPCM. On dit que a et b sont *premiers entre eux* si $a \wedge b = 1$.

Théorème 4
Deux entiers a et b sont premiers entre eux si et seulement s'il existe deux entiers u et v tels que

$$au + bv = 1.$$

Proposition 3 (*Lemme de Gauss*)
Soient a, b et c trois entiers. Si a divise bc et $a \wedge b = 1$ *alors a divise c.*

Proposition 4
Soient a, b et c trois entiers.
a) *Si a divise c et b divise c et si* $a \wedge b = 1$ *alors ab divise c.*
b) *Si* $a \wedge b = 1$ *et* $a \wedge c = 1$ *alors* $a \wedge bc = 1$.
c) *Si p est un nombre premier et si p divise ab alors p divise a ou p divise b.*

3 Congruences

Dans toute la suite, n désigne un entier naturel non nul fixé.

3.1 Définitions et premières propriétés

Définition 4
On dit que deux entiers relatifs a et b sont congrus modulo n ou encore que a est congru à b modulo n si n divise $a - b$. On notera $a \equiv b \mod n$ ou $a \equiv b\ [n]$.

Proposition 5
La relation de congruence modulo n vérifie les propriétés suivantes

1) $\forall a \in \mathbb{Z} \quad a \equiv a \mod n$ *("Réfléxivité"),*

2) $\forall (a,b) \in \mathbb{Z}^2 \quad a \equiv b \mod n \iff b \equiv a \mod n$ *("Symétrie"),*

3) $\forall (a,b,c) \in \mathbb{Z}^3 \quad (a \equiv b \mod n \wedge b \equiv c \mod n) \Rightarrow a \equiv c \mod n$ *("Transitivité").*

On dit que la relation de congruence est une ***relation d'équivalence*** *sur l'ensemble des entiers.*

Proposition 6
Pour tout entier relatif a, il existe un unique entier naturel $r \in \{0, \ldots, n-1\}$ tel que $n \equiv r \mod n$

Preuve. Il suffit de considérer le reste de la division euclidienne de a par n. □

Définition 5
Pour tout $a \in \mathbb{Z}$, on note $a + n\mathbb{Z}$ ou $\overline{a}$ la classe de congruence de a modulo n, c'est-à-dire

$$a + n\mathbb{Z} = \overline{a} := \{b \in \mathbb{Z} \mid b \equiv a \mod n\}.$$

On note $\mathbb{Z}/n\mathbb{Z}$ l'ensemble des classes de congruence modulo n.

La Proposition 6 admet le corollaire suivant :

Corollaire 2
$\mathbb{Z}/n\mathbb{Z} = \{\overline{0}, \overline{1}, \ldots, \overline{n-1}\}$.

Proposition 7
Soit n un entier naturel non nul. On note a, b, a' et b' quatre entiers relatifs. On a les propriétés suivantes : si $a \equiv b \mod n$ et $a' \equiv b' \mod n$ alors

$$a + a' \equiv b + b' \mod n \qquad a - a' \equiv b - b' \mod n \qquad aa' \equiv bb' \mod n$$

Remarque : On dit que la relation de congruence est compatible avec l'addition, la soustraction et la multiplication définies sur $\mathbb{Z}$.
La Proposition7 permet en particulier de munir l'ensemble quotient $\mathbb{Z}/n\mathbb{Z}$ d'une addition et d'une multiplication définies comme suit.

Définition 6
Soient $\overline{x}$ et $\overline{y}$ deux éléments de $\mathbb{Z}/n\mathbb{Z}$. On pose :

1) *(Addition) $\overline{x} + \overline{y} := \overline{s}$, où s désigne le reste de la division euclidienne de $x + y$ par n,*

2) *(Multiplication) $\overline{x}\ \overline{y} := \overline{p}$, où p désigne le reste de la division euclidienne de xy par n.*

Muni de ces deux opérations, l'ensemble $\mathbb{Z}/n\mathbb{Z}$ a une structure d'anneau.
Pour illustrer cette construction, on donne ci-dessous les tables d'addition et de multiplication de $\mathbb{Z}/3\mathbb{Z}$:

$+$	$\overline{0}$	$\overline{1}$	$\overline{2}$
$\overline{0}$	$\overline{0}$	$\overline{1}$	$\overline{2}$
$\overline{1}$	$\overline{1}$	$\overline{2}$	$\overline{0}$
$\overline{2}$	$\overline{2}$	$\overline{0}$	$\overline{1}$

$\times$	$\overline{0}$	$\overline{1}$	$\overline{2}$
$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$
$\overline{1}$	$\overline{0}$	$\overline{1}$	$\overline{2}$
$\overline{2}$	$\overline{0}$	$\overline{2}$	$\overline{1}$

3.2 Le groupe $(\mathbb{Z}/n\mathbb{Z}, +)$

Proposition 8
L'ensemble $\mathbb{Z}/n\mathbb{Z}$, muni de l'addition définie ci-dessus est un groupe commutatif, d'élément neutre $\overline{0}$. L'opposé d'un élément $x = \overline{k}$ de $\mathbb{Z}/n\mathbb{Z}$ est égal à $\overline{-k}$:

$$-\overline{k} = \overline{-k}.$$

Soit x un élément de $Z/n\mathbb{Z}$; il existe donc un entier k tel que $x = \overline{k}$. Si ℓ est un entier naturel, il est naturel de noter "ℓx" la somme $\underbrace{x + x + \cdots + x}_{\ell \text{ fois}}$.
En vertu de la compatibilité de l'addition dans $\mathbb{Z}$ et de la relation de congruence, on a donc

$$\ell\overline{k} = \underbrace{\overline{k} + \overline{k} + \cdots + \overline{k}}_{\ell \text{ fois}} = \overline{\ell k}. \tag{1.4}$$

Si ℓ est un entier négatif, alors $-\ell$ est un entier naturel et

$$\ell\overline{k} = -(-\ell)\overline{k} = -\overline{(-\ell)k} = \overline{\ell k}.$$

En résumé :

Proposition 9

$$\forall \ell \in \mathbb{Z}\ ,\ \forall k \in \mathbb{Z}, \ell\overline{k} = \overline{\ell k}.$$

Pour finir, introduisons la notion d'ordre d'un élément

Proposition 10
Pour tout élément $\overline{k}$ de $\mathbb{Z}/n\mathbb{Z}$, il existe un plus petit entier naturel non nul r tel que

$$r\overline{k} = \overline{0}.$$

Cet entier s'appelle ***l'ordre de*** $\overline{k}$ ***dans*** $\mathbb{Z}/n\mathbb{Z}$.
C'est aussi le ***plus petit entier naturel non nul*** r ***tel que*** n ***divise*** rk.

Preuve. Observons tout d'abord que les propriétés *"n divise rk"* et *"$r\overline{k} = \overline{0}$"* sont équivalentes, puisque $r\overline{k} = \overline{rk}$. Ainsi, le *"plus petit entier naturel non nul r tel que $r\overline{k} = \overline{0}$"*, s'il existe, est aussi le *"plus petit entier naturel non nul r tel que n divise rk"*.

Considérons alors l'ensemble $\{\ell k, \ell \in \mathbb{Z}\}$. C'est clairement un ensemble infini. Comme l'ensemble des restes modulo n est lui fini, il existe donc deux entiers distincts $p < q$ tels que pk et qk aient même reste modulo n, autrement dit

$$pk \equiv qk \mod n$$

c'est-à-dire

$$(q-p)k \equiv 0 \mod n$$

ou encore

$$n \text{ divise } (q-p)k.$$

L'ensemble E des entiers $r > 0$ tels que n divise rk contient donc au moins l'élément $q - p$. C'est donc une partie non vide de $\mathbb{N} \setminus \{0\}$, qui possède donc un plus petit élément r_0

$$r_0 = \min \{r \in \mathbb{N} \setminus \{0\} \text{ tels que } n \text{ divise } rk\}.$$

□