Chapitre 3

Les anneaux

3.1 Définitions

Définition

Un *anneau*[1] est un ensemble A muni de deux opérations internes, notées $\oplus$ et $\odot$. Un anneau est donc un triplet $(A, \oplus, \odot)$.

L'opération $\oplus$ satisfait les propriétés suivantes[2].

1. À chaque paire d'éléments de A, notés a_1 et a_2, on associe un unique élément de l'anneau A, noté $a_1 \oplus a_2$. En d'autres termes, $\oplus$ est une application bien définie
$$\oplus : A \times A \to A;\ (a_1; a_2) \mapsto a_1 \oplus a_2$$
2. Quelque soit a_1, a_2 et a_3 dans A, on a $(a_1 \oplus a_2) \oplus a_3 = a_1 \oplus (a_2 \oplus a_3)$.
3. Il existe un élément spécial de A, appelé *neutre additif* et noté 0 tel que
$$a \oplus 0 = 0 \oplus a = a \quad \text{quelque soit } a \in A$$
4. Pour chaque $a \in A$, il existe un *opposé*, noté $-a$ tel que $a \oplus -a = 0$.
5. Pour chaque paire d'éléments de A, notés a_1 et a_2, on a $a_1 \oplus a_2 = a_2 \oplus a_1$.

L'opération $\odot$ satisfait les propriétés suivantes[3].

6. Il existe un élément spécial de A, appelé *neutre multiplicatif* et noté 1 tel que
$$1 \odot a = a \ \text{ et } \ a \odot 1 = a \quad \text{quelque soit } a \in A$$
7. Quelque soit a_1, a_2 et a_3 dans A, on a $(a_1 \odot a_2) \odot a_3 = a_1 \odot (a_2 \odot a_3)$.

Il y a encore deux règles de compatibilité entre les opérations $\oplus$ et $\odot$. Il s'agit des règles de distributivité ou de mise en évidence.

$$a_1 \odot (a_2 \oplus a_3) = a_1 \odot a_2 \oplus a_1 \odot a_3$$
$$(a_2 \oplus a_3) \odot a_1 = a_2 \odot a_1 \oplus a_3 \odot a_1$$

1. Dans ce cours, il s'agit en fait d'un anneau unitaire.
2. Le couple $(A, \oplus)$ est d'un groupe additif commutatif (donnée par le cinquième axiome).
3. Ces propriétés sont proches de celles que l'on trouve dans les axiomes d'espaces vectoriels. Elles font penser à une action de groupe.

Définition

Un anneau $(A, \oplus, \odot)$ est dit *commutatif* si la propriété suivante est satisfaite.

Pour chaque paire d'éléments de A, notés a_1 et a_2, on a $a_1 \odot a_2 = a_2 \odot a_1$.

Conséquences

Des règles ci-dessus, on peut en DÉDUIRE les trois règles suivantes

$$0 \odot a = 0 \qquad a \odot 0 = 0 \qquad (-1) \odot a = -a$$

La deuxième règle n'est pas superflue si l'anneau n'est pas commutatif. Pour la troisième règle, l'élément -1 est l'opposé du neutre multiplicatif, c'est-à-dire $-1 \oplus 1 = 0$.

Preuve

Montrons d'abord que pour chaque élément de l'anneau, il n'y a qu'un opposé possible (les règles disent a priori qu'il y a en au moins un).

Pour cela, supposons que si on prend deux opposés d'un élément $a \in A$, appelés a_1 et a_2, alors ils sont forcément égaux, c'est-à-dire $a_1 = a_2$.

En effet, puisque a_1 et a_2 sont des opposés de a, par définition, on a

$$a_1 \oplus a = 0 = a_2 \oplus a$$

Ainsi, on a

$$a_1 \oplus a = a_2 \oplus a$$

En faisant $-a$ de chaque côté, on trouve $a_1 = a_2$ (on a le droit car l'application $\oplus$ est bien définie et tout élément de l'anneau possède un opposé).

Déduisons maintenant les trois règles énoncées ci-dessus.

1. Soit $a \in A$, on a

$$0 \odot a \ \oplus \ a \ = \ 0 \odot a \ \oplus \ 1 \odot a \ = \ (0 \oplus 1) \odot a \ = \ 1 \odot a \ = \ a$$

   En faisant $-a$ de chaque côté, on trouve $0 \odot a = 0$ (on a le droit car l'application $\oplus$ est bien définie et tout vecteur possède un opposé).

2. Soit $a \in A$, on a

$$a \odot 0 \ \oplus \ a \ = \ a \odot 0 \ \oplus \ a \odot 1 \ = \ a \odot (0 \oplus 1) \ = \ a \odot 1 \ = \ a$$

   En faisant $-a$ de chaque côté, on trouve $0 \odot a = 0$ (on a le droit car l'application $\oplus$ est bien définie et tout vecteur possède un opposé).

3. Soit $a \in A$, on a

$$(-1) \odot a \ \oplus \ a \ = \ (-1) \odot a \ \oplus \ 1 \odot a \ = \ \big((-1) \oplus 1\big) \odot a \ = \ 0 \odot a \ = \ 0$$

   Donc, par unicité de l'opposé, on a $(-1) \odot a = -a$ pour tout $a \in A$.

Exemples d'anneaux

1. Les nombres entiers $(\mathbb{Z}, +, \cdot)$, les nombres rationnels $(\mathbb{Q}, +, \cdot)$, les nombres réels $(\mathbb{R}, +, \cdot)$ et les nombres complexes $(\mathbb{C}, +, \cdot)$ sont tous des anneaux commutatifs. Le neutre additif est le 0 et le neutre multiplicatif est le 1.
2. Les fonctions réelles, dont le domaine de définition et le domaine d'arrivée est $\mathbb{R}$, forment un anneau commutatifs pour les opérations $+$ et $\cdot$ conventionnelles. Le neutre additif est la fonction $0 : \mathbb{R} \to \mathbb{R};\ x \mapsto 0$ (c'est la fonction qui vaut 0 quelque soit la valeur de x) et le neutre multiplicatif est la fonction $1 : \mathbb{R} \to \mathbb{R};\ x \mapsto 1$ (c'est la fonction qui vaut 1 quelque soit la valeur de x).
3. Les fonctions réelles, dont le domaine de définition et le domaine d'arrivée est $\mathbb{R}$, forment un anneau non commutatif pour les opérations $+$ et $\circ$ (composition de fonctions) conventionnelles. Le neutre additif est la fonction $0 : \mathbb{R} \to \mathbb{R};\ x \mapsto 0$ (c'est la fonction qui vaut 0 quelque soit la valeur de x) et le neutre multiplicatif est la fonction $\mathrm{id} : \mathbb{R} \to \mathbb{R};\ x \mapsto x$ (c'est la fonction qui dont l'image est la même que l'élément de départ).

Les nombres naturels ne forment pas un anneau

En effet, dans $\mathbb{N}$ muni de l'addition et de la multiplication usuelles, aucun nombre non nul n'admet d'opposé (dans $\mathbb{N}$). Ce qui contredit la propriété 4.

Définitions

Soit $(A, \oplus, \odot)$ un anneau.

1. Un élément a de A est dit *inversible* s'il existe b dans A tel que $a \odot b = 1$ et $b \odot a = 1$. Dans ce cas, on dit que b est l'*inverse de* a et on note $b = a^{-1}$.
2. On note $A^\times$ l'ensemble des éléments inversibles de A.
3. On dit que A est un anneau *intègre* si pour tout élément a, b dans A, on a

$$a \odot b = 0 \quad \Longrightarrow \quad a = 0 \ \text{ ou } \ b = 0$$

Définition

Un *corps* est un anneau A tel que $A^\times = A \setminus \{0\}$. C'est-à-dire lorsque tout élément non nul est inversible.

Théorème

Tout anneau A fini et intègre est un corps.

Preuve

On doit montrer que tout élément non nul de l'anneau est inversible. Soit $a \in A$ tel que $a \neq 0$. Disons que A possède exactement n éléments différents (c'est possible puisque A est supposé fini). Ainsi

$$A = \{a_1, \ldots, a_n\}$$

Regardons l'ensemble

$$B = \{a \odot a_1, \ldots, a \odot a_n\}$$

Cet ensemble a n éléments distincts (en exercice). Ainsi $A = B$ et par conséquent, il existe $a_i \in A$ tel que $a \odot a_i = 1$. Cela signifie que a est inversible, ce qu'on voulait montrer. $\square$

3.2 L'anneau des matrices de taille 2 fois 2

Considérons un nouvel objet mathématique appelé *matrice*. Pour simplifier, on ne va étudier que les matrices à coefficients réels de taille 2 fois 2. Voici l'ensemble de telles matrices.

$$M_2(\mathbb{R}) = \left\{ \begin{pmatrix} a_{1,1} & a_{1,2} \\ a_{2,1} & a_{2,2} \end{pmatrix} : a_{i,j} \in \mathbb{R} \right\}$$

On définit l'addition de deux matrices de la manière suivante.

$$\begin{pmatrix} a_{1,1} & a_{1,2} \\ a_{2,1} & a_{2,2} \end{pmatrix} + \begin{pmatrix} b_{1,1} & b_{1,2} \\ b_{2,1} & b_{2,2} \end{pmatrix} = \begin{pmatrix} a_{1,1}+b_{1,1} & a_{1,2}+b_{1,2} \\ a_{2,1}+b_{2,1} & a_{2,2}+b_{2,2} \end{pmatrix}$$

On définit la multiplication de deux matrices de la manière suivante. Elle est effectuée ligne par colonne.

$$\begin{pmatrix} a_{1,1} & a_{1,2} \\ a_{2,1} & a_{2,2} \end{pmatrix} \cdot \begin{pmatrix} b_{1,1} & b_{1,2} \\ b_{2,1} & b_{2,2} \end{pmatrix} = \begin{pmatrix} a_{1,1}b_{1,1}+a_{1,2}b_{2,1} & a_{1,1}b_{1,2}+a_{1,2}b_{2,2} \\ a_{2,1}b_{1,1}+a_{2,2}b_{2,1} & a_{2,1}b_{1,2}+a_{2,2}b_{2,2} \end{pmatrix}$$

Les matrices sont très importantes en mathématiques et sont utilisées dans beaucoup de sujets de mathématiques appliquées (le moteur de recherche de `Google`, la programmation linéaire, les stratégies de jeux (en tandem avec la théorie des probabilités), les modèles économiques, l'imagerie par ordinateur, les modèles de populations animales, ...).

3.3 Les anneaux de congruences

3.3.1 Division euclidienne

On considère deux entiers a, b de l'anneau des nombres entiers $(\mathbb{Z}, +, \cdot)$. Si b n'est pas nul, on peut effectuer une division euclidienne de a par b. Cela permet d'obtenir un *quotient* q et un *reste* r tels que :

$$a = b \cdot q + r$$

Afin d'avoir l'unicité pour le quotient et pour le reste, on va toujours choisir le plus petit reste positif possible ! Cela signifie que l'on impose $r \geqslant 0$ et $r < |b|$.

Exemple

Si on veut distribuer 20 pièces de 5 centimes à 7 personnes, on va donner 2 pièces à chacune et il en restera 6. La division euclidienne de 20 par 7 livre donc un quotient de 2 et un reste de 6.

$$20 = 7 \cdot 2 + 6$$

3.3.2 Les congruences

Soit a et b deux nombres entiers et m un nombre naturel positif. Si la division euclidienne de a par m donne le même reste que celle de b par m, on dit que a *est congru à* b *modulo* m et on note

$$a \equiv b \pmod{m}$$

Exemple. L'exemple ci-dessus montre que $20 \equiv 6 \pmod{7}$.

Proposition

On a l'équivalence : $a \equiv b \pmod{m} \iff a - b$ est divisible par m
Autrement dit : $a \equiv b \pmod{m} \iff a - b \equiv 0 \pmod{m}$

Preuve

On effectue la division euclidienne de a par m et celle de b par m. On obtient :

$$a = mq_a + r_a \quad \text{avec} \quad 0 \leqslant r_a < m \quad \text{et} \quad b = mq_b + r_b \quad \text{avec} \quad 0 \leqslant r_b < m$$

Ainsi, on a $\boxed{a - b = m(q_a - q_b) + r_a - r_b}$ (♠) avec $-m < r_a - r_b < m$ (♣).
Remarquons que $r_a - r_b$ n'est pas forcément le reste de la division euclidienne de $a - b$ par m. En effet, on n'a pas forcément $0 \leqslant r_a - r_b < m$, puisque $r_a - r_b$ peut être négatif.

Ainsi, on a : $a \equiv b \pmod{m} \iff a$ et b ont les mêmes restes de division par m

$$\iff r_a = r_b \iff r_a - r_b = 0 \overset{(\clubsuit)}{\iff} r_a - r_b \text{ est divisible par } m$$
$$\overset{(\spadesuit)}{\iff} a - b \text{ est divisible par } m$$ □

Proposition

Si $a \equiv \alpha \pmod{m}$ et $b \equiv \beta \pmod{m}$. Alors :

a) $a + b \equiv \alpha + \beta \pmod{m}$ b) $a \cdot b \equiv \alpha \cdot \beta \pmod{m}$

Preuve

Par la proposition précédente, on sait que $a - \alpha$ et $b - \beta$ sont divisibles par m. Ainsi, il existe k_a et k_b dans $\mathbb{Z}$ tels que :

$$a - \alpha = k_a m \quad \text{et} \quad b - \beta = k_b m$$

a) Il faut s'assurer que $a + b - (\alpha + \beta)$ soit divisible par m. C'est bien le cas car :

$$a + b - (\alpha + \beta) = a - \alpha + b - \beta = k_a m + k_b m = (k_a + k_b)m$$

b) Il faut s'assurer que $a \cdot b - (\alpha \cdot \beta)$ soit divisible par m. Ici c'est un peu plus subtil. On a

$$a = k_a m + \alpha \quad \text{et} \quad b = k_b m + \beta$$

Donc

$$ab = (k_a m + \alpha) \cdot (k_b m + \beta) = k_a k_b m^2 + \alpha k_b m + \beta k_a m + \alpha\beta$$

Ce qui est équivalent à dire que $ab - \alpha\beta$ est bien divisible par m, car

$$ab - \alpha\beta = (k_a k_b m + \alpha k_b + \beta k_a)m$$ □

Remarque

On vient de montrer que l'on peut utiliser l'addition et la multiplication des nombres entiers dans le contexte des congruences. Cela permet de simplifier les calculs. Par exemple, on a :

$$\begin{cases} 49 \equiv 5 \pmod{11} \\ 118 \equiv 8 \pmod{11} \end{cases} \implies \begin{cases} 49 + 118 \equiv 5 + 8 \equiv 13 \pmod{11} \\ 49 \cdot 118 \equiv 5 \cdot 8 \equiv 40 \pmod{11} \end{cases}$$

Et ceci sans avoir eu à calculer les valeurs de $49 + 118$ et de $49 \cdot 118$ dans $\mathbb{Z}$.

Principe

Lorsqu'on calcule des congruences, on s'arrange toujours pour inscrire le plus petit nombre positif ou nul possible. Par exemples :

c) $125 \equiv 0 \pmod 5$ d) $591 \equiv 0 \pmod 3$ e) $50 \equiv 2 \pmod 4$

f) $53 \equiv 4 \pmod 7$ g) $-20 \equiv 1 \pmod 3$ h) $-44 \equiv 6 \pmod{10}$

Définition

Pour chaque $m \in \mathbb{N}$, on définit :

$$\mathbb{Z}_m = \{0, 1, 2, \ldots, m-1\}$$

En suivant le principe ci-dessus, l'addition et la multiplication de $\mathbb{Z}$ permet de mettre une structure d'anneau sur cet ensemble.

L'anneau $(\mathbb{Z}_m, +, \cdot)$ est appelé l'*anneau des restes de division modulo m*. Lorsqu'on calcule dans un tel anneau, on utilise le symbole $\equiv$ au lieu de $=$.

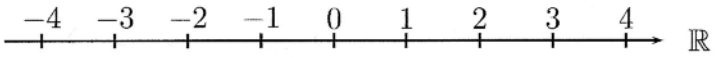
Utilités de tels anneaux

Ces anneaux apparaissent naturellement :

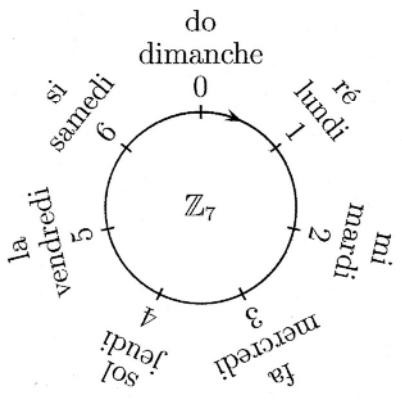
1. Les heures sont comptés modulo 24.
2. Les jours sont comptés modulo 7.
3. Les noms des notes naturelles (do, ré, mi, fa, sol, la, si) obéissent à une règle de calcul modulo 7.

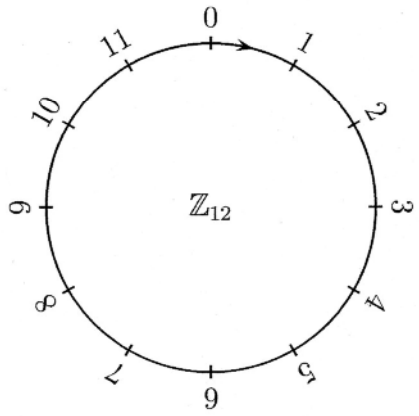
Vision géométrique

Alors que les nombres entiers sont placés sur la droite réelle.



Les congruences modulo m sont représentés sur un cercle. Voici par exemple une représentation de $\mathbb{Z}_7$ et de $\mathbb{Z}_{12}$.





Remarque

On peut démontrer que : $\mathbb{Z}_m$ est un anneau intègre $\iff$ m est un nombre premier