

De l'arithmétique ailleurs que sur $\mathbb{Z}$

Gonzalo Romero-García

d'après Uli Fahrenberg
et Bashar Dudin

Résumé

Cette feuille de travaux dirigés vise à vous donner un aperçu de ce qu'est la structure d'anneau, les différents types d'anneaux que vous avez déjà rencontrés et les inter-connections entre ces types. Elle vous invite également à découvrir des anneaux qui se matérialisent en informatique.

Table des matières

1	Axiomes d'un anneau	1
2	Catégories d'anneaux	4

1 Axiomes d'un anneau

Dans cette section, vous devrez utiliser les axiomes d'anneaux pour prouver des propriétés qui vous sembleront évidentes (car elles sont enracinées dans le fond de votre esprit mathématique) mais qui en fait découlent des axiomes qu'on a établis et qui ne sont pas forcément vraies si l'un de ces axiomes ne s'applique pas.

Il faudra que vous procédiez étape par étape en n'utilisant qu'un axiome à la fois pour comprendre à quel moment vous appliquez quel axiome.

Dans toute cette section, $(A, +, \cdot)$ désigne un anneau.

Question 1-1 Montrer que l'élément neutre pour l'addition (noté 0) est unique.

Indice : Supposez l'existence d'un autre élément et prouvez qu'il est égal à 0.

Supposons que 0 soit
est neutre pour +

$$\forall x \in A \quad x + 0 = x$$

Question 1-2 Montrer que, pour tout $a \in A$, l'opposé de a (noté $-a$) est unique.

Indice : Supposez l'existence de deux opposés b et b' de a et concluez.

Soit $x \in A$ $a + x = x$
 $(a+x) + (-x) = x + (-x)$
 Associativité? $a + (x + (-x)) = 0$
 $= 0$ par opp.

Question 1-3

a) Montrer que $\forall a \in A, -(-a) = a$.

$a + 0 = 0$ car 0 neutre
 a car 0 neutre

Soit $a \in A$
 Supposons que $a + 0 = 0 = b + a$ mg $b = -a$

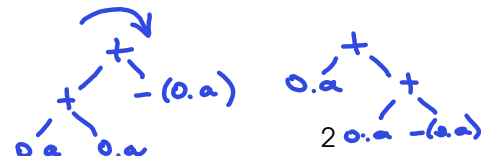
$a = a + 0 = 0$
 0 est neutre

$a + (b + (-a)) \leftarrow (a+b) + (-a) = 0 + (-a) = -a$
 0 est neutre
 || commut.
 $(b+a) + (-a)$
 $= b + (a + (-a)) = b + 0 = b$
 assoc. $= 0$ par 0 est neutre

par unicité de l'opposé

3a) Mg $-(-a) = a$: $-(-a)$ vérifie $-(-a) + (-a) = 0$

Or comme $-a$ est l'opp de a on a
 $a + (-a) = 0$ car qu'a est l'opp de a



b) Montrer que $\forall a, b \in A, -(a+b) = (-a) + (-b)$.

Question 1-4 Montrer que $\forall a \in A, 0 \cdot a = 0$.

Question 1-5

a) Montrer que $\forall a, b \in A, (-a) \cdot b = -(a \cdot b)$.

c) Montrer que $\forall a, b \in A, (-a) \cdot (-b) = a \cdot b$.

Handwritten proof for Question 1-4:

$$0 = 0 + 0 \text{ (0 est neutre)}$$

$$0 \cdot a = (0 + 0) \cdot a \stackrel{\text{dist}}{=} 0 \cdot a + 0 \cdot a$$

$$0 \cdot a + (-0 \cdot a) = (0 \cdot a + 0 \cdot a) + (-0 \cdot a)$$

$$\stackrel{\text{opp}}{=} 0 \cdot a + (0 \cdot a + (-0 \cdot a))$$

$$\stackrel{\text{assoc}}{=} 0 \cdot a + (0 \cdot a + (-0 \cdot a))$$

$$\stackrel{\text{opp}}{=} 0 \cdot a + 0 = 0 \text{ (0 est neutre)}$$

2 Catégories d'anneaux

Dans cette section vous allez être amenés à décider du fait que des ensembles standards ou leurs sous-ensembles soient naturellement munis de structures d'anneaux. Vous allez également naviguer à travers les différentes propriétés des anneaux et vérifier une partie de celles-ci sur des cas pratiques.

