Chapitre 3

Entiers

Le but de ce chapitre est de rappeler les propriétés essentielles de l'ensemble $\mathbb{N}$ des entiers naturels. On s'en tiendra à une présentation "intuitive", basée sur les connaissances du lycée et du collège et en particulier on se gardera de toute "construction". En revanche, on pourra mettre l'accent sur les propriétés "axiomatiques", qui permettent entre autres de donner un fondement un peu rigoureux au raisonnement par récurrence, à la division euclidienne etc.

3.1 Entiers naturels.

On admet l'existence d'un ensemble ordonné non vide $(\mathbb{N}, \leq)$ non vide vérifiant les trois propriétés suivantes :

(N1) Toute partie non vide de $\mathbb{N}$ possède un plus petit élément.

(N2) Toute partie non vide et *majorée* de $\mathbb{N}$ possède un plus grand élément.

(N3) L'ensemble $\mathbb{N}$ lui-même n'est pas majoré (en particulier, il ne possède pas de plus grand élément).

On ne cherchera pas à construire l'addition et la multiplication (c'est non trivial). En revanche, il peut être utile d'indiquer quelques conséquences faciles (et utiles) des axiomes (N1), (N2) et (N3). C'est l'objet des deux sous-paragraphes suivants.

3.1.1 Raisonnement par récurrence.

Théorème 19. Soit n_0 un entier, et $\mathcal{P}(n)$ une propriété de l'entier n, définie pour tout $n \geq n_0$. On fait les hypothèses suivantes :

(R1) La propriété $\mathcal{P}(n_0)$ est vraie.

(R2) Pour tout $n \geq n_0$, si la propriété $\mathcal{P}(n)$ est vraie alors la propriété $\mathcal{P}(n+1)$ est vraie.

Sous ces hypothèses, la propriété $\mathcal{P}(n)$ est vraie pour tout $n \geq n_0$.

Preuve. Par l'absurde, on suppose que l'ensemble $E := \{m \geq n_0 \mid \mathcal{P}(m) \text{ fausse }\}$ est non vide. Il admet alors un plus petit élement n par (N1), qui est strictement plus grand que n_0 à cause de (R1). Par suite $n-1 \notin E$ et $\mathcal{P}(n-1)$ est vraie. Mais n est *strictement* supérieur à n_0 donc $n-1 \geq n_0$ et $\mathcal{P}(n)$ est donc vraie à cause de (R2), contradiction. □

Variante (*"Récurrence forte"*) : dans le théorème précédent, on peut remplacer (R2) par l'hypothèse (R3) suivante

(R3) Pour tout $n \geq n_0$, si $\mathcal{P}(k)$ est vraie pour tout $n_0 \leq k \leq n$, alors $\mathcal{P}(n+1)$ est vraie. La conclusion est alors la même.

Deuxième variante (*"Récurrence descendante"*) :

Proposition 20. Soit Soit n_0 un entier non nul, et $\mathcal{P}(n)$ une propriété de l'entier n, définie pour tout $n \leq n_0$. On suppose que

(RD1) La propriété $\mathcal{P}(n_0)$ est vraie.

(RD2) Pour tout entier $n \in \{1, \dots n_o\}$, si la propriété $\mathcal{P}(n)$ est vraie, alors la propriété $\mathcal{P}(n-1)$ est vraie.

Sous ces hypothèses, la propriété $\mathcal{P}(n)$ est vraie pour tout $0 \leq n \leq n_0$.

3.1.2 Division euclidienne

Théorème 21. Pour tout couple d'entiers naturels (a, b) avec $b \neq 0$, il existe un unique couple (q, r) d'entiers naturels tels que

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

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

Preuve. Pour l'existence, appliquer l'axiome (N1) à l'ensemble $\{q \in \mathbb{N} \mid bq > a\}$ ou bien l'axiome (N2) à l'ensemble $\{q \in \mathbb{N} \mid bq \leq a\}$... □

On peut de la même façon justifier l'existence de PPCM, PGCD et démontrer quelques unes de leur propriétés. Par exemple, on peut définir le PPCM de deux entiers naturels a et b comme le minimum de l'ensemble $\{m \in \mathbb{N} \mid a \text{ divise } m \text{ et } b \text{ divise } m\}$ grâce à l'axiome (N1), puis montrer que tout multiple commun à a et b est un multiple du PPCM (ce qui n'est pas contenu dans la définition que l'on vient de donner), en utilisant la division euclidienne.

3.2 Entiers relatifs et arithmétique

Pour introduire l'ensemble $\mathbb{Z}$ des entiers relatifs, on pourra s'en tenir à une présentation "intuitive", ou bien (mieux !) utiliser la construction classique comme quotient de $\mathbb{N} \times \mathbb{N}$ par une relation d'équivalence *ad hoc* : $\mathbb{Z} = \mathbb{N} \times \mathbb{N}/\mathfrak{R}$, la relation $\mathfrak{R}$ étant définie par

$$(n_1, n_2)\ \mathfrak{R}\ (n_1', n_2') \text{ si } n_1 + n_2' = n_2 + n_1'.$$

3.2.1 PGCD, PPCM, théorème de Bézout

Définition 3.1. 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 :

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

Définition 3.2. 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 aa 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 22.

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.

Théorème 23. 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 :

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

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 $a \in g\mathbb{Z}$. □

Proposition 24. Soient a et b deux entiers non tous les deux nuls. On note d leur PGCD et m leur PPCM. Alors

1. $a\mathbb{Z} + b\mathbb{Z}$ et $a\mathbb{Z} \cap b\mathbb{Z}$ sont des sous-groupes de $\mathbb{Z}$.
2. $a\mathbb{Z} + b\mathbb{Z} = d\mathbb{Z}$ et $a\mathbb{Z} \cap b\mathbb{Z} = m\mathbb{Z}$.

Preuve.

1. Clair

2. Soit c l'unique entier positif tel que $a\mathbb{Z} + b\mathbb{Z} = c\mathbb{Z}$. Puisque a et b appartiennent à $a\mathbb{Z} + b\mathbb{Z} = c\mathbb{Z}$, on peut affirmer que c divise a et b, donc $c \leq d$ par définition du PGCD. Inversement, puisque d divise a et b, on a les inclusions $a\mathbb{Z} \subset d\mathbb{Z}$ et $b\mathbb{Z} \subset d\mathbb{Z}$, et donc

$$c\mathbb{Z} = a\mathbb{Z} + b\mathbb{Z} \subset d\mathbb{Z}$$

ce qui implique que d divise c et en particulier $d \leq c$. Par conséquent, $d = c$. Démonstration analogue pour le PPCM.

□

Corollaire 25 (Théorème de Bézout)**.** Soient a et b deux entiers non tous les deux nuls. Si $\text{pgcd}(a, b) = d$ alors il existe deux entiers u et v tels que

$$au + bv = d.$$

Remarque : La relation dans le théorème ci-dessus est appelée *une identité de Bézout.*

3.2.2 Algorithme d'Euclide

Proposition 26. Soient a et b deux entiers, avec $b \neq 0$. Si r est le reste de la division euclidienne de a par b alors

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

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 tant que $r_i > 0$ on effectue les divisions euclidiennes suivantes :

$$\begin{cases} r_0 = r_1 q_1 + r_2 & \text{où} \quad 0 \leq r_2 < r_1 \\ r_1 = r_2 q_2 + r_3 & \text{où} \quad 0 \leq r_3 < r_2 \\ \quad \cdots & \cdots \quad \cdots \\ r_{k-2} = r_{k-1} q_{k-1} + r_k & \text{où} \quad 0 \leq r_k < r_{k-1} \\ r_{k-1} = r_k q_k + r_{k+1} & \text{où} \quad 0 \leq r_{k+1} < r_k \end{cases}$$

Il résulte de la proposition ci-dessus que pour chaque $k \geq 0$, on a $\text{PGCD}(a, b) = \text{PGCD}(r_k, r_{k+1})$. La suite des restes $(r_1, r_2, r_3, \dots)$ étant une suite strictement décroissante d'entiers positifs, on obtient nécessairement un reste nul au bout d'un nombre fini de divisions. Soit r_n le dernier reste non nul. On a donc $r_{n+1} = 0$ et par conséquent :

$$\text{PGCD}(a, b) = \text{PGCD}(r_n, r_{n+1}) = \text{PGCD}(r_n, 0) = r_n.$$

Voici un algorithme qui permet de déterminer le $\text{PGCD}(a, b) = d$ ainsi que deux entiers u et v tels que $au + bv = d$, c'est-à-dire une version "effective" du théorème de Bézout. Il est généralement appelé *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

$$\text{pgcd}(a, b) = r_n = au_n + bv_n.$$

3.2.3 Compléments *(facultatif)*

Théorème 27. Les entiers a et b sont premiers entre eux ($\text{pgcd}(a,b) = 1$) si et seulement s'il existe deux entiers u et v tels que

$$au + bv = 1.$$

Proposition 28. *Lemme de Gauss* Soient a, b et c trois entiers. Si a divise bc et a premier avec b alors a divise c.

Proposition 29. Soient a, b et c trois entiers.
a) Si a divise c et b divise c et si $(a,b) = 1$ alors ab divise c.
b) Si $(a,b) = 1$ et si $(a,c) = 1$ alors $(a,bc) = 1$.
c) Si p est un nombre premier et si p divise ab alors p divise a ou p divise b.

Théorème 30. Tout entier $a > 1$ s'écrit de manière unique

$$a = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}$$

où $\begin{cases} \text{les entiers } p_i \text{ sont premiers et vérifient } p_1 < p_2 < \cdots < p_k \\ \text{les entiers } \alpha_i \text{ sont strictement positifs} \end{cases}$

Preuve. Pour l'unicité, on utilise le lemme de Gauss. □