

Correction des exercices - Chapitre III

Exercice 1 (Anneaux de Boole)

- 1) Soient a et b des éléments de A . On a l'égalité

$$(a + b)^2 = a^2 + b^2 + ab + ba.$$

Par hypothèse, on a $a^2 = a$, $b^2 = b$ et $(a + b)^2 = a + b$, d'où l'égalité annoncée.

- 2) En utilisant la première question avec $b = 1$, on obtient $a + a = 0$ i.e. $a = -a$.
3) Pour tous $a, b \in A$, on a $ab = -ba = ba$, donc A est commutatif.
4) L'anneau A n'est pas nul, donc $0 \neq 1$. Par hypothèse, il existe $a \in A$ qui est distinct de 0 et 1. On a

$$a(a + 1) = a^2 + a = a + a = 0,$$

d'où l'assertion, car a et $a + 1$ ne sont pas nuls.

- 5) On a $A = \{0, 1\}$. C'est un corps, car tout élément non nul de A est inversible, il est en particulier intègre.
6) Soit E un ensemble. Notons A l'ensemble des parties de E . Pour tous $U, V \in A$ posons

$$U \triangle V = U \cup V - (U \cap V).$$

On définit ainsi une loi de composition interne sur A . Elle s'appelle la différence symétrique. On vérifie que le triplet (A, \triangle, \cap) , avec \triangle comme addition, et l'intersection comme multiplication, est un anneau ; l'élément neutre additif est l'ensemble vide et l'élément neutre multiplicatif est E . Pour tout $U \in A$, on a l'égalité $U \cap U = U$, donc l'hypothèse de l'énoncé est satisfaite.

Exercice 2

Soient a et b des éléments de A .

- 1) On a l'égalité (voir l'indication)

$$b^2 + bab + ab^2 + (ab)^2 = b^2 + 2ab^2 + a^2b^2,$$

d'où $bab = ab^2$.

- 2) On a

$$(1 + b)a(1 + b) = (1 + b)(a + ab) = a + ab + ba + bab.$$

Par ailleurs, on a

$$a(1+b)^2 = a + 2ab + ab^2.$$

On en déduit, avec la première question, l'égalité $ab = ba$, d'où le résultat.

Exercice 3

Posons $c = (1 - ab)^{-1}$. On a les égalités

$$(1 + bca)(1 - ba) = 1 + bca - ba - bcaba = 1 - ba + bc(1 - ab)a.$$

On a $c(1 - ab) = 1$, d'où $(1 + bca)(1 - ba) = 1$. De même, on vérifie que l'on a

$$(1 - ba)(1 + bca) = 1 - ba + bca - babca = 1 - ba + b(1 - ab)ca = 1.$$

Exercice 4

Supposons que A soit un corps. Soit I un idéal non nul de A . Il existe $x \in I$ non nul. C'est un élément inversible de A . Ainsi, $xx^{-1} = 1$ appartient à I , d'où $I = A$. Inversement, A étant non nul, on a $1 \neq 0$. Par ailleurs, soit x un élément non nul de A . L'idéal $I = xA$ étant non nul, on a donc $I = A$. Il existe ainsi $y \in A$ tel que l'on ait $1 = xy$, donc x est inversible. Cela prouve que A est un corps.

Exercice 5

Le noyau $\text{Ker}(f)$ de f est un idéal de K . On a donc (exercice 4) $\text{Ker}(f) = \{0\}$ ou $\text{Ker}(f) = K$. Par ailleurs, on a $f(1_K) = 1_A$. Parce que A est non nul, on a $1_A \neq 0_A$, donc $\text{Ker}(f)$ est distinct de K . On obtient $\text{Ker}(f) = \{0\}$ et le résultat.

Exercice 6

Soit I un idéal de A . L'image $f(I)$ est un sous-groupe de B (chap. II, lemme 2.9). Soit x un élément de $f(I)$ et y un élément de B . On a $f(t) = x$ où $t \in I$. Parce que f est surjectif, il existe $z \in A$ tel que $f(z) = y$. L'élément tz est dans I , donc $f(tz) = f(t)f(z) = xy$ est dans $f(I)$, d'où l'assertion.

Exercice 7

Soit x un élément non nul de A . Montrons que x est inversible. Pour tout $n \in \mathbb{N}$, l'idéal $x^{n+1}A$ est contenu dans x^nA . Puisque A n'a qu'un nombre fini d'idéaux, il existe donc un entier n tel que l'on ait $x^{n+1}A = x^nA$. Par suite, il existe $a \in A$ tel que $x^n = ax^{n+1}$, d'où $x^n(1 - ax) = 0$. On a $x \neq 0$ et A est intègre, d'où $1 = ax$ et x est inversible.

Exercice 8

- 1) L'ensemble $\mathbb{Z}[\sqrt{2}]$ est un sous-groupe additif de \mathbb{C} , qui contient 1. Par ailleurs, soient $x + y\sqrt{2}$ et $x' + y'\sqrt{2}$ des éléments de $\mathbb{Z}[\sqrt{2}]$. On a

$$(x + y\sqrt{2})(x' + y'\sqrt{2}) = xx' + 2yy' + (yx' + xy')\sqrt{2} \in \mathbb{Z}[\sqrt{2}].$$

Cela montre que $\mathbb{Z}[\sqrt{2}]$ est un sous-anneau de \mathbb{C} (déf. 3.2). La démonstration pour $\mathbb{Z}[\sqrt{3}]$ est la même.

- 2) Supposons qu'il existe un homomorphisme d'anneaux $f : \mathbb{Z}[\sqrt{2}] \rightarrow \mathbb{Z}[\sqrt{3}]$. On a $f(1) = 1$, donc pour tout $n \in \mathbb{Z}$, on a $f(n) = n$. On obtient $(f(\sqrt{2}))^2 = f(2) = 2$ et 2 est donc un carré dans $\mathbb{Z}[\sqrt{3}]$. Il existe ainsi $x, y \in \mathbb{Z}$ tels que $(x + y\sqrt{3})^2 = 2$. On obtient

$$2xy\sqrt{3} = 2 - x^2 - 3y^2.$$

Nécessairement, on a $xy \neq 0$, donc $\sqrt{3}$ est un nombre rationnel i.e. il existe $m, n \in \mathbb{N}$ tels que $\sqrt{3} = \frac{n}{m}$, d'où $3m^2 = n^2$. L'exposant de 3 dans la décomposition en facteurs premiers de $3m^2$ (resp. n^2) est impair (resp. pair), d'où une contradiction.

Exercice 9 (Idéaux premiers)

- 1) L'idéal nul est premier car \mathbb{Z} est intègre (comme dans tout anneau intègre). Soit p un nombre premier. Vérifions que $p\mathbb{Z}$ est un idéal premier de \mathbb{Z} . On a $p\mathbb{Z} \neq \mathbb{Z}$ car $p \neq \pm 1$. Soient a et b des entiers relatifs tels que ab soit dans $p\mathbb{Z}$. Alors, p divise ab , donc p divise a ou b (lemme d'Euclide) i.e. a ou b est dans $p\mathbb{Z}$, d'où l'assertion. Inversement, soit I un idéal premier non nul de \mathbb{Z} . C'est en particulier un sous-groupe de \mathbb{Z} , donc il existe $n \in \mathbb{N}$ tel que $I = n\mathbb{Z}$ (chap. II, prop. 2.1). On a $n \geq 2$, sinon I est nul ou $I = \mathbb{Z}$. Soit a un diviseur positif de n . On a $n = ab$ où $b \in \mathbb{N}$. Parce que I est un idéal premier, a ou b est dans I , donc n divise a ou b , autrement dit, $a = n$ ou $a = 1$, ce qui prouve que n est premier.
- 2) Si A est un corps, ses idéaux sont $\{0\}$ et A . Par suite, $\{0\}$ est l'unique idéal premier de A .
- 3) Supposons I premier. L'anneau A/I est non nul car $I \neq A$. Soient $a + I$ et $b + I$ des éléments de A/I tels que $(a + I)(b + I)$ soit nul. Cela signifie que ab est dans I et donc que a ou b est dans I . Ainsi, $a + I$ ou $b + I$ est nul, par suite A/I est intègre. Inversement, supposons A/I intègre. Par définition, A/I n'est pas nul, d'où $A \neq I$. Soient $a, b \in A$ tels que ab soit dans I . On a alors $ab + I = (a + I)(b + I) = 0$, d'où $a + I = 0$ ou $b + I = 0$, autrement dit, a ou b est dans I , donc I est un idéal premier de A .

Exercice 10 (Éléments nilpotents)

Notons $N(A)$ le nilradical de A .

- 1) Soient x et y des éléments de $N(A)$. Il existe des entiers naturels non nuls m et n tels que $x^m = 0$ et $y^n = 0$. D'après la formule du binôme de Newton (valable dans tout anneau commutatif), $(x-y)^{n+m}$ est une somme de multiples entiers des produits $x^r y^s$ avec $r+s = m+n$. Chacun de ces produits est nul, car on ne peut avoir simultanément $r < m$ et $s < n$, d'où $(x-y)^{m+n} = 0$ i.e. $x-y$ est dans $N(A)$. Puisque $0 \in N(A)$, il en résulte que $N(A)$ est un sous-groupe de $(A, +)$. Par ailleurs, pour tout $a \in A$, l'élément ax est aussi dans $N(A)$, donc $N(A)$ est un idéal de A .
- 2) Il existe $n \geq 1$ tel que $x^n = 0$. On obtient

$$1 = 1 - x^n = (1 - x)(1 + \cdots + x^{n-1}),$$

donc $1 - x$ est inversible.

- 3) Notons N le nilradical de $\mathbb{Z}/n\mathbb{Z}$. Si $n = 0$, $\mathbb{Z}/n\mathbb{Z}$ est un groupe isomorphe à \mathbb{Z} , donc N est nul dans ce cas. Si $n = 1$, $\mathbb{Z}/n\mathbb{Z}$ est l'anneau nul, et N est nul. Supposons $n \geq 2$. Soit $s : \mathbb{Z} \rightarrow \mathbb{Z}/n\mathbb{Z}$ la surjection canonique. Soit

$$n = \prod_{i=1}^r p_i^{n_i} \quad (n_i \geq 1),$$

la décomposition de n en produit de nombres premiers. Le groupe

$$\left(\prod_{i=1}^r p_i \right) \mathbb{Z}$$

est un sous-groupe de \mathbb{Z} , qui contient $n\mathbb{Z}$. Vérifions que l'on a

$$N = \left(\prod_{i=1}^r p_i \right) \mathbb{Z} / n\mathbb{Z}.$$

L'image réciproque de N par s est un idéal de \mathbb{Z} . Il existe donc $a \in \mathbb{N}$ tel que l'on ait $s^{-1}(N) = a\mathbb{Z}$. Puisque $s(a) \in N$, il existe $t \geq 1$ tel que a^t soit dans $n\mathbb{Z}$, d'où il résulte que le produit des p_i divise a . Par ailleurs, il existe un entier $k \geq 1$ tel que $(p_1 \cdots p_r)^k$ soit dans $n\mathbb{Z}$ (on peut prendre pour k le maximum des n_i). Ainsi, $s(p_1 \cdots p_r)$ est dans N i.e. $p_1 \cdots p_r$ appartient à $a\mathbb{Z}$. On a donc $a\mathbb{Z} = (p_1 \cdots p_r)\mathbb{Z}$. Parce que s est une surjection, on a $N = s \circ s^{-1}(N)$, d'où $N = s(a\mathbb{Z})$ et l'égalité annoncée.

Exercice 11 (Anneaux principaux)

- 1) Les idéaux d'un corps commutatif K sont $\{0\}$ et K (exercice 4), donc K est principal.
- 2) L'anneau \mathbb{Z} est intègre. Par ailleurs, si I est un idéal de \mathbb{Z} , il existe $n \in \mathbb{N}$ tel que $I = n\mathbb{Z}$, donc I est un idéal principal, d'où l'assertion.

- 3) Le fait que I soit un idéal de $\mathbb{Z}[X]$ résulte de la définition idéal. Supposons qu'il soit principal, autrement dit qu'il existe un polynôme $f \in \mathbb{Z}[X]$ tel que $I = f\mathbb{Z}[X]$. Il existe alors P et Q dans $\mathbb{Z}[X]$ tels que l'on ait $2 = fP$ et $X = fQ$. On en déduit que le degré de f est nul, i.e. que f est dans \mathbb{Z} , puis que le degré de Q vaut 1. Posons $Q = aX + b$ où $a, b \in \mathbb{Z}$. On obtient $X = faX + fb$, d'où $fa = 1$ et $f = \pm 1$. On a ainsi $I = \mathbb{Z}[X]$. Il existe donc $U, V \in \mathbb{Z}[X]$ tels que $1 = 2U + XV$, d'où $1 = 2U(0)$ et une contradiction.

Exercice 12 (Anneaux euclidiens)

- 1) Soient A un anneau euclidien et σ un stathme euclidien pour A . Soit I un idéal non nul de A . Il existe a non nul dans I tel que $\sigma(a)$ soit minimum. Vérifions que l'on a $I = aA$. Puisque a est dans I , l'idéal engendré par a est contenu dans I . Inversement, soit x un élément de I . Il existe q et r dans A tels que $x = aq + r$ avec $r = 0$ ou $\sigma(r) < \sigma(a)$. Puisque r est dans I , le caractère minimal de a entraîne $r = 0$, donc x est dans aA , d'où le résultat.
- 2) L'anneau \mathbb{Z} est euclidien, avec comme stathme euclidien l'application $\mathbb{Z} \setminus \{0\} \rightarrow \mathbb{N}$ qui à x associe $|x|$, la valeur absolue de x .

Exercice 13 (L'anneau des entiers de Gauss)

- 1) C'est un sous-groupe additif qui contient 1. Par ailleurs, pour tous $x, y, x', y' \in \mathbb{Z}$, on a

$$(x + iy)(x' + iy') = xx' - yy' + i(yx' + xy') \in \mathbb{Z}[i]$$

d'où l'assertion.

- 2) Soit $x + iy$ un élément inversible de $\mathbb{Z}[i]$. Il existe $z \in \mathbb{Z}[i]$ tel que $(x + iy)z = 1$, d'où $(x^2 + y^2)|z|^2 = 1$, ce qui conduit à $x^2 + y^2 = 1$, autrement dit, à $(x, y) = (0, \pm 1)$ ou $(x, y) = (\pm 1, 0)$. Il en résulte que l'on a (i est inversible)

$$\mathbb{Z}[i]^* = \{1, -1, i, -i\}.$$

On a $i^2 = -1$, donc i est d'ordre 4, d'où le fait que $\mathbb{Z}[i]^*$ soit cyclique d'ordre 4.

- 3) L'anneau $\mathbb{Z}[i]$ est intègre car il est contenu dans \mathbb{C} . Soient a et b des éléments de $\mathbb{Z}[i]$ avec $b \neq 0$. Il existe α et β dans \mathbb{Q} tels que l'on ait

$$\frac{a}{b} = \alpha + i\beta.$$

Il existe des entiers relatifs u et v tels que l'on ait

$$(1) \quad |\alpha - u| \leq \frac{1}{2} \quad \text{et} \quad |\beta - v| \leq \frac{1}{2}.$$

Posons

$$(2) \quad q = u + iv \quad \text{et} \quad r = a - bq.$$

Ce sont des éléments de $\mathbb{Z}[i]$. Supposons $r \neq 0$ et vérifions que l'on a

$$(3) \quad \sigma(r) < \sigma(b).$$

On a $r = b\left(\frac{a}{b} - q\right)$, d'où l'on déduit les égalités

$$\sigma(r) = \sigma(b) \left| \frac{a}{b} - q \right|^2 = \sigma(b) ((\alpha - u)^2 + (\beta - v)^2).$$

Compte tenu de (1), on obtient ainsi

$$\sigma(r) \leq \frac{\sigma(b)}{2} < \sigma(b),$$

d'où l'inégalité (3) et le fait que $\mathbb{Z}[i]$ soit euclidien. D'après l'exercice 12, il est donc principal.

4) Posons $a = 11 + 7i$ et $b = 3 + 7i$. On a

$$\frac{a}{b} = \frac{41}{29} - \frac{28}{29}i.$$

Les entiers $u = 1$ et $v = -1$ vérifient les inégalités (1). On obtient (cf. (2))

$$a = bq + r \quad \text{avec} \quad q = 1 - i \quad \text{et} \quad r = 1 + 3i.$$

Conformément à l'inégalité (3), on a $\sigma(r) < \sigma(b)$.