Pour rappel :

1. $\mathbb{Z}/n\mathbb{Z} = \{[0], [1], [2], \dots, [n-1]\}$ où la classe d'équivalence est définie de la manière suivante :

$$[a] = \{a + k \cdot n \in \mathbb{Z} : k \in \mathbb{Z}\}.$$

On rappelle que les opérations d'addition et de multiplication suivantes sont bien définies :

$$[a] + [b] = [a + b]$$

et

$$[a] \cdot [b] = [a \cdot b]$$

2. $A[X]$ est l'ensemble des polynômes à coefficients sur un anneau A (par exemple $A = \mathbb{Z}, \mathbb{Q}, \mathbb{R}, \dots$). De manière générale, on dit qu'un élément de A est un $P = a_0 + a_1 \cdot X + a_2 \cdot X^2 + \dots + a_n \cdot X^n$ (où n est le degré du polynôme). La définition formelle de cet ensemble est :

$$A[X] = \bigcup_{n \in \mathbb{N}} \left\{ \sum_{k=0}^n a_k \cdot X^k : \forall k \in [0, n], a_k \in A \right\}.$$

3. $A(X)$ est l'ensemble des fractions rationnelles à coefficients sur un anneau A (par exemple $A = \mathbb{Z}, \mathbb{Q}, \mathbb{R}, \dots$). De manière générale, on dit qu'un élément de A est un $\frac{P}{Q} = \frac{a_0 + a_1 \cdot X + a_2 \cdot X^2 + \dots + a_n \cdot X^n}{b_0 + b_1 \cdot X + b_2 \cdot X^2 + \dots + b_m \cdot X^m}$ (où n et m sont les degrés du numérateur et du dénominateur, respectivement). La définition formelle de cet ensemble est :

$$A(X) = \bigcup_{m \in \mathbb{N}} \bigcup_{n \in \mathbb{N}} \left\{ \frac{\sum_{k=0}^n a_k \cdot X^k}{\sum_{i=0}^m b_i \cdot X^i} : \forall k \in [0, n], a_k \in A, \forall i \in [0, m], b_i \in A, \exists i \in [0, m], b_i \neq 0 \right\}.$$

4. $B^A = \{f : A \rightarrow B\}$, c'est à dire les fonctions de A en B . À noter que quand $A = \mathbb{N}$, on parle de *suites* à valeurs en B ; en effet, si (a_n) est une suite, on peut définir la fonction $a : \mathbb{N} \rightarrow B, n \mapsto a_n$.

Question 2-6 On s'intéresse à la liste des ensembles, munis dans chaque cas de deux opérations internes :

CIKF	$(\mathbb{N}, +, \times)$	pas d'app	
CIKF	$(\mathbb{Z}/5\mathbb{Z}, +, \times)$	✓	[0] [1]
CXKF	$(\mathbb{Z}/6\mathbb{Z}, +, \times)$	✓	
CIKX	$(\mathbb{Q}, +, \times)$	✓	
CIKX	$(\mathbb{Z}[X], +, \times)$	✓	
CIKX	$(\mathbb{Q}(X), +, \times)$	✓	
CIKX	$(\mathbb{N}^{\mathbb{N}}, +, \times)$	pas d'app	
XXXX	$(M_5(\mathbb{R}), +, \times)$ (les matrices carrées de taille 5 munies de la multiplication matricielle)	✓	(0) (Id ₅)
CXXX	$(M_5(\mathbb{R}), +, \cdot)$ (les matrices carrées de taille 5 munies de la multiplication coefficient par coefficient)	✓	(0) (1)
CXXX	$(E, +, \times)$ où E est l'ensemble des suites convergentes ayant pour limite 0	pas d'elt neutre pax	
CXXX	$(S, +, \times)$ où S est l'ensemble des suites convergentes	✓	(0) _n (1) _n
CXXX	$(\mathbb{R}^{\mathbb{R}}, +, \times)$	✓	0R, 1R

Handwritten formula for fraction addition:

$$\left[\frac{P}{Q} \right] + \left[\frac{R}{S} \right] = \left[\frac{PS + QR}{QS} \right]$$

$$\left(\frac{P}{Q} \right) = \frac{P \cdot A}{Q \cdot A} \quad \forall A$$

Handwritten proof for Question 1-5c:

$$a \cdot b = 0$$

$$\neq 0$$

$$a \cdot b \cdot b^{-1} = 0$$

$$\uparrow$$

$$a$$

$$\forall a, b \quad -(a+b) = (-a) + (-b)$$

$$\begin{aligned} \text{calculons } (a+b) + ((-a) + (-b)) &= (a+b) + ((-b) + (-a)) \\ &\stackrel{\text{assoc.}}{=} a + (b + ((-b) + (-a))) \\ &\stackrel{\text{assoc.}}{=} a + ((b + (-b)) + (-a)) \\ &\stackrel{=0 \text{ opp}}{=} a + (0 + (-a)) \\ &\stackrel{0 \text{ est neutre}}{=} a + (-a) \\ &\stackrel{=0 \text{ opp}}{=} 0 \end{aligned}$$

$$\forall x, y, z \quad (x+y)+z = x+(y+z)$$

Par unicité de l'opp (2) : l'opp de $a+b$ est $(-a) + (-b)$

$$\forall a, b : \underline{(-a) \cdot b = -(ab)}$$

$$\forall x, y, z \quad (x \cdot y) + (y \cdot z) = (x+y) \cdot z$$

$$\text{calculons } (a \cdot b) + ((-a) \cdot b) \stackrel{\text{dist}}{=} (a + (-a)) \cdot b \stackrel{=0 \text{ opp}}{=} 0 \cdot b \stackrel{0}{=} 0$$

$\Rightarrow (-a) \cdot b$ est un opposé de ab , or l'opposé unique (2)

$$\text{donc } -(ab) = (-a) \cdot b$$

$$\forall a, b \quad (-a) \cdot (-b) = a \cdot b$$

$$\forall a, b \quad \underline{(-a) \cdot (-b) + (-ab)} = 0 \text{ alors on aura } (-a) \cdot (-b) = -(-ab) = ab \text{ par (3)}$$

$$(-a) \cdot (-b) + (-ab) = (-a) \cdot (-b) + (-a) \cdot b$$

$$\stackrel{(5a)}{=} (-a) \cdot b$$

$$\stackrel{\text{dist.}}{=} (-a) \cdot ((-b) + b) = (-a) \cdot 0 \stackrel{=0 \text{ opp}}{=} 0$$

$$\text{or } \forall c \quad c \cdot 0 = 0 \text{ car } c \cdot 0 = c \cdot (0 + 0) = c \cdot 0 + c \cdot 0 \quad [\dots] \\ + (-c \cdot 0) \quad 0 = c \cdot 0.$$

— $(\mathbb{R}^{\mathbb{Q}}, +, \circ)$

1. Quels éléments de la liste ne sont pas des anneaux ? Justifier.
2. Pour ceux qui sont des anneaux, identifier les éléments neutres et relever les axiomes d'anneaux qui ne sont pas évidents à vérifier pour chacun des cas. ✓
3. Regrouper graphiquement les anneaux de la liste au regard des propriétés suivantes, être :
 - commutatif —
 - intègre —
 - un corps —
 - fini. —

Dans chaque cas justifier vos choix.

est neutre $\checkmark + \checkmark$
 $\times ?$

$f: \mathbb{Q} \rightarrow \mathbb{R}$
 $g: \mathbb{Q} \rightarrow \mathbb{R}$

$f \circ g = f \circ g$

$g = \sqrt{2}$

$f \circ (g+h) = f \circ g + f \circ h$

LINEARITE

IK-er.

$(\mathbb{F}, +, \circ)$

$\forall a, b \text{ si } a \cdot b = 0 \Rightarrow a = 0 \text{ ou } b = 0$

$f \circ (g+h) = f \circ g + f \circ h$