ÉCOLE D'INGENIEURS EN INFORMATIQUE

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.

+ commutatif

$\exists 0 \quad \forall a \quad a+0 = 0+a = a$

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

$\forall a \quad \exists -a \quad a+(-a) = (-a)+a = 0$

Table des matières

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 enracinés 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.

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.

Question 1-3

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

① si a est élt neutre pour + : on a $\underbrace{\underbrace{a+0}_{0 \text{ est neutre}}}_{0 \text{ car } a \text{ est neutre}} = a$ donc $a = 0$

② supposons que $a+b = 0$

$-a$

$\underbrace{(a+b)+(-a)}_{\text{assoc}} = \underbrace{0+(-a)}_{\text{élt neutre}}$

$a+\underbrace{(b+(-a))}_{\text{comm.}} = -a$

$\underbrace{a+(-a+b)}_{\text{assoc}} = -a$

$\underbrace{(a+(-a))}_{\text{opp.}}+b = -a$

élt neutre

$0+b = -a$ $\boxed{b = -a}$

③ ⓐ Mq $\forall a \in A \quad -(-a) = a$

on sait $\forall a \quad \boxed{a} + (-a) = 0 = (-a) + \boxed{a}$ => a est un opposé de $(-a)$
comme l'opposé est unique
on a donc $-(-a) = a$

③b Mq $\forall a, b \quad -(a+b) = (-a) + (-b)$

$\underbrace{(a+b) + [(-a)+(-b)]}_{\text{associativité}} =$

$b = [(a+b) + (-a)] + (-b) = \underbrace{((-a) + (a+b))}_{\text{associativité}} + (-b)$

com.

$(b+a)+(-a)$ $\quad = ((\underbrace{(-a)+a}_{\text{opp.}}) + b) + (-b)$

$b + (\underbrace{a+(-a)}_{=0})$ $\quad = \underbrace{(0+b)}_{\text{elt neutre}} + (-b)$

$b + 0$

b $\quad = \underbrace{b + (-b) = 0}_{\text{opp}}$

cl: $(a+b) + ((-a)+(-b)) = 0$

donc $-(a+b) = (-a) + (-b)$

---

④ Mq $\forall a \quad 0.a = 0$ $\qquad$ Distributivité: $\forall x,y,z \quad x(y+z) = xy + xz$

a $\quad 0.(-a) + 0.a = 0.((-a)+a) = 0.0$

$1.a = a$

$(-1).a = -a$?

$\underbrace{(1+(-1))}_{=0}.a = 1.a + (-1).a = a + (-a) = 0$

$0.a$ $\qquad 0 + 0 = 0$

$0.a + 0.a = (0+0).a = 0.a$

$+ (-(0.a))$

Soit $a \in A$

$\underbrace{(0+0)}_{\text{elt neutre de } 0}.a = 0.a$

$(0+0) \times a = \underbrace{0.a + 0.a}_{\text{distributivité}}$

$0.a = \boxed{0.a + 0.a}$

$\underbrace{0.a + (-(0.a))}_{\text{opp } 0} = \underbrace{(0.a + 0.a) + (-(0.a))}_{\text{assoc}}$

$= 0.a + (\underbrace{0.a + (-(0.a))}_{\text{opp } =0})$

$0 = 0.a + 0$

$0 = 0.a$ (elt neutre)

⑤ⓐ Mq $\forall a, b \quad (-a).b = -(ab)$

Mq $(a.b) + ((-a).b) = 0$

$(a.b) + ((-a).b) \underset{\text{distr.}}{=} (\underbrace{a + (-a)}_{=0 \text{ (opp)}}).b = 0.b \underset{④}{=} 0$

⑥ Mq $\forall a, b \quad (-a).(-b) = a.b$

$(-a)(-b) \underset{5a}{=} -(a.(-b)) \underset{5a'}{=} -(-(a.b)) \underset{3a}{=} a.b$

$\boxed{\text{Mq } (5a') \ \forall a, b \quad a.(-b) = -(a.b)}$

$a.(-b) + a.b = a.(\underbrace{(-b)+b}_{=0}) = a.0 = 0$ à démo

$a.0 = a.(0+0) = a.0 + a.0 \longrightarrow a.0 = 0$

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

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. $\mathbb{Z}/n\mathbb{Z} = \{[0], [1], [2], \ldots, [n-1]\}$ 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 :
$$[a] + [b] = [a+b] \qquad \text{et} \qquad [a] \cdot [b] = [a \cdot b]$$
2. $A[X]$ est l'ensemble des polynômes à coefficients sur un anneau A (par exemple $A = \mathbb{Z}, \mathbb{Q}, \mathbb{R}, \ldots$). De manière générale, on dit qu'un élément de A est un $P = a_0 + a_1 \cdot X + a_2 \cdot X^2 + \cdots + a_n \cdot X^n$ (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 $A = \mathbb{Z}, \mathbb{Q}, \mathbb{R}, \ldots$). De manière générale, on dit qu'un élément de A est un $\frac{P}{Q} = \frac{a_0 + a_1 \cdot X + a_2 \cdot X^2 + \cdots + a_n \cdot X^n}{b_0 + b_1 \cdot X + b_2 \cdot X^2 + \cdots + b_m \cdot X^m}$ (où n et m sont les degrés du numérateur et du dénominateur, respectivement). La définition formelle de cet ensemble est :
$$A(X) = \bigcup_{m \in \mathbb{N}} \bigcup_{n \in \mathbb{N}} \left\{ \frac{\sum_{k=0}^{n} a_k \cdot X^k}{\sum_{i=0}^{m} b_i \cdot X^i} : \forall k \in [\![0, n]\!], a_k \in A, \forall i \in [\![0, m]\!], b_i \in A, \exists i \in [\![0, m]\!], b_i \neq 0 \right\}.$$
$\{1, \ldots, n\}^A \to B \equiv B^n = B^A$
4. $B^A = \{f : A \to B\}$, 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 un suite, on peut définir la fonction $a : \mathbb{N} \to B$, $n \mapsto a_n$. $\quad \mathrm{Card}\, B^A = |B|^{|A|}$

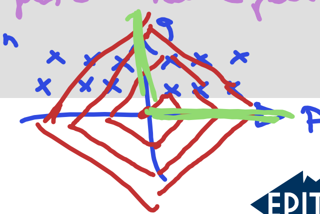
Anneau?

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

x pas d'opp. — elt neutres — $+$ — $\times$

— $(\mathbb{N}, +, \times)$
CIKF — $(\mathbb{Z}/5\mathbb{Z}, +, \times)$ ✓ $0=5$ $1=6$ $\quad \frac{P}{Q} + \frac{R}{S} = \frac{PS+RQ}{QS}$
CxxF — $(\mathbb{Z}/6\mathbb{Z}, +, \times)$ ✓ 0 $1=7$
CIKx — $(\mathbb{Q}, +, \times)$ ✓ 0 1
CIxx — $(\mathbb{Z}[X], +, \times)$ ✓ 0 1
CIKx — $(\mathbb{Q}(X), +, \times)$ ✓ $0/1$ $1/1 = x/x$ $\quad \frac{P \cdot A}{Q \cdot A} = \frac{P}{Q}$
— $(\mathbb{N}^{\mathbb{N}}, +, \times)$ pas opp.
xxxx — $(\mathscr{M}_5(\mathbb{R}), +, \times)$ (les matrices carrés de taille 5 munies de la multiplication matricielle) ✓ (0) I_{d_5}
cxxx — $(\mathscr{M}_5(\mathbb{R}), +, \cdot)$ (les matrices carrés de taille 5 munies de la multiplication coefficient par coefficient) ✓ (0) (1)
— $(E, +, \times)$ où E est l'ensemble des suites convergentes ayant pour limite 0. pas d'elt neutre pour $\times$
cxxx — $(S, +, \times)$ où S est l'ensemble des suites convergentes ✓ $(0)_n$ $(1)_n$
cxxx — $(\mathbb{R}^{\mathbb{R}}, +, \times)$ ✓ $0^{\mathbb{R}}$ $1^{\mathbb{R}}$

$-0,10111\ 01$
$-0,01\ 00 \ldots$
$-0,0001110$



$\mathbb{Z} = \mathbb{Z}^2 \leq \mathbb{R}$

$(f \cdot g) = f \circ g$

$\mathbb{R} \leftarrow \mathbb{Q}$

$g(x) = \sqrt{2} \ \forall x$

$f \cdot g$ n'est pas défini

$f \circ (g+h) \overset{?}{=} f \circ g + f \circ h$

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

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.

$\forall a,b \quad a.b = 0 \Rightarrow a = 0$ ou $b = 0$

$\forall a \quad a.0 = 0$

$\rightarrow a = 0$