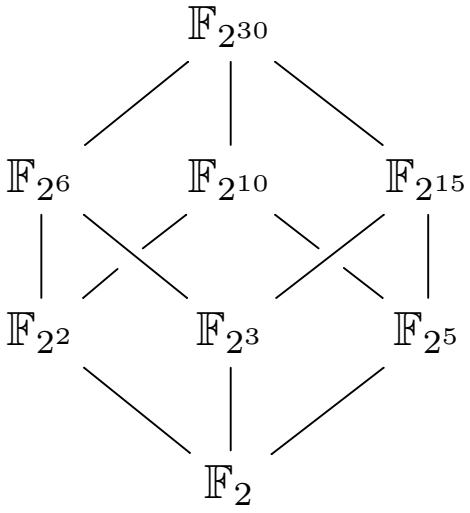
Lycée Chateaubriand
Colas Bardavid

Chapitre 11

Anneaux et corps



Petits corps en treillis.

Les anneaux et les corps, structures algébriques fondamentales, formalisent la notion de nombre et d'opération.

L'anneau par excellence est $\mathbb{Z}$.
Le corps par excellence est $\mathbb{R}$.

Sommaire

I. Anneaux 3
1) Anneaux 3
2) Exemples 3
3) Premières propriétés des anneaux 5
4) Calcul dans un anneau 7
5) Inversibles d'un anneau 9
6) Entiers dans un anneau 9
7) Sous-anneaux 10
8) L'anneau nul 10
9) Anneau produit 11

II. Morphismes d'anneaux 11
1) Définition 11
2) Exemples 12
3) Composition entre morphismes 12
4) Isomorphismes d'anneaux 12
5) Anneaux isomorphes 13
6) Noyau 13

III. Anneaux commutatifs 13
1) Définition 13
2) Anneaux intègres 14

IV. Corps 14
1) Définition 14
2) Exemples 15
3) Les corps sont intègres 15

V. L'anneau $\mathbb{Z}/n\mathbb{Z}$ 16
1) Rappels et notations 16
2) Addition 16
3) Multiplication 18
4) Structure d'anneau 19
5) Les $\mathbb{Z}/p\mathbb{Z}$ sont des corps 19

I. Anneaux

1) Anneaux

Définition ANN.1
Un anneau *est un* 5*-uplet* $(R, +, \times, 0_R, 1_R)$ *tel que*

- $(R, +, 0_R)$ *est un groupe commutatif ;*
- $(R, \times, 1_R)$ *est un monoïde ;*
- *la loi* $\times$ *est* distributive à gauche et à droite *par rapport à la loi* $+$, ie

$$\forall x, y, z \in R, \quad \begin{cases} (x+y) \times z = x \times z + y \times y \\ x \times (y+z) = x \times y + x \times z. \end{cases}$$

Les anneaux constituent la structure algébrique qui formalise le calcul algébrique. Un anneau est un « endroit mathématique » où l'on dispose d'une addition et d'une multiplication qui sont compatibles entre elles.

Remarques

- Par abus de notation, on dira souvent que R est un anneau au lieu de parler de $(R, +, \times, 0_R, 1_R)$.
- Si R est un anneau,
  - ▷ la loi $+$ est appelée *loi additive de* R ;
  - ▷ la loi $\times$ est appelée *loi multiplicative de* R ;
  - ▷ l'élément 0_R est appelé *zéro de* R ;
  - ▷ l'élément 1_R est appelé *un de* R.
- Si R est un anneau et si $x, y \in R$, on note aussi xy ou $x \cdot y$ à la place de $x \times y$.
- Si le contexte le demande, on notera $+_R$ et $\times_R$ au lieu de $+$ et $\times$ les lois de R.

2) Exemples

3) Premières propriétés des anneaux

- Les anneaux, comme on l'a dit, sont des « endroits » où l'on peut faire du calcul, comme on a l'habitude d'en faire.
- Vérifions-le en démontrant les faits suivants, qui doivent devenir des réflexes.
- Paradoxalement, ces petites propriétés ne sont pas si simples à démontrer et peuvent être déroutantes pour les débutants. Ainsi, lors d'une première lecture, on pourra sauter les preuves. Au contraire, le lecteur ambitieux pourra essayer de démontrer ces petits faits sans lire les preuve.

a) propriétés immédiates

Fait ANN.**2**
Soit R un anneau et soit $x \in R$.

