Anneaux[1]

Luc Menichi

1. 13 janvier 2026

Table des matières

Ce cours s'inspire beaucoup de l'excellent livre américain [**DF04**] mais aussi de mes bibles françaises [**RDO82, AF87, Voe02**].

Pour vous déplacer dans le fichier pdf, veuillez cliquer sur la table des matières ou sur les numéros des théorèmes, propositions....

Chapitre 1

La catégorie des anneaux

En mathématiques, en particulier en algèbre, on travaille dans des catégories.

En algèbre linéaire, vous avez vu la catégorie des espaces vectoriels sur un corps commutatif donné $\mathbb{K}$ dont les objets sont les espaces vectoriels et les morphismes, les applications linéaires.

Au premier semestre, vous avez aussi vu la catégorie des espaces topologiques dont les objets sont les espaces topologiques et les morphismes, les applications continues.

Nous allons commencer par revoir la catégorie des groupes déjà définie dans le cours de groupes au premier semestre. Les objets de cette catégorie sont les groupes et les morphismes sont les morphismes de groupes. Puis nous définissons la catégorie des anneaux.

Ce chapitre est survolé dans la Vidéo de la classe à distance du Lundi 13 Janvier 2026, partie 2.

1. Les objets

DEFINITION 1.1. [**RDO82**, 1.5.1.1° Définition] Soit E un ensemble. On appelle *loi de composition interne*, toute application $\star : E \times E \to E$, $(x, y) \mapsto x \star y$. Le couple $(E, \star)$ est appelé *magma*.

DEFINITION 1.2. Soit $(E, \star)$ un magma. On dit que $(E, \star)$ est un *monoïde* si la loi de composition interne $\star$ est associative et unitaire.

PROPRIÉTÉ 1.3. [**RDO82**, 1.5.1.3° Théorème] Soit $(E, \star)$ un monoide.

1) Tout élément neutre e est unique.

2) Supposons que a admet un inverse a^{-1} à gauche. Alors pour tout x et $y \in E$, $a \star x = a \star y$ implique $x = y$. (On dit que a est régulier à gauche).

3) Si a admet un inverse à droite et un inverse à gauche. Alors cet inverse à droite est égale à cet inverse à gauche. En particulier, si a admet un inverse alors il est unique.

Exercice 1

Démontrer la propriété.

DEFINITION 1.4. Soit $(G, \star)$ un monoïde. On dit que $(G, \star)$ est un *groupe* si tout élément admet un inverse.

Lorsque la loi de composition interne $\star$ est commutative, il est courant de la noter $+$ et de l'appeler *addition*. L'élément neutre sera noté 0_G ou 0 et appelé élément *nul*. L'inverse d'un élément x pour le groupe commutatif $(A, +)$ sera appelé *opposé* et noté $-x$.

Sinon souvent, la loi de composition interne est noté $\times$ et est appelé *multiplication*. L'élément neutre est noté 1_G ou 1 et appelé élément *unité*.

DEFINITION 1.5. Soit $(G, \times)$ un groupe noté multiplicativement. Soit $x \in G$. Soit $n \in \mathbb{Z}$. On appelle *puissance n-ièmes* de x notée x^n : $x^0 := 1_G$. Si $n > 0$ alors $x^n := x \times \cdots \times x$. Si $n < 0$ alors $x^n := (x^{-1})^{-n}$. Dans le cas d'un groupe $(G, +)$ noté additivement, x^n est noté nx. Donc $0x := 0_G$. Si $n > 0$ alors $nx := x + \cdots + x$. Si $n < 0$ alors $nx := (-n)(-x)$.

PROPRIÉTÉ 1.6. Pour tout p, $q \in \mathbb{Z}$, i) $x^p \times x^q = x^{p+q}$ et ii) $(x^p)^q = x^{pq}$. En notation additive, i) $px + qx = (p+q)x$ et ii) $(pq)x = q(px)$.

DEFINITION 1.7. [**RDO82**, 3.1.1° Définition] Soit A un ensemble muni de deux lois de compositions internes $+$ et $\times$. On dit que $(A, +, \times)$ est un *anneau* si

$(A, +)$ est un groupe commutatif.

$(A, \times)$ est un monoïde. et

distributivité : pour tout a, b et $c \in A$,

$$a \times (b + c) = a \times b + a \times c$$

et

$$(b + c) \times a = b \times a + c \times a.$$

Dans un anneau A, la loi du groupe commutatif est noté additivement et la loi du monoïde est noté multiplicativement, même si souvent elle sera aussi commutative.

La multiplication de deux éléments $x \times y$ sera simplement noté xy.

L'exemple le plus important d'anneau est $\mathbb{Z}$. Par contre $\mathbb{N}$ n'est pas un anneau.

PROPRIÉTÉ 1.8. Soit $(G, \star)$ un monoïde. Soient x et $y \in G$. si x et y sont inversibles alors le produit $x \star y$ est inversible d'inverse $(x \star y)^{-1} = y^{-1} \star x^{-1}$. Et l'ensemble des éléments inversibles de G est un groupe. En particulier, soit A un anneau, l'ensemble des éléments inversibles est un groupe noté $A^\star$.

Par exemple, soit E un ensemble. Alors E^E l'ensemble des applications de E dans E est un monoïde pour $\circ$ la composition des applications. D'après la propriété, l'ensemble des bijections de E dans E appelées permutation forment un groupe appelé le groupe symetrique de E. Plus généralement, soit $\mathcal{C}$ une categorie. Soit E un objet de $\mathcal{C}$. Alors l'ensemble des morphismes de E dans E (appelé endomorphisme de E), noté $\mathrm{Hom}_{\mathcal{C}}(E, E)$ est un monoide et l'ensemble des isomorphismes de E dans E (appelé automorphisme de E), noté $\mathrm{Iso}_{\mathcal{C}}(E, E)$, est un groupe.

DEFINITION 1.9. Soit $\mathbb{K}$ un anneau. On dit que $\mathbb{K}$ est un *corps* si $\mathbb{K}^\star = \mathbb{K} - \{0\}$.

PROPOSITION 1.10. *Soit $\mathbb{K}$ un anneau. Alors $\mathbb{K}$ est un corps ssi $\mathbb{K}$ n'est pas l'anneau trivial et si tout élément non nul est inversible pour la multiplication.*

L'anneau $\mathbb{Z}$ n'est pas un corps. Vous connaissez les corps $\mathbb{Q}$, $\mathbb{R}$ et $\mathbb{C}$.

Dans un anneau, nous avons les règles de calcul suivante.

PROPRIÉTÉ 1.11. [**RDO82**, 3.1.2.2° Théorème] Soit A un anneau. Alors pour tout $a \in A$,

i) $0a = a0 = 0$ (On dit que 0 est un élément *absorbant*)

ii) pour tout a et $b \in A$, $(-a)b = a(-b) = -(ab)$. En particulier $(-1)a = -a$.

iii) pour tout $n \in \mathbb{Z}$, pour tout a et $b \in A$, $(na)b = a(nb) = n(ab)$. En particulier $na = (n1_A)a$.

Exercice 2

Démontrer la propriété.

Un ensemble réduit à un seul élément est clairement un anneau, appelé anneau nul ou *trivial* où $1 = 0$. Réciproquement,

Exercice 3

Montrer si $1 = 0$ dans un anneau A alors A est l'anneau nul.

Exercice 4

Considérons un ensemble A à deux éléments. Montrer qu'il existe au plus une seule façon de construire une table d'addition et une table de multiplication sur A qui lui donne une structure d'anneau.

Exercice 5

Considérons un ensemble A à trois éléments. Montrer qu'il existe au plus une seule façon de construire une table d'addition et une table de multiplication sur A qui lui donne une structure d'anneau.

PROPOSITION 1.12. *Soit A un anneau. Soit $a \in A$. Les conditions suivantes sont équivalentes.*

i) pour tout x et $y \in A$, $ax = ay$ implique $x = y$. (On dit que a est régulier à gauche).

ii) pour tout $b \in A$ ($ab = 0$ implique $b = 0$).

iii) pour tout x et $y \in A$, $xa = ya$ implique $x = y$. (On dit que a est régulier à droite).

DÉMONSTRATION. Supposons i). Alors en prenant $x = b$ et $y = 0$, comme $a0 = 0$ on obtient ii).

Supposons ii). Soient x et $y \in A$ tel que $ax = ay$. Alors $ax - ay = a(x - y) = 0$. Donc par ii), $x - y = 0$, i. e. $x = y$.

Pour montrer que ii) et iii) sont équivalents, il suffit de considérer l'anneau opposé où la multiplication est effectuée dans l'ordre opposé. □

Donc un élément a n'est pas régulier si il existe $b \neq 0$ tel que $ab = 0$. Souvent, dans la littérature, les éléments non nuls pas réguliers sont appelés diviseurs de zéro. Mais nous n'adopterons pas cette terminologie qui porte à confusion avec la définition 2.6 de diviseur d'un élément.

DEFINITION 1.13. Soit A un anneau. On dit que A est intègre si A n'est pas l'anneau trivial et si pour tout a, $b \in A$ ($ab = 0$ implique $a = 0$ ou $b = 0$).

PROPOSITION 1.14. *Un anneau est intègre ssi il est non trivial et tous les éléments non nuls sont réguliers.*

Comme tout élément inversible est régulier, on obtient

PROPOSITION 1.15. *Tout corps $\mathbb{K}$ est un anneau intègre.*

Réciproquement

PROPOSITION 1.16. *Tout anneau fini intègre est un corps.*

DÉMONSTRATION. Soit A un anneau intègre. On suppose que A est de cardinal fini. Soit a un élément non nul de A. Comme a est régulier à gauche, l'application $A \to A$, $x \mapsto ax$ est injective donc aussi surjective. Donc il existe $x \in A$ tel que $ax = 1$. Donc a admet x pour inverse à droite.

De même, comme a est régulier à droite, il existe $z \in A$ tel que $ya = 1$. Donc a admet z pour inverse à gauche.

Comme a est inversible à gauche et à droite, a est inversible d'après Propriete 1.3 iii). □

2. Les morphismes

DEFINITION 1.17. Soit $(E, \star)$ et $(E', \star)$ deux magmas. Soit $f : E \to E'$ une application. On dit que f est un morphisme de magmas si pour tout x, $y \in E$, $f(x \star y) = f(x) \star f(y)$.

DEFINITION 1.18. Soit $(E, \star)$ et $(E', \star)$ deux monoïdes. Soit $f : E \to E'$ une application. On dit que f est un morphisme de monoïdes si pour tout x, $y \in E$, $f(x \star y) = f(x) \star f(y)$ et si $f(e) = e'$.

DEFINITION 1.19. Soit $(G, \times)$ et $(G', \times)$ deux groupes notés multiplicativement. Soit $f : G \to G'$ une application. On dit que f est un morphisme de groupes si tout x, $y \in E$, $f(xy) = f(x)f(y)$, si $f(1_G) = 1_{G'}$ et si pour tout $x \in G$, $f(x^{-1}) = f(x)^{-1}$.

PROPOSITION 1.20. *Soit $(G, \times)$ et $(G', \times)$ deux groupes. Soit $f : G \to G'$ un morphisme de magmas. Alors f est nécessairement un morphisme de groupes et pour tout $n \in \mathbb{Z}$, pour tout $x \in G$, $f(x^n) = (f(x))^n$.*

DÉMONSTRATION. $f(1_G)f(1_G) = f(1_G 1_G) = f(1_G) = f(1_G)1_{G'}$. Donc d'après la propriété 1.3 2), $f(1_G) = 1_{G'}$.

$f(x)f(x^{-1}) = f(xx^{-1}) = f(1_G) = 1'_G$. Donc $f(x^{-1}) = f(x)^{-1}$.

$f(x^0) = f(1_G) = 1_{G'} = f(x)^0$. Supposons que $n > 0$. Par récurrence, si $f(x^n) = f(x)^n$ alors $f(x^{n+1}) = f(x^n x) = f(x)^n f(x) = f(x)^{n+1}$. $f(x^{-n}) = f((x^{-1})^n) = (f(x^{-1}))^n = ((f(x))^{-1})^n = (f(x))^{-n}$. □

DEFINITION 1.21. Soit A et B deux anneaux. Soit $f : A \to B$ une application. On dit que f est un morphisme d'anneaux si f est à la fois un morphisme de groupes pour l'addition et un morphisme de monoïdes pour la multiplication : i.e pour tout x, $y \in A$, $f(x + y) = f(x) + f(y)$, $f(xy) = f(x)f(y)$ et $f(1) = 1$.

La condition $f(1) = 1$ est nécessaire sinon l'application constamment nulle marche. Voir aussi l'exercice 8

PROPRIÉTÉ 1.22. i) Tout morphisme d'anneaux $f : A \to B$ induit par restriction un morphisme de groupes du groupe des inversibles de A, $A^\star$, vers le groupe des inversibles de B, $B^\star$.

ii) En particulier, tout morphisme d'anneaux $f : \mathbb{K} \to A$ d'un corps $\mathbb{K}$ dans un anneau A non trivial est injectif.

.

Exercice 6

Démontrer la propriété précédente.

3. Anneaux produits

DEFINITION 1.23. [**RDO82**, 3.1.5] Soit $(A_i, +, \times)_{i \in I}$ une famille d'anneaux. Alors A le produit d'ensembles $\Pi_{i \in I} A_i$ est un anneau appele *anneau produit* où l'addition et la multiplication sont définis composantes par composantes : soit $a = (a_i)_{i \in A}$ et $b = (b_i)_{i \in A}$. Alors $a + b = (a_i + b_i)_{i \in A}$ et $a \times b = (a_i \times b_i)_{i \in A}$. $0_A = (0_{A_i})_{i \in A}$. $1_A = (1_{A_i})_{i \in A}$.

Remarquons [**RDO82**, 3.1.5] que le produit d'au moins deux anneaux non trivials n'est jamais intègre. En effet $(0, 1) \times (1, 0) = (1 \times 0, 0 \times 1) = (0, 0)$.

Dans le cas particulier de la famille constante, on obtient que A^I, l'ensemble des applications d'un ensemble I vers un anneau A est un anneau.[**RDO82**, 4.2.2.1° Exemple b)].

4. les sous-objets

Soit E un ensemble. Soit A une partie de E. On appelle inclusion de A dans E, l'application injective de A dans E qui à tout élément de A associe ce même élément vu comme élément de E.

DEFINITION 1.24. Soit G un groupe. Soit H une partie de G. On dit que H est un *sous-groupe* de G si H est un groupe tel que l'inclusion de H dans G soit un morphisme de groupes.

Les deux propositions suivantes sont très utile pour montrer qu'un ensemble est un groupe.

PROPOSITION 1.25. *Soit $(G,\star)$ un groupe. Soit H une partie de G. Alors H est un sous-groupe de G ssi*
H est non vide,
pour tout x, $y \in H$, $x \star y \in H$ (On dit que H est stable pour $\star$) et
pour tout $x \in H$, $x^{-1} \in H$ (On dit que H est stable pour passage à l'inverse).

DÉMONSTRATION. Comme H est non vide, il existe $x \in H$. Par stabilité par passage à l'inverse $x^{-1} \in H$. Par stabilité pour $\star$, $e = xx^{-1} \in H$. Comme e est un élément neutre dans G, c'est aussi un élément neutre dans H. Comme $\star$ est associatif dans G, la restriction de $\star$ dans H est aussi associative. L'inclusion de H dans G est clairement un morphisme de magmas. □

PROPOSITION 1.26. [**RDO82**, 1.6.2]*(Transmission des propriétés) Soit $(G,\star)$ un monoïde. Soit $f : (G,\star) \to (G',\star)$ un morphisme de magmas. Alors la partie $f(G)$ est stable pour $\star$ et est un monoïde pour la loi induite.*
Pour tout x inversible dans G, $f(x)$ est inversible dans le monoide $f(G)$ d'inverse $f(x)^{-1} = f(x^{-1})$. En particulier si G est un groupe alors $f(G)$ est un groupe.

DÉMONSTRATION. Soit y et $y' \in f(G)$ alors il existe x et $x' \in G$ tel que $y = f(x)$ et $y' = f(x')$. Donc $y \star y' = f(x) \star f(x') = f(x \star x') \in f(G)$.
Soit e un élément neutre pour G. Alors pour $y \in f(G)$, il existe $x \in G$ tel que $y = f(x)$. Donc $f(e) \star y = f(e) \star f(x) = f(e \star x) = f(x) = y$. Donc $f(e)$ est un élément neutre pour $f(G)$.
Supposons que $\star$ est associative dans G. Soit a, b et $c \in f(G)$. Alors il existe x, y et $z \in G$ tels que $a = f(x)$, $b = f(y)$ et $c = f(z)$. Donc

$$(a \star b) \star c = (f(x) \star f(y)) \star f(z) = f(x \star y) \star f(z) = f((x \star y) \star z)$$

De même

$$a \star (b \star c) = f(x) \star (f(y) \star f(z)) = f(x) \star f(y \star z) == f(x \star (y \star z))$$

Comme $(x \star y) \star z = x \star (y \star z)$ alors $(a \star b) \star c = a \star (b \star c)$.
$f(x)f(x^{-1}) = f(xx^{-1}) = f(e)$. Donc $f(x^{-1}) = f(x)^{-1}$. □

COROLLAIRE 1.27. *L'image de tout sous-groupe par un morphisme de groupes est un sous-groupe : Soit $f : (G,\star) \to (G',\star)$ un morphisme de groupes. Soit H un sous-groupe de G. Alors $f(G)$ est un sous-groupe de G'. En particulier, Im f est un sous-groupe de G'.*

DÉMONSTRATION. Montrons d'abord le corollaire pour Im f. D'après la proposition précédente, Im $f = f(G)$ est un groupe telle que l'inclusion de $f(G)$ dans G' soit un morphisme de magmas.
Dans le cas général, considérons la restriction de f à H, $f_{|H} : H \to G'$ qui est un clairement un morphisme de groupes. Donc Im $f_{|H} = f(H)$ est un sous-groupe de G'. □

DEFINITION 1.28. Soit A un anneau. Soit B une partie de A. On dit que B est un *sous-anneau* de A si B est un anneau tel que l'inclusion de B dans A soit un morphisme d'anneaux.

PROPOSITION 1.29. *Soit A un anneau. Soit B une partie de A. Alors B est un sous-anneau de A ssi*
$1 \in B$,
pour tout x, $y \in B$, $x + y \in B$ (On dit que B est stable pour l'addition),
pour tout $x \in B$, $-x \in B$ (On dit que B est stable par passage à l'opposée), et
pour tout x, $y \in B$, $xy \in B$. (On dit que B est stable pour la multiplication).

DEFINITION 1.30. Soit A un anneau. On appelle *centre* de A, noté $Z(A)$, l'ensemble des éléments de A commutant avec tous les autres éléments : $a \in Z(A)$ ssi pour tout $x \in A$, $ax = xa$.

Exercice 7

Montrer que le centre de A est un sous-anneau de A.

Exercice 8

Soit A et B deux anneaux.

1. Soit $f : A \to B$ une application additive et multiplicative i.e pour tout x, $y \in A$, $f(x + y) = f(x) + f(y)$, et $f(xy) = f(x)f(y)$. Montrer que si $f(1)$ est régulier ou appartient à l'image de f alors $f(1) = 1$. En particulier si B est intégré et si f n'est pas constamment nulle alors f est un morphisme d'anneaux.
2. Soit $i_1 : A \hookrightarrow A \times B$ l'application définie par $i_1(a) = (a, 0)$ appelé inclusion dans le premier facteur. Montrer que i_1 est additive et multiplicative et que pourtant $i_1(1_A) \neq 1_{A\times B}$ si B n'est pas l'anneau trivial.

En particulier le produit de deux anneaux n'est jamais un corps si un des deux anneaux est non trivial.

Cette exercice montre qu'il n'est pas facile d'étendre un corps. Nous connaissons les extensions de corps $\mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}$.

5. Les entiers modulo n : $\mathbb{Z}/n\mathbb{Z}$

Dans cette section, nous allons introduire l'anneau des entiers modulo n, $\mathbb{Z}/n\mathbb{Z}$. Soit n un entier naturel supérieur ou égal à 2. On définit sur $\mathbb{Z}$ la relation de congruence modulo n par a est congru à b modulo n si n divise $(b - a)$ ssi il existe $k \in \mathbb{Z}$ tel que $b = a + kn$. Notation $a \equiv b \pmod{n}$.

Cette relation est une relation d'équivalence. Pour tout $a \in \mathbb{Z}$, notons par $\overline{a}$, la classe d'équivalence de a. Alors $\overline{a}$ est la partie de $\mathbb{Z}$ donné par

$$\overline{a} = \{a, a \pm n, a \pm 2n, a \pm 3n....\}$$

L'ensemble des classes d'équivalence est l'ensemble quotient $\mathbb{Z}/n\mathbb{Z}$.

Si $a \equiv a' \pmod{n}$ et $b \equiv b' \pmod{n}$ alors $a + b \equiv a' + b' \pmod{n}$. Donc $\overline{a + b}$ dépends que de $\overline{a}$ et de $\overline{b}$.

Donc on peut définir l'opération $+$ sur $\mathbb{Z}/n\mathbb{Z}$ par $\overline{a} + \overline{b} := \overline{a + b}$.

La surjection canonique $q : (\mathbb{Z}, +) \to (\mathbb{Z}/n\mathbb{Z}, +)$ définie par $q(a) = \overline{a}$ est un morphisme de magmas. Comme $(\mathbb{Z}, +)$ est un groupe abélien, d'après la proposition 1.26, $(\mathbb{Z}/n\mathbb{Z}, +)$ est aussi un groupe abélien.

Si $a \equiv a' \pmod{n}$ et $b \equiv b' \pmod{n}$ alors $ab \equiv a'b' \pmod{n}$. Donc on peut définir l'opération $\times$ sur $\mathbb{Z}/n\mathbb{Z}$ par $\overline{a} \times \overline{b} := \overline{a \times b}$.

La surjection canonique $q : (\mathbb{Z}, \times) \to (\mathbb{Z}/n\mathbb{Z}, \times)$ est un morphisme de magmas. Comme $(\mathbb{Z}, \times)$ est un monoïde abélien, d'après la proposition 1.26, $(\mathbb{Z}/n\mathbb{Z}, +)$ est aussi un monoïde abélien.

Comme la surjection canonique $q : (\mathbb{Z}, +, \times) \to (\mathbb{Z}/n\mathbb{Z}, +, \times)$ est à la fois un morphisme de groupes pour l'addition et un morphisme de monoïdes pour la multiplication, la distributivité dans l'anneau $(\mathbb{Z}, +, \times)$ implique la distributivité dans $(\mathbb{Z}/n\mathbb{Z}, +, \times)$ qui est donc aussi un anneau. Nous avons donc prouvé

THÉORÈME 1.31. *L'ensemble quotient $\mathbb{Z}/n\mathbb{Z}$ est un anneau commutatif tel que la surjection canonique $q : (\mathbb{Z}, +, \times) \to (\mathbb{Z}/n\mathbb{Z}, +, \times)$ soit un morphisme d'anneaux.*

PROPOSITION 1.32. *Soit $a \in \mathbb{Z}$. Alors $\overline{a}$ est un élément inversible de l'anneau $\mathbb{Z}/n\mathbb{Z}$ ssi a est premier avec n. En particulier $\mathbb{Z}/n\mathbb{Z}$ est un corps ssi n est un nombre premier.*

DÉMONSTRATION. $\overline{a}$ est un élément inversible ssi il existe $u \in \mathbb{Z}$ tel que $\overline{a} \times \overline{u} = 1$ dans $\mathbb{Z}/n\mathbb{Z}$ ssi il existe $u \in \mathbb{Z}$ tel que $au \equiv 1 \pmod{n}$ ssi il existe $u \in \mathbb{Z}$ et $k \in \mathbb{Z}$ tel que $au = 1 - kn$ ssi a est premier avec n d'après l'identité de Bezout. □

L'algorithme d'Euclide pour calculer le pgcd donne les entiers u et k tel que $au + kn = 1$. La classe $\overline{u}$ est l'inverse multiplicatif de $\overline{a}$. Par exemple, calculons l'inverse de $\overline{17}$ modulo 60. $60 = 17 \times 3 + 9$, $17 = 9 \times 1 + 8$, $9 = 8 \times 1 + 1$. Donc le pgcd de 17 et 60 est bien 1. Donc en partant de la fin, $1 = 9 - 8 = 9 - (17 - 9) = 2 * 9 - 17 = 2 * (60 - 17 \times 3) - 17 = 2 * 60 - 7 * 17$. Donc $\overline{-7} = \overline{53}$ est l'inverse multiplicatif de 17 dans $\mathbb{Z}/60\mathbb{Z}$.

DummitFoote Foot page 11

6. Caractéristique d'un anneau

DEFINITION 1.33. Soit $(G, \times)$ un groupe noté multiplicativement. Soit x un élément de G. Par définition, l'ordre de x est le plus entier naturel n strictement positif tel que $x^n = 1$. Si il n'en existe pas, on dit que x est d'ordre infini.

Soit $\varphi : (\mathbb{Z}, +) \to (G, \times)$ l'unique morphisme de groupes tel que $\varphi(1) = x$. D'après la proposition 1.20, pour tout $n \in \mathbb{Z}$, $\varphi(n) = x^n$. Alors $\ker \varphi$ sous-groupe de $\mathbb{Z}$ est forcément de la forme $a\mathbb{Z}$ où $a \in \mathbb{N}$. Si x est d'ordre infini, alors $\ker \varphi = \{0\}$ et donc $a = 0$ et φ est injectif. Si x est d'ordre n alors $a = n$ et $\ker \varphi = n\mathbb{Z}$.

DEFINITION 1.34. Soit A un anneau. On appelle *caractéristique* de A, l'ordre de 1_A dans le groupe additif $(A, +)$ avec la convention que si cet ordre est infini, on dit que la caractéristique est nulle.

Un anneau est trivial ssi sa caractéristique est égale à 1.

PROPRIÉTÉ 1.35. Soit n la caractéristique d'un anneau A.
i) [**DF04**, 13.1 Proposition 1] Alors pour tout $a \in A$, $na = 0$.
ii) Soit $\varphi : (\mathbb{Z}, +) \to (A, +)$ l'unique morphisme de groupes tel que $\varphi(1) = 1_A$. Alors φ est un morphisme d'anneaux de noyau $\ker \varphi = \{nZ\}$.

DÉMONSTRATION. i) Par définition, $0a := 0_A$ donc si $n = 0$ alors $na = 0_A$. d'après d'après propriété 1.11 iii),

$$na = (n1_A)a = 0_A a = 0_A.$$

ii) D'après la proposition 1.20, pour tout $n \in \mathbb{Z}$, $\varphi(n) = n1_A$. Pour tout p et $q \in \mathbb{Z}$, d'après le ii) de la propriété 1.6 puis d'après propriété 1.11 iii) avec $a = q1_A$,

$$\varphi(pq) = (pq)1_A = p(q1_A) = (p1_A)(q1_A) = \varphi(p)\varphi(q).$$

□

Pour tout anneau A, il existe donc un unique morphisme φ d'anneaux de $\mathbb{Z}$ dans A.

Exercice 9

i) Montrer que l'image de φ est incluse dans le centre de A. On dit que A est une $\mathbb{Z}$-*algèbre*.
ii) Montrer que si A est un corps et φ est injectif alors φ s'étend de manière unique en un morphisme d'anneaux $\Psi : \mathbb{Q} \to A$.

PROPOSITION 1.36. [**DF04**, 13.1 Proposition 1] *Si A est un anneau intègre, alors la caractéristique de A est soit nulle, soit un nombre premier.*

Démonstration. Soit n la caractéristique de A. Supposons que n est non nulle. Alors n est le plus entier strictement positif tel que $n1_A = 0$. Supposons par l'absurde que $n = pq$ avec $p < n$ et $q < n$. D'après la démonstration de iii) de la propriété précédente, $n1_A = (pq)1_A = (p1_A)(q1_A) = 0$. Donc si A est intègre, alors $p1_A = 0$ ou $q1_A = 0$. Contradiction. □

Corollaire 1.37. [**DF04**, 13.1 Definition]*(Sous-corps premier)*
Tout corps $\mathbb{K}$ contient un corps isomorphe à $\mathbb{Q}$ si sa caractéristique est nulle et à $\mathbb{Z}/p\mathbb{Z}$ si sa caractéristique p est non nulle.

Démonstration. Soit $\varphi : \mathbb{Z} \to \mathbb{K}$ l'unique morphisme d'anneaux.

Supposons que la caractéristique soit nulle. Alors $\ker\varphi = \{0\}$ et φ est injectif. Si $\mathbb{K}$ est un corps, φ s'étend de manière unique en un morphisme d'anneaux $\Psi : \mathbb{Q} \to \mathbb{K}$ d'après l'exercice 9. D'après la propriété 1.22 ii), Ψ est injectif.

Supposons que la caractéristique p de $\mathbb{K}$ est non nulle. Alors φ induit un morphisme d'anneaux injectifs $\overline{\varphi} : \mathbb{Z}/p\mathbb{Z} \to A$. Supposons maintenant que $\mathbb{K}$ est un corps. Alors $\mathbb{K}$ est un anneau intègre. Donc p est un nombre premier. Et donc $\mathbb{Z}/p\mathbb{Z}$ est un corps. □

Soit $\varphi : \mathbb{K} \to \mathbb{K}'$ un morphisme de corps. Alors tout $\mathbb{K}'$-espace vectoriel E peut être vu *par restriction de scalaires* comme un espace vectoriel sur $\mathbb{K}$ par l'action définie pour tout $a \in \mathbb{K}$, pour tout $x \in E$ $a \star x := \varphi(a)\dot{x}$. Par exemple, tout $\mathbb{C}$-espace vectoriel peut-etre vu commme un $\mathbb{R}$-espace vectoriel.

Théorème 1.38. [**DF04**, p. 529-30][**?**, 3.C.1° Théorème 1] *Tout corps fini admet pour caractéristique p, un nombre premier et a pour cardinal, une puissance p^d où d est un entier naturel non nul.*

Démonstration. Soit $\mathbb{K}$ un corps. Alors $\mathbb{K}$ est un anneau intègre. Comme $\mathbb{K}$ est de cardinal fini, $\mathbb{K}$ ne peut pas contenir $\mathbb{Z}$. Donc la caractéristique de $\mathbb{K}$ est un nombre premier et $\mathbb{K}$ contient le corps $\mathbb{Z}/p\mathbb{Z}$. Considérons $\mathbb{K}$ vue comme espace vectoriel sur $\mathbb{Z}/p\mathbb{Z}$ par restriction de scalaire via l'inclusion d'anneaux $\overline{\varphi} : \mathbb{Z}/p\mathbb{Z} \to \mathbb{K}$. Comme $\mathbb{K}$ est de cardinal fini, $\mathbb{K}$ admet lui-meme comme famille génératrice fini donc est de dimension finie. Soit d la dimension de $\mathbb{K}$. Alors $\mathbb{K}$ est isomorphe (en particulier en bijection) à $(\mathbb{Z}/p\mathbb{Z})^d$ comme $\mathbb{Z}/p\mathbb{Z}$-espace vectoriels. □

Pour tout nombre premier p et entier naturel non nul d, il existe un corps unique à isomorphisme près de cardinal p^d. On le note $\mathbb{F}_{p^d}$. Nous les construirons dans les chapitres suivant.

Exercice 10

1. Montrer que si un anneau A est de cardinal p, un nombre premier. Alors A est isomorphe au $\mathbb{Z}/p\mathbb{Z}$. ‘
2. Montrer que si un anneau A est de caractéristique p, un nombre premier. Alors A est de cardinal, une puissance p^d où d est un entier naturel non nul.
3. En déduire que si un anneau A est de cardinal pq, où p et q sont deux nombres premiers. Alors A est isomorphe au $\mathbb{Z}/pq\mathbb{Z}$.

7. Corrigé des exercices

Solution de l'exercice 1

1. Soient e et e' deux éléments neutres. Alors $e \star e' = e$ car e' élément neutre. et $e \star e' = e'$ car e élément neutre. Par suite, $e = e'$.
2. Par associativité $x = e \star x = a^{-1} \star a \star x = a^{-1} \star a \star y = e \star y = y$.

3. Soit $x \in E$ un inverse à gauche de a : $x \star a = e$. Soit $y \in E$ un inverse à droite de a : $a \star y = e$. Donc $x = x \star e = x \star (a \star y) = (x \star a) \star y = e \star y = y$.

Solution de l'exercice 2

Vidéo de la classe à distance du Lundi 13 Janvier 2026, partie 1.

Solution de l'exercice 3

Soit $a \in A$. Alors $a = a1 = a0 = 0$. Donc $A = \{0\}$.

Solution de l'exercice 4

Soit 0 l'élément nul et 1 l'élément unité de A. Comme A n'est pas réduit à un seul élément, d'après l'exercice 3, $1 \neq 0$. Donc $A = \{0, 1\}$.

Comme 0 est l'élément nulle $0 + 0 = 0$, $1 + 0 = 1 = 0 + 1$. Supposons que $1 + 1 = 1$ alors $1 + 1 = 1 + 0$. Comme 1 est régulier, $1 = 0$. Contradiction. Donc $1 + 1 = 1 + 0$. D'où la table d'addition

+	0	1
0	0	1
1	1	0

.

Comme 1 est l'élément unité $0 \times 1 = 0$, $1 \times 0 = 0$ et $1 \times 1 = 1$. D'après la propriété 1.11 i), $0 \times 0 = 0$. D'où la table de multiplication

×	0	1
0	0	0
1	0	1

.

On pourra vérifier à la section 5 que cette anneau est $\mathbb{Z}/2\mathbb{Z}$ et donc existe.

Solution de l'exercice 5

Soit 0 l'élément nul et 1 l'élément unité de A. Comme A n'est pas réduit à un seul élément,d'après l'exercice 3, $1 \neq 0$. Soit 2 le troisième élément de A.

Pour tout $x \neq 0$ et tout y, $y + x \neq y + 0 = y$ et $x + y \neq 0 + y = y$ car y est régulier. Donc $2 + 1$ est différent de 1 et de 2 donc est égale à 0. De meme, $1 + 2 = 0$.

Supposons que $1 + 1 = 0$. Première méthode : $2 = 2 + 0 = (2 + 1) + 1 = 0 + 1 = 1$. Contradiction. Seconde méthode : $2 + 1 = 0 = 1 + 1$. Donc comme 1 est régulier, $2 = 1$.

Donc $1 + 1 = 2$. Donc $2 + 2 = 2 + 1 + 1 = 0 + 1 = 1$. Comme 0 est l'élement nul, on a donc la table d'addition

+	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

.

D'après la propriété 1.11 i), $a \times 0 = 0 \times a = 0$ pour tout $a \in A$. Comme 1 est l'élément unité, $a \times 1 = 1 \times a = A$ pour tout $a \in A$. Il reste $2 \times 2 = (1+1) \times 2 = 1 \times 2 + 1 \times 2 = 2 + 2 = 1$. D'où la table de multiplication.

×	0	1	2
0	0	0	0
1	0	1	2
2	0	2	1

.

On pourra vérifier à la section 5 que cette anneau est $\mathbb{Z}/3\mathbb{Z}$ et donc existe.

Solution de l'exercice 6

i) Soit $x \in A$ inversible. Alors $f(x)f(x^{-1}) = f(xx^{-1}) = f(1) = 1$ et $f(x^{-1})f(x) = f(x^{-1}x) = f(1) = 1$. Donc $f(x)$ est inversible d'inverse $(f(x))^{-1} = f(x^{-1})$. (Nous avions déjà fait cette démonstration dans la preuve de la proposition 1.20). Donc f induit par restriction

un un morphisme de groupes du groupe des inversibles de A vers le groupe des inversibles de B.

ii) Soit $x \neq 0 \in K$. Alors $f(x)f(x^{-1}) = f(xx^{-1}) = f(1) = 1$. Comme A n'est pas l'anneau trivial, $1 \neq 0$. D'après le i) de la propriété 1.11, $f(x)f(x^{-1}) \neq 0$ implique $f(x) \neq 0$. Donc $\ker f = \{0\}$. Donc f est injectif.

Solution de l'exercice 7

Pour tout $a \in A$, $1_A a = a = a1_A$. Donc $1_A \in Z(A)$.

Solution de l'exercice 8

1. Supposons que $f(1_A)$ est régulier. Nous avons déjà fait cette démonstration pour montrer qu'un morphisme de magmas entre groupes est un morphisme de groupes :
$$f(1_A)(f(1_A) = f(1_A \times 1_A) = f(1_A) = f(1_A)1_B.$$
Donc comme $f(1_A)$ est régulier à gauche, $f(1_A) = 1_B$.
Supposons que $1_B \in \text{Im } f$. Alors il existe $x \in A$ tel que $1_B = f(x)$. Donc $f(1_A) = f(1_A)1_B = f(1_A)f(x) = f(1_A \times x) = f(x) = 1_B$.
2. $i_1(1_A) = (1_A, 0_B) \neq (1_A, 1_B)$.

Solution de l'exercice 9

i) D'après la proposition 1.20, pour tout $n \in \mathbb{Z}$, $\varphi(n) = n1_A$. Comme le centre $Z(A)$ est un sous-anneau de A, $1_A \in Z(A)$ et donc aussi $n1_A \in Z(A)$.

ii) Unicité : Soit $\Psi : \mathbb{Q} \to A$ un morphisme d'anneaux étendant φ. Soit $x \in \mathbb{Q}$. Supposons que x s'écrive sous la forme $x = p/q$. Comme q est inversible, d'après la propriété 1.22, $\Psi(q^{-1}) = \Psi(q)^{-1} = \varphi(q)^{-1}$. Donc $\Psi(p/q) = \Psi(p)\Psi(1/q) = \varphi(p)\varphi(q)^{-1}$.

Existence : Soit $x \in \mathbb{Q}$. Supposons que x s'écrive sous la forme $x = a/b$. Posons $\Psi(a/b) = \varphi(a)\varphi(b)^{-1}$. Il faut montrer que $\Psi(x)$ est bien définie. Supposons que $x = a/b = c/d$. Alors $ad = bc$. Donc $\varphi(a)\varphi(d) = \varphi(b)\varphi(c)$. Donc $\varphi(b)^{-1}\varphi(a) = \varphi(c)\varphi(d)^{-1}$. D'après i), $\varphi(b)^{-1}\varphi(a) = \varphi(a)\varphi(b)^{-1}$. Donc finalement, on a bien $\varphi(a)\varphi(b)^{-1} = \varphi(c)\varphi(d)^{-1}$.

Soient $x = a/b$ et $y = c/d$. Alors $xy = \frac{ac}{db}$. Donc d'après la propriété 1.8 et i), $\Psi(xy) = \varphi(ac)\varphi(db)^{-1} = \varphi(a)\varphi(c)\varphi(b)^{-1}\varphi(d)^{-1} = \varphi(a)\varphi(b)^{-1}\varphi(c)\varphi(d)^{-1} = \Psi(x)\Psi(y)$. De plus $\Psi(1/1) = \varphi(1)\varphi(1)^{-1} = 1_A \times 1_A = 1_A$. Donc Ψ est un morphisme d'anneaux.

Solution de l'exercice 10

On rappelle que l'ordre d'un groupe divise le cardinal du groupe. En particulier, la caractéristique d'un anneau divise le cardinal de l'anneau.

1. Si ce cardinal est un nombre premier p, alors la caractéristique de A est donc 1 ou p. Mais 1 est impossible car l'anneau serait trivial de cardinal 1. L'unique morphisme d'anneaux $\mathbb{Z} \to A$ a pour noyau $p\mathbb{Z}$ et induit donc un morphisme d'anneaux injectifs $\overline{\varphi} : \mathbb{Z}/p\mathbb{Z} \to A$. Comme $\mathbb{Z}/p\mathbb{Z}$ et A ont même cardinal, $\overline{\varphi}$ est donc une bijection.
2. Si la caractéristique de A est un nombre premier, alors les mêmes arguments que pour le Théorème 1.38 montrer que A est cardinal p^d.
3. Dans ce cas, la caractéristique de A est p ou q ou pq. Mais si la caractéristique de A est p ou q, son cardinal est une puissance de nombres premiers d'après 2). Donc la caractéristique de A est égale à son cardinal et donc A est isomorphe à $\mathbb{Z}/pq\mathbb{Z}$.

Bibliographie

[AF87] Jean-Marie Arnaudiès and Henri Fraysse, *Cours de mathématiques. 1*, Dunod, Paris, 1987, Algèbre. [Algebra].

[DF04] David S. Dummit and Richard M. Foote, *Abstract algebra*, third ed., John Wiley & Sons, Inc., Hoboken, NJ, 2004.

[LFA77a] Jacqueline Lelong-Ferrand and Jean-Marie Arnaudiès, *Cours de mathématiques. Tome 1*, Dunod, Paris, 1977, Algèbre, Troisième édition, 1er Cycle Universitaire. Classes Préparatoires. Mathématiques.

[LFA77b] ———, *Cours de mathématiques. Tome 2*, Dunod, Paris, 1977, Analyse, Quatrième édition, 1er Cycle Universitaire. Classes Préparatoires. Mathématiques.

[RDO82] E. Ramis, C. Deschamps, and J. Odoux, *Cours de mathématiques spéciales. 1*, second ed., Masson, Paris, 1982, Algèbre.

[Voe02] Jean Voedts, *Cours de mathématiques MP-MP**, Ellipses, Paris, 2002.

8. Livres à télécharger

Pour vous aider, j'ai mis les livres de la bibliographie (à l'exception notable de [**LFA77a, LFA77b**] que je n'ai pas trouvé sur Internet) et d'autres livres à télécharger rapidement sur la page cachée suivante de ma page web

`http://www.math.univ-angers.fr/perso/lmenichi/Groupedetravail/`

Veuillez ne pas faire de lien sur cette page web. Car cette page illégale ne doit pas être indexée par google. Merci.

La plupart des livres sont sous le format .djvu. Il faut donc un logiciel de lecture qui lit le format deja vu. Cliquer pour accéder à la page wikipedia qui explique :

-Si vous êtes sous linux, Evince est sûrement déjà installé.

-Vous pouvez installer par exemple, le logiciel libre DjVuLibre. Si vous êtes sous Windows, cliquer ici pour télécharger la version pour Windows.

-Sur votre smartphone, à vous de voir.

Vous pouvez télécharger d'autres livres sur le site pirate library genesis.