Université de Provence 2009–2010

Mathématiques Générales 1 - Parcours PEI

Anneaux, Corps, $\mathbb{Z}/n\mathbb{Z}$.

1 Anneaux, Corps.

1.1 Définitions.

Définition. Soit A un ensemble muni de deux lois de composition interne, $+$ et $\cdot$. On dit que A est un *anneau* si et seulement si $(A,+)$ est un groupe commutatif, $\cdot$ est une loi de composition interne associative et de plus,

$$\forall (x,y,z) \in A^3 \qquad x \cdot (y+z) = x \cdot y + x \cdot z$$

$$\forall (x,y,z) \in A^3 \qquad (y+z) \cdot x = y \cdot x + z \cdot x.$$

On dit alors que la multiplication est *distributive* par rapport à l'addition. On dit aussi que $(A,+,\cdot)$ est un anneau. On note 0 l'élément neutre pour l'addition. Si la multiplication a un élément neutre (ce qui n'est pas nécessairement le cas), on le note 1 et on dit que A est un anneau *unitaire*.

Enfin, si la multiplication est commutative, on dit que A est un anneau *commutatif*.

Exemples. $(\mathbb{N},+,\times)$ n'est pas un anneau. $(\mathbb{Z},+,\times,)$, $(\mathbb{Q},+,\times,)$, $(\mathbb{R},+,\times,)$ et $(\mathbb{C},+,\times,)$ sont des anneaux.

Proposition. *Soit $(A,+,\cdot)$ un anneau. Alors, pour tout $x \in A$, $x \cdot 0 = 0 \cdot x = 0$.*

Preuve. En effet, si $x \in A$, on a $x \cdot 0 = x \cdot (0+0) = x \cdot 0 + x \cdot 0$, ce qui nous donne $x \cdot 0 = 0$. De même $0 \cdot x = 0$. □

On déduit de cela que, si $(A,+,\cdot)$ est un anneau unitaire, alors 0 n'admet jamais de symétrique pour la multiplication, ce qui généralise un phénomène bien connu dans $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ et $\mathbb{C}$. Par contre, les anneaux pour lesquels tous les éléments différents de 0 admettent un symétrique pour la multiplication ont un rôle crucial en mathématiques : on les appelle les corps.

Définition. Soit $(K,+,\cdot)$ un anneau unitaire. On dit que K est un *corps* si et seulement si $(K^*,\cdot)$ est un groupe, où $K^* = K \setminus \{0\}$ et où 0 est l'élément neutre de la loi $+$.

Exemples. $(\mathbb{N},+,\times)$ et $(\mathbb{Z},+,\times,)$ ne sont pas des corps. $(\mathbb{Q},+,\times,)$, $(\mathbb{R},+,\times,)$ et $(\mathbb{C},+,\times,)$ sont des corps.

1.2 Sous-anneaux, sous-corps, morphismes d'anneaux et de corps.

Définition. On appelle *sous-anneau* d'un anneau $(A,+,\cdot)$ une partie B non vide de A qui vérifie les propriétés :

- B est un sous-groupe de A pour l'addition.

- B est stable pour la multiplication.

Par exemple, l'ensemble de entiers pairs est un sous-anneau de $\mathbb{Z}$.

Enfin, si B est un sous-anneau d'un anneau A, l'addition et la multiplication dans A "induisent" une addition et une multiplication dans B qui est lui-même un anneau.

Définition. Etant donné deux anneaux $(A, +, \cdot)$ et $(A', \oplus, \odot)$, on appelle *morphisme* de A sur A' (pour l'addition et la multiplication) une application f de A dans A' qui soit un morphisme de $(A, +)$ dans $(A', \oplus)$ et telle que

$$\forall (x, y) \in A^2, \qquad f(x \cdot y) = f(x) \odot f(y).$$

Si f est de plus bijective, on dit que f est un *isomorphisme* de A dans A'. f^{-1} est alors un morphisme de $(A', \oplus, \odot)$ dans $(A, +, \cdot)$. On note alors $A \simeq A'$.

Enfin, si deux corps sont isomorphes en tant qu'anneaux, ont dit qu'ils sont isomorphes en tant que corps.

2 $\mathbb{Z}/n\mathbb{Z}$ avec $n \in \mathbb{N}^*$

Dans toute cette section, $n \in \mathbb{N}^*$ est fixé.

Définition. On rappelle que la relation binaire $\mathscr{R}$ définie sur $\mathbb{Z}$ par $x \mathscr{R} y$ si et seulement si $x - y$ est divisible par n est une relation d'équivalence sur $\mathbb{Z}$. L'ensemble quotient de $\mathbb{Z}$ par cette relation est noté $\mathbb{Z}/n\mathbb{Z}$. C'est l'ensemble des classes d'équivalences $\{\overline{0}, \overline{1}, \ldots, \overline{n-1}\}$

En effet, il est clair que pour tout $x \in \mathbb{Z}$, $x \mathscr{R} x$, donc $\mathscr{R}$ est réflexive.

Si x et y sont deux éléments de $\mathbb{Z}$ tels que $x \mathscr{R} y$, alors il existe $p \in \mathbb{Z}$ tel que $x - y = np$. On en déduit que $y - x = n(-p)$, donc que $y \mathscr{R} x$, ce qui prouve que $\mathscr{R}$ est symétrique.

Enfin, si x, y et z sont trois éléments de $\mathbb{Z}$ tels que $x \mathscr{R} y$ et $y \mathscr{R} z$, il existe $p \in \mathbb{Z}$ et $q \in \mathbb{Z}$ tels que $x - y = np$ et $y - z = nq$. On a alors $x - z = (x - y) + (y - z) = np + nq = n(p + q)$, ce qui prouve que $x \mathscr{R} z$, et donc que $\mathscr{R}$ est bien transitive.

Ceci achève de prouver que $\mathscr{R}$ est une relation d'équivalence.

Enfin pour montrer que l'ensemble quotient de $\mathbb{Z}$ par $\mathscr{R}$ est bien $\{\overline{0}, \overline{1}, \ldots, \overline{n-1}\}$, il suffit de remarquer que, si $x \in \mathbb{Z}$, en faisant la division euclidienne de x par n, on peut écrire de manière unique

$$x = nq + r$$

avec $q \in \mathbb{Z}$ et $r \in \{0, \ldots, n-1\}$. On dit que r est le reste de la division de x par n, et on remarque de plus que $x \mathscr{R} r$. En particulier, pour tout $x \in \mathbb{Z}$, $\overline{x} = \overline{r}$ où $r \in \{0, \ldots, n-1\}$ est le reste de la division de x par n.

La relation d'équivalence $\mathscr{R}$ est compatible avec les lois $+$ et $\cdot$ de $\mathbb{Z}$, c'est-à-dire que si x, y, x', y' dans $\mathbb{Z}$ sont tels que $x \mathscr{R} x'$ et $y \mathscr{R} y'$, alors $(x+y) \mathscr{R} (x'+y')$ et $xy \mathscr{R} x'y'$. En effet, le fait que $x \mathscr{R} x'$ et $y \mathscr{R} y'$ est équivalent à l'existence de $p, q \in \mathbb{Z}$ tels que $x - x' = np$ et $y - y' = nq$. On a alors $(x+y) - (x'+y') = (x-x') + (y-y') = np + nq = n(p+q)$, donc $(x+y) \mathscr{R} (x'+y')$. De même, $xy - x'y' = x(y-y') + xy' - x'y' = x(y-y') + (x-x')y' = xnq + npy' = n(xq + py')$, donc $xy \mathscr{R} x'y'$.

Il découle de cela que l'on peut munir $\mathbb{Z}/n\mathbb{Z}$ d'une addition et d'une multiplication en posant, pour $(x, y) \in Z^2$:

$$\overline{x} + \overline{y} = \overline{x+y}, \qquad \overline{x} \cdot \overline{y} = \overline{x \cdot y}.$$

En effet, pour que cela soit valable, il suffit de montrer que si on prend d'autres x', y' dans $\mathbb{Z}$ tels que $\overline{x} = \overline{x}'$ et $\overline{y} = \overline{y}'$, alors $\overline{x+y} = \overline{x'+y'}$ et $\overline{x \cdot y} = \overline{x' \cdot y'}$, et ceci découle exactement du fait que $\mathscr{R}$ est compatible avec l'addition et la multiplication. Tout ceci se résume dans la proposition et définition suivante :

Proposition et Définition. On peut définir une multiplication et une addition sur $\mathbb{Z}/n\mathbb{Z}$ par les formules :

$$\forall (x, y) \in \mathbb{Z}^2, \qquad \overline{x} + \overline{y} = \overline{x+y}, \qquad \overline{x} \cdot \overline{y} = \overline{x \cdot y}.$$

$(\mathbb{Z}/n\mathbb{Z}, +, \cdot)$ devient alors un anneau commutatif unitaire. L'élément neutre pour l'addition est $\overline{0}$, tandis que l'élément neutre pour la multiplication est $\overline{1}$.

Etablissons à titre d'exemples les tables d'additions et de multiplication de $\mathbb{Z}/n\mathbb{Z}$ pour $n = 1, 2, 3$ et 4.

Pour $n = 1$, le seul élément de $\mathbb{Z}/\mathbb{Z}$ est $\overline{0}$ et nous avons

$$\overline{0} + \overline{0} = \overline{0} \qquad \overline{0} \cdot \overline{0} = \overline{0}.$$

Pour $n = 2$, les deux éléments de $\mathbb{Z}/2\mathbb{Z}$ sont $\overline{0}$ et $\overline{1}$, et nous avons

$$\overline{0} + \overline{0} = 0, \quad \overline{0} + \overline{1} = \overline{1} + \overline{0} = \overline{0+1} = \overline{1}, \quad \overline{1} + \overline{1} = \overline{1+1} = \overline{2} = \overline{0}.$$

$$\overline{0} \cdot \overline{0} = \overline{0}, \quad \overline{0} \cdot \overline{1} = \overline{1} \cdot \overline{0} = \overline{0 \cdot 1} = \overline{0}, \quad \overline{1} \cdot \overline{1} = \overline{1 \cdot 1} = \overline{1}.$$

De même, pour $n = 3$, nous avons les trois éléments $\overline{0}, \overline{1}, \overline{2}$ et

$$\overline{0} + \overline{0} = \overline{0}, \quad \overline{0} + \overline{1} = \overline{1}, \quad \overline{0} + \overline{2} = \overline{2}, \quad \overline{1} + \overline{0} = \overline{1}, \quad \overline{1} + \overline{1} = \overline{2}, \quad \overline{1} + \overline{2} = \overline{3} = \overline{0}$$

$$\overline{2} + \overline{0} = \overline{2}, \quad \overline{2} + \overline{1} = \overline{3} = \overline{0}, \quad \overline{2} + \overline{2} = \overline{4} = \overline{1}.$$

$$\overline{0} \cdot \overline{0} = \overline{0}, \quad \overline{0} \cdot \overline{1} = \overline{0}, \quad \overline{0} \cdot \overline{2} = \overline{0}, \quad \overline{1} \cdot \overline{0} = \overline{0}, \quad \overline{1} \cdot \overline{1} = \overline{1}, \quad \overline{1} \cdot \overline{2} = \overline{2}$$

$$\overline{2} \cdot \overline{0} = \overline{0}, \quad \overline{2} \cdot \overline{1} = \overline{2}, \quad \overline{2} \cdot \overline{2} = \overline{4} = \overline{1}.$$

Enfin, pour $n = 4$, nous avons les quatre éléments $\overline{0}, \overline{1}, \overline{2}, \overline{3}$ et

$$\overline{0} + \overline{0} = \overline{0}, \quad \overline{0} + \overline{1} = \overline{1}, \quad \overline{0} + \overline{2} = \overline{2}, \quad \overline{0} + \overline{3} = \overline{3}, \quad \overline{1} + \overline{0} = \overline{1}, \quad \overline{1} + \overline{1} = \overline{2}, \quad \overline{1} + \overline{2} = \overline{3}, \quad \overline{1} + \overline{3} = \overline{4} = \overline{0}$$

$$\overline{2}+\overline{0} = \overline{2}, \quad \overline{2}+\overline{1} = \overline{3}, \quad \overline{2}+\overline{2} = \overline{4} = \overline{0} \quad \overline{2}+\overline{3} = \overline{5} = \overline{1}, \quad \overline{3}+\overline{0} = \overline{3}, \quad \overline{3}+\overline{1} = \overline{4} = \overline{0}, \quad \overline{3}+\overline{2} = \overline{5} = \overline{1}, \quad \overline{3}+\overline{3} = \overline{6} = \overline{2}.$$

$$\overline{0} \cdot \overline{0} = \overline{0}, \quad \overline{0} \cdot \overline{1} = \overline{0}, \quad \overline{0} \cdot \overline{2} = \overline{0}, \quad \overline{0} \cdot \overline{3} = \overline{0}, \quad \overline{1} \cdot \overline{0} = \overline{0}, \quad \overline{1} \cdot \overline{1} = \overline{1}, \quad \overline{1} \cdot \overline{2} = \overline{2}, \quad \overline{1} \cdot \overline{3} = \overline{3}$$

$$\overline{2} \cdot \overline{0} = \overline{0}, \quad \overline{2} \cdot \overline{1} = \overline{2}, \quad \overline{2} \cdot \overline{2} = \overline{4} = \overline{0}, \quad \overline{2} \cdot \overline{3} = \overline{6} = \overline{2}, \quad \overline{3} \cdot \overline{1} = \overline{3}, \quad \overline{3} \cdot \overline{2} = \overline{6} = \overline{2}, \quad \overline{3} \cdot \overline{3} = \overline{9} = \overline{1}.$$

On remarque une propriété surprenante de $\mathbb{Z}/4\mathbb{Z}$: l'élément $\overline{2}$ est non nul, et pourtant $\overline{2} \cdot \overline{2} = \overline{0}$. Les anneaux qui possèdent cette propriété sont dits *non intègres*.

De manière plus précise, un anneau $(A, +, \cdot)$ est *intègre* si et seulement si,

$$\forall (x, y) \in A^2, \qquad (x \cdot y = 0) \Leftrightarrow [(x = 0) \text{ ou } (y = 0)].$$

En particulier, les corps sont des anneaux intègres : en effet, si x, y sont deux éléments d'un corps K tels que $x \cdot y = 0$, et si $x \neq 0$, alors x possède un inverse x^{-1} et on a $x^{-1} \cdot (x \cdot y) = x^{-1} \cdot 0 = 0 = (x^{-1} \cdot x) \cdot y = 1 \cdot y = y$, ce qui prouve que nécessairement $y = 0$.

On remarque ensuite que $\mathbb{Z}/2\mathbb{Z}$ et $\mathbb{Z}/3\mathbb{Z}$ sont des corps (l'inverse de $\overline{1}$ dans $\mathbb{Z}/2\mathbb{Z}$ est $\overline{1}$, les inverses de $\overline{1}$ et $\overline{2}$ dans $\mathbb{Z}/3\mathbb{Z}$ sont respectivement $\overline{1}$ et $\overline{2}$). Par contre $\mathbb{Z}/4\mathbb{Z}$ n'est pas un corps (ce n'est même pas un anneau intègre) ; on peut aussi voir plus directement que $\overline{2}$ n'a pas d'inverse dans $\mathbb{Z}/4\mathbb{Z}$.

Plus généralement, on peut montrer que $\mathbb{Z}/n\mathbb{Z}$ est intègre si et seulement si n est premier, et que $\mathbb{Z}/n\mathbb{Z}$ est un corps si et seulement si n est premier, mais cela dépasse le niveau de ce cours.