$$\boxed{x + 0_R = 0_R + x = x} \qquad \textit{et} \qquad \boxed{x \times 1_R = 1_R \times x = x.}$$

Démonstration. —

- Par définition, $(R, +, 0_R)$ est un groupe. Donc, par définition, 0_R est un neutre pour la loi $+$. Donc, par définition,
$$\forall x \in R, \quad x + 0_R = 0_R + x = x.$$
D'où le premier résultat.
- Par définition, $(R, \times, 1_R)$ est un monoïde. Donc, par définition, 1_R est un neutre pour la loi $\times$. Donc, par définition,
$$\forall x \in R, \quad x \times 1_R = 1_R \times x = x.$$
D'où le second résultat.

■

b) propriétés sur le zéro et sur le un

Fait ANN.**3**
Soit R un anneau. Alors,

$$0_R + 0_R = 0_R \qquad \textit{et} \qquad -0_R = 0_R.$$

Démonstration. —

- On particularise le fait ANN.2 avec $x = 0_R$. On trouve $0_R + 0_R = 0_R$.
- Dans un groupe $(G, \cdot, e)$, on a toujours $e^{-1} = e$. En particulier, dans le groupe $(R, +, 0_R)$, on a
$$-0_R = 0_R.$$

■

Fait ANN.**4**
Soit R un anneau. Alors,

$$1_R \times 1_R = 1_R.$$

Démonstration. — On particularise le fait ANN.2 avec $x = 1_R$. On trouve $1_R \times 1_R = 1_R$. ■

c) zéro est absorbant

Fait ANN.**5**
Soit R un anneau. Alors,

$$\forall x \in R, \quad x \times 0_R = 0_R \times x = 0_R.$$

Démonstration. — Soit $x \in R$.

- Notons $y \coloneqq x \times 0_R$.
- Comme $0_R + 0_R = 0_R$, on a
$$x \times (0_R + 0_R) = x \times 0_R.$$
Donc, par distributivité, on a
$$x \times 0_R + x \times 0_R = x \times 0_R.$$
Ie, on a
$$y + y = y.$$
- Maintenant, ajoutons des deux côtés de cette égalité l'opposé $-y$ de y. On a
$$(y + y) - y = y - y.$$
Ie, on a
$$y + (y - y) = 0_R.$$
Ie, on a
$$y + 0_R = 0_R.$$
- Comme 0_R et le neutre pour la loi $+$, on a $y + 0_R = y$. Donc, on a $y = 0_R$, *ie*
$$\boxed{x \times 0_R = 0_R.}$$
- On laisse le lecteur montrer que $x \times 0_R = 0_R$, à titre d'exercice.

■

Remarque
On dit que 0_R est un élément absorbant pour la multiplication.

d) opposé et multiplication par -1_R

Fait ANN.**6**
Soit R un anneau. Alors,

$$\forall x \in R, \quad (-1_R) \times x = x \times (-1_R) = -x.$$

Démonstration. —

- Par définition de -1_R, qui l'opposé de 1_R, on a $1_R - 1_R = 0_R$.
- Soit maintenant $x \in R$. On a donc, d'après le fait ANN.5,
$$(1_R - 1_R) \times x = 0_R.$$
- Donc, par distributivité,
$$1_R \times x + (-1)_R \times x = 0_R.$$
- Comme $1_R \times x = x$ (d'après ANN.2), on a donc $x + (-1)_R \times x = 0_R$.

- Ajoutons à chacun des membres de cette égalité l'opposé $-x$ de x ; on obtient

$$\underbrace{-x+x}_{=0_R} + (-1)_R \times x = -x + 0_R.$$

- D'où

$$\boxed{(-1)_R \times x = -x.}$$

- On laisse le lecteur montrer que $x \times (-1)_R = -x$, à titre d'exercice.

■

e) règle des signes

Fait ANN.**7** (Règle des signes)
Soit R un anneau. Alors,

$$(-1_R) \times (-1_R) = 1_R.$$

Démonstration. —

- On particularise le fait ANN.6 pour $x = -1_R$.
- On obtient $(-1_R) \times (-1_R) = -(-1_R)$.
- Or, dans tout groupe $(G, \cdot, e)$ et pour tout $x \in G$, on a $(x^{-1})^{-1} = x$.
- Dans $(R, +, 0_R)$, pour tout $x \in R$, on a $-(-x) = x$.
- D'où

$$\boxed{(-1_R) \times (-1_R) = 1_R.}$$

■

4) Calcul dans un anneau

Soit R un anneau et soient $x, y \in R$.

a) formule de Newton

Proposition ANN.**8**
Soit $n \in \mathbb{N}$. On suppose que $xy = yx$. Alors, on a

$$(x+y)^n = \sum_{k=0}^{n} \binom{n}{k} x^k y^{n-k}.$$

⚠ Attention
Cette formule est fausse si x et y ne commutent pas !

Démonstration. — On note, pour $n \in \mathbb{N}$,

$$\mathscr{P}(n) \coloneqq \text{« } (x+y)^n = \sum_{k=0}^{n} \binom{n}{k} x^k y^{n-k} \text{ ».}$$

- Déjà, $\mathscr{P}(0)$ est vraie. En effet, on a bien

$$(x+y)^0 = 1_R = \binom{0}{0} x^0 y^{0-0}.$$

- Montrons l'hérédité, *ie* montrons que
$$\forall n \in \mathbb{N}, \quad \mathscr{P}(n) \implies \mathscr{P}(n+1).$$
Soit $n \in \mathbb{N}$ tel que $\mathscr{P}(n)$. On calcule (à l'aide de la formule de Pascal) :
$$\begin{aligned}
(x+y)^{n+1} &= (x+y)^n(x+y) \\
&= \left(\sum_{k=0}^{n} \binom{n}{k} x^k y^{n-k}\right)(x+y) \\
&= \sum_{k=0}^{n} \binom{n}{k} x^{k+1} y^{n-k} + \sum_{k=0}^{n} \binom{n}{k} x^k y^{(n+1)-k} \\
&= \sum_{\ell=1}^{n+1} \binom{n}{\ell-1} x^{\ell} y^{(n+1)-\ell} + \sum_{k=0}^{n} \binom{n}{k} x^k y^{(n+1)-k} \\
&= \binom{n}{n} x^{n+1} + \sum_{k=0}^{n} \underbrace{\left(\binom{n}{k-1} + \binom{n}{k}\right)}_{=\binom{n+1}{k}} x^k y^{(n+1)-k} + \binom{n}{0} y^{n+1} \\
&= \sum_{k=0}^{n+1} \binom{n+1}{k} x^k y^{(n+1)-k}.
\end{aligned}$$
Ainsi, $\mathscr{P}(n+1)$ est vraie.
- Grâce au principe de récurrence, on conclut.

■

Remarques

- C'est exactement la même démonstration que pour $\mathbb{C}$.
- À quel endroit a-t-on utilisé que $xy = yx$?

b) formule de Bernoulli

Proposition ANN.9
Soit $n \in \mathbb{N}^*$. On suppose que $xy = yx$. Alors, on a
$$x^n - y^n = (x-y)\sum_{k=0}^{n-1} x^k y^{(n-1)-k}.$$

⚠ Attention
Cette formule est fausse si x et y ne commutent pas !

Démonstration. — On force à apparaître une somme télescopique. On calcule
$$\begin{aligned}
(x-y)\sum_{k=0}^{n-1} x^k y^{(n-1)-k} &= \sum_{k=0}^{n-1} x^{k+1} y^{(n-1)-k} - \sum_{k=0}^{n-1} x^k y^{n-k} && (\text{car } xy = yx) \\
&= \sum_{k=0}^{n-1} x^{k+1} y^{n-(k+1)} - \sum_{k=0}^{n-1} x^k y^{n-k} \\
&= \sum_{k=0}^{n-1} x^{k+1} y^{n-(k+1)} - x^k y^{n-k}.
\end{aligned}$$

Il s'agit d'une somme télescopique. On a donc

$$(x-y)\sum_{k=0}^{n-1} x^k y^{(n-1)-k} = x^n y^{n-n} - x^0 y^{n-0} = x^n - y^n.$$

■

5) Inversibles d'un anneau

Soit R un anneau.

a) définition

Définition ANN.10

- *Soit $x \in R$. On dit que x* est un inversible R $\overset{\Delta}{\text{ssi}}$

$$\exists y \in R : \begin{cases} xy = 1_R \\ yx = 1_R. \end{cases}$$

- *On note $R^\times$ ou $\mathsf{U}(R)$ l'ensemble des éléments inversibles de R.*

Remarque

Autrement dit, x est un inversible R si, et seulement si, x est inversible dans le monoïde $(R, \times, 1_R)$.

Exemples

- On a $\mathbb{R}^\times = \mathbb{R}^*$.
- De même, on a $\mathbb{C}^\times = \mathbb{C}^*$.
- En revanche, on a $\mathbb{Z}^\times = \{-1, 1\}$. C'est pour cette raison qu'on n'écrit jamais $\mathbb{Z}^*$.
- Les éléments inversible dans $\mathsf{M}_n(\mathbb{R})$ sont les matrices inversibles.

b) groupe des inversibles

Proposition ANN.11

Le triplet $\big(\mathsf{U}(R), \times, 1_R\big)$ est un groupe, appelé groupe des inversibles de R.

6) Entiers dans un anneau

Si $n \in \mathbb{N}$, on note

$$n \cdot 1_R \coloneqq \underbrace{1 + 1 + \cdots + 1}_{n \text{ fois}} ;$$

et, si $n \in \mathbb{Z}$ et $n < 0$, on note

$$n \cdot 1_R \coloneqq -((-n) \cdot 1_R).$$

Rappelons que ces notations ont déjà introduites pour n'importe quel groupe abélien $(G, +, 0_G)$.

7) Sous-anneaux

Définition ANN.12
Soit R un anneau et soit $T \subset R$. On dit que T est un sous-anneau de R $\overset{\Delta}{\text{ssi}}$

$$T \text{ est un sous-groupe de } (R, +, 0_R) \qquad et \qquad \begin{cases} \forall x, y \in T,\ xy \in T \\ 1_R \in T. \end{cases}$$

Remarques

- Autrement dit, T est un sous-anneau de R $\overset{\Delta}{ssi}$ T est stable par addition, par multiplication et contient le un de R.
- * Soit R un anneau et soit $T \subset R$ un sous-anneau de R. On considère la loi $+$ de R. C'est une application
$$+ : R \times R \longrightarrow R.$$
Comme T est stable par addition, la restriction de $+$ à $T \times T$ peut-être corestreinte à T. *Ie*, on peut considérer
$$\left(+|_{T\times T}\right)\Big|^{T} : T \times T \longrightarrow T.$$
De même, on peut considérer
$$\left(\times|_{T\times T}\right)\Big|^{T} : T \times T \longrightarrow T.$$
Alors, le 5-uplet
$$\left(T, \left(+|_{T\times T}\right)\Big|^{T}, \left(+|_{T\times T}\right)\Big|^{T}, 0_R, 1_R\right)$$
est un anneau.

Exemples

- $\mathbb{Z}$ est un sous-anneau de $\mathbb{R}$.
- $\mathrm{M}_n(\mathbb{Z})$ est un sous-anneau de $\mathrm{M}_n(\mathbb{R})$.

8) L'anneau nul

Proposition ANN.13
Soit R un anneau.
On a

$$\big(\forall x \in R,\ x = 0_R\big) \quad \Longleftrightarrow \quad 0_R = 1_R.$$

Démonstration. —

- Le sens $\Longrightarrow$ est évident.
- Montrons le sens $\Longleftarrow$. On suppose que $0_R = 1_R$. Soit $x \in R$. On a alors $x \times 0_R = x \times 1_R$. Donc, par propriétés des anneaux : $0_R = x$. Ainsi, on a bien
$$0_R = 1_R \quad \Longrightarrow \quad \big(\forall x \in R,\ x = 0_R\big).$$

■

Remarques

- Cela peut paraître étrange mais ça marche bien : si 0_R est un « élément », alors l'ensemble $\{0_R\}$ peut bien être muni de lois $+$ et $\times$ qui en font un anneau.
- Ainsi, on a montré que
$$0_R = 1_R \iff R = \{0_R\}.$$

Exercice ANN.14
Soit R un anneau. Est-ce que $\{0_R\}$ est un sous-anneau de R ?

Définition ANN.15
Soit R un anneau. On dit que R est nul $\overset{\Delta}{\text{ssi}}$ $1_R = 0_R$.

Remarque
On peut parler de l'anneau nul car tous les anneaux nuls sont isomorphes.

9) Anneau produit

Soit R et S des anneaux.
Alors, comme on l'a fait pour les groupes, on peut munir $R \times S$ d'une structure d'anneau. Les lois $+$ et $\times$ et leurs neutres respectifs sont définis par

$$\begin{cases} (x,y) + (x',y') = (x + x', y + y') \\ (x,y) \times (x',y') = (x \times x', y \times y') \\ 0_{R\times S} = (0_R, 0_S) \\ 1_{R\times S} = (1_R, 1_S) \end{cases}$$

pour tous $(x,y),(x',y') \in R \times S$.

II. Morphismes d'anneaux

Soient R, S et T des anneaux.

1) Définition

a) morphismes

Définition ANN.16
Soit $\varphi : R \longrightarrow S$. On dit que φ est un morphisme (d'anneaux, de R dans S) $\overset{\Delta}{\text{ssi}}$

$$\begin{cases} \forall x, y \in R, & \begin{cases} f(x +_R y) = f(x) +_S f(y) \\ f(x \times_R y) = f(x) \times_S f(y) \end{cases} \\ f(1_R) = 1_S. \end{cases}$$

Remarque
Autrement dit, un morphisme d'anneaux est une application compatible à l'addition et à la multiplication, et qui envoie le un sur le un.

Notation ANN.**17**
On note $\mathsf{Hom}_{(\mathsf{Ann})}(R,S)$ *l'ensemble des morphismes de* R *dans* S.

b) endomorphismes

Définition ANN.**18**
Un endomorphisme (d'anneau) de R *est un morphisme d'anneaux* $\varphi : R \longrightarrow R$.
On note $\mathsf{End}_{(\mathsf{Ann})}(R)$ *l'ensemble des endomorphismes de* R.

2) Exemples

- Si R est un anneau, $\mathrm{Id}_R : R \longrightarrow R$ est un morphisme.
- L'application
$$\begin{aligned} \mathscr{F}(\mathbb{R},\mathbb{R}) &\longrightarrow \mathbb{R} \\ f &\longmapsto f(0) \end{aligned}$$
est un morphisme d'anneaux.
- La conjugaison complexe
$$\begin{aligned} \mathbb{C} &\longrightarrow \mathbb{C} \\ z &\longmapsto \overline{z} \end{aligned}$$
est un morphisme d'anneaux.
- Si R est un anneau, l'application
$$\begin{aligned} \mathbb{Z} &\longrightarrow R \\ n &\longmapsto n \cdot 1_R \end{aligned}$$
est un morphisme d'anneaux.

3) Composition entre morphismes

Proposition ANN.**19**
Soient $\varphi : R \longrightarrow S$ *et* $\psi : S \longrightarrow T$. *Alors,*
$$\left.\begin{array}{l} \varphi \text{ morphisme} \\ \psi \text{ morphisme} \end{array}\right\} \implies \psi \circ \varphi \text{ morphisme.}$$

Démonstration. — .....

.....

.....

..... ■

4) Isomorphismes d'anneaux

Soit $\varphi : R \longrightarrow S$ un morphisme.

a) isomorphismes

Définition ANN.**20**
On dit que φ est un isomorphisme (d'anneaux) $\overset{\Delta}{\text{ssi}}$ φ *est bijectif.*

Proposition ANN.**21**
On a
$$\varphi : R \longrightarrow S \text{ isomorphisme} \implies \varphi^{-1} : S \longrightarrow R \text{ morphisme.}$$

b) automorphismes

Définition ANN. **22**
Un automorphisme (d'anneau) de R *est un isomorphisme d'anneaux* $\varphi : R \longrightarrow R$.
On note $\mathsf{Aut}_{(\mathsf{Ann})}(R)$ *l'ensemble des automorphismes de* R.

Exemple
La conjugaison complexe est un automorphisme de $\mathbb{C}$.

Exercice ANN. **23**
Montrer que $\left(\mathsf{Aut}_{(\mathsf{Ann})}(R), \circ, \mathrm{Id}_R\right)$ *est un groupe.*

5) Anneaux isomorphes

Définition ANN. **24**
On dit que R et S sont isomorphes $\overset{\Delta}{\text{ssi}}$

$$\exists \varphi : R \longrightarrow S : \ \varphi \text{ est un isomorphisme.}$$

6) Noyau

Soit $\varphi : R \longrightarrow S$ un morphisme d'anneaux.
En particulier, φ est un morphisme de groupes entre $(R, +_R, 0_R)$ et $(S, +_S, 0_S)$. On dispose donc de son noyau $\mathsf{Ker}(\varphi)$. On a encore

$$\boxed{\varphi \text{ injectif} \iff \mathsf{Ker}(\varphi) = \{0_R\}.}$$

III. Anneaux commutatifs

1) Définition

Définition ANN. **25**
Soit R *un anneau. On dit que* R est commutatif $\overset{\Delta}{\text{ssi}}$

$$\forall x, y \in R, \ \ xy = yx.$$

Remarques
- On s'efforcera de noter R les anneaux quelconques et A, B, C, *etc.* les anneaux commutatifs.
- La lettre « R » correspond à la première lettre de « *ring* », *anneau* en anglais.

2) Anneaux intègres

a) définition

Définition ANN.**26**
Soit A un anneau commutatif. On dit que A est intègre $\overset{\Delta}{\text{ssi}}$ *A est non nul et*

$$\forall a, b \in A, \qquad ab = 0_A \implies (a = 0_A \text{ ou } b = 0_A).$$

b) simplifiabilité dans un anneau intègre

Proposition ANN.**27**
Soit A un anneau intègre et soit $a \in A \setminus \{0_A\}$. Alors,

$$\forall b, c \in A, \qquad (ab = ac \implies b = c).$$

Démonstration. — .....

.....

.....

..... ■

IV. Corps

1) Définition

a) définition

Définition ANN.**28**
Soit A un anneau commutatif. On dit que A est un corps $\overset{\Delta}{\text{ssi}}$ $\mathsf{U}(A) = A \setminus \{0_A\}$.

Remarques

- Autrement dit, un anneau commutatif A est un corps, si et seulement si, tous les éléments de A sont inversibles sauf 0_A.
- Les corps sont notés K, L, *etc.* Parfois, on note également k un corps.
- Lorsqu'on se restreint aux corps $\mathbb{R}$ ou $\mathbb{C}$, on utilise le symbole $\mathbb{K}$.

Exercice ANN.**29**
Soit A un anneau commutatif non nul, soit K un corps et soit $\varphi : K \longrightarrow A$ un morphisme d'anneaux. Montrer que φ est injectif.

b) une notation

Ainsi, si K est un corps et si $x \in K \setminus \{0_K\}$, x est inversible. Son inverse x^{-1} est aussi notée $\dfrac{1}{x}$.

2) Exemples

a) exemples classiques

- $\mathbb{R}$ est un corps.
- $\mathbb{C}$ est un corps.
- $\mathbb{Q}$ est un corps.
- $\mathbb{Z}$ n'est un corps.

b) l'anneau nul n'est pas un corps

- Notons N un anneau nul.
- On a donc $N = \{0_N\}$. De plus, comme $0_N = 1_N$, on a $N = \{1_N\}$. Donc, tous les éléments de N sont inversibles. Donc, $\mathsf{U}(N) = N$.
- Donc, $\mathsf{U}(N) \neq N \setminus \{0_N\}$. Ainsi, on a montré :

Fait ANN.**30**
L'anneau nul n'est pas un corps.

3) Les corps sont intègres

Proposition ANN.**31**
Soit A un anneau. Alors,

$$A \text{ corps} \implies A \text{ intègre.}$$

Démonstration. —

- On suppose que A est un corps.
- Déjà, A est commutatif.
- Ensuite, A est non nul.
- Maintenant, soient $a, b \in A$ tels que $ab = 0_A$. On veut montrer que $a = 0_A$ ou $b = 0_A$.
  - ▷ Si $a = 0_A$, c'est terminé.
  - ▷ Sinon, on a $a \neq 0_A$ et donc, a est inversible. Comme $ab = 0_A$, on a

$$\frac{1}{a}ab = \frac{1}{a}0_A = 0_A.$$

Donc, $b = 0_A$.

■

V. L'anneau $\mathbb{Z}/n\mathbb{Z}$

Dans cette partie, on fixe $n \geqslant 2$.
On va munir $\mathbb{Z}/n\mathbb{Z}$ d'une structure d'anneau commutatif.

1) Rappels et notations

a) classes

- Si $a \in \mathbb{Z}$, on note $\overline{a}$ la classe d'équivalence de a pour la relation de congruence modulo n. On a donc
$$\overline{a} = \Big\{ b \in \mathbb{Z} \;\Big|\; b \equiv a \ [n] \Big\}.$$
On peut aussi écrire
$$\begin{aligned} \overline{a} &= \Big\{ a + kn \ ; \ k \in \mathbb{Z} \Big\} \\ &= \Big\{ \ldots, a-2n, a-n, a, a+n, a+2n, \ldots \Big\}. \end{aligned}$$
- Par exemple, on a
$$\overline{0} = n\mathbb{Z} = \Big\{ \ldots, -2n, -n, 0, n, 2n, \ldots \Big\}.$$
- On peut vérifier qu'on a
$$\boxed{\overline{0} = \overline{n}.}$$

b) ensemble-quotient et projection canonique

- On note
$$\boxed{\mathbb{Z}/n\mathbb{Z} \coloneqq \Big\{ \overline{a} \ ; \ a \in \mathbb{Z} \Big\}.}$$
- On peut montrer (à l'aide de la division euclidienne) que
$$\mathbb{Z}/n\mathbb{Z} = \Big\{ \overline{0}, \overline{1}, \ldots, \overline{n-1} \Big\}.$$
et donc en particulier que $\big|\mathbb{Z}/n\mathbb{Z}\big| = n$.
- La *projection canonique de* $\mathbb{Z}$ *sur* $\mathbb{Z}/n\mathbb{Z}$, notée π_n, est l'application définie par
$$\pi_n : \left\{ \begin{array}{ccc} \mathbb{Z} & \longrightarrow & \mathbb{Z}/n\mathbb{Z} \\ a & \longmapsto & \overline{a}. \end{array} \right.$$

2) Addition

a) un lemme

Lemme ANN.**32**
Soient $a, b, a', b' \in \mathbb{Z}$. *Alors,*
$$\left.\begin{array}{l} \overline{a} = \overline{a'} \\ \overline{b} = \overline{b'} \end{array}\right\} \implies \overline{a+b} = \overline{a'+b'}$$

Démonstration. —
- On suppose que $\overline{a} = \overline{a'}$ et $\overline{b} = \overline{b'}$.
- On a donc (pourquoi ?) : $a \equiv a' \ [n]$ et $b \equiv b' \ [n]$.
- Donc, d'après les propriétés de la congurence, on a $a + b \equiv a' + b' \ [n]$.
- Donc, on a $\overline{a+b} = \overline{a'+b'}$.

■

b) définition de l'addition

- On veut définir une addition sur $\mathbb{Z}/n\mathbb{Z}$. Soient donc $x, y \in \mathbb{Z}/n\mathbb{Z}$.
- On écrit
$$x = \overline{a} \quad \text{et} \quad y = \overline{b}.$$
avec $a, b \in \mathbb{Z}$.
- On aimerait poser
$$x + y \coloneqq \overline{a + b}. \tag{$*$}$$
- Pour cela, il faut vérifier que si on avait écrit également
$$x = \overline{a'} \quad \text{et} \quad y = \overline{b'}$$
alors on aurait $\overline{a + b} = \overline{a' + b'}$.
- C'est exactement ce que montre le lemme précédent.
- Ainsi, la formule $(*)$ est bien définie.

c) propriétés de l'addition

Fait ANN.**33**
Soient $x, y, z \in \mathbb{Z}/n\mathbb{Z}$. Alors,
1) $(x + y) + z = x + (y + z)$;
2) $x + y = y + x$;
3) $x + \overline{0} = \overline{0} + x = x$;
4) *il existe $x' \in \mathbb{Z}/n\mathbb{Z}$ tel que $x + x' = x' + x = \overline{0}$.*

Démonstration. — .....

.....

.....

.....

.....

.....

.....

.....

.....

..... ■

Autrement dit, on a montré que

Fait ANN.**34**
Le triplet $\left(\mathbb{Z}/n\mathbb{Z}, +, \overline{0}\right)$ est un groupe commutatif.

Exercice ANN.**35**
Montrer que $\left(\mathbb{Z}/n\mathbb{Z}, +, \overline{0}\right)$ *est cyclique.*

3) Multiplication

a) un lemme

Lemme ANN.**36**
Soient $a, b, a', b' \in \mathbb{Z}$. *Alors,*

$$\left.\begin{array}{l}\overline{a} = \overline{a'} \\ \overline{b} = \overline{b'}\end{array}\right\} \implies \overline{ab} = \overline{a'b'}$$

Démonstration. —

- On suppose que $\overline{a} = \overline{a'}$ et $\overline{b} = \overline{b'}$.
- On a donc (pourquoi ?) : $a \equiv a'\ [n]$ et $b \equiv b'\ [n]$.
- Donc, d'après les propriétés de la congurence, on a $ab \equiv a'b'\ [n]$.
- Donc, on a $\overline{ab} = \overline{a'b'}$.

■

b) définition de la multiplication

- On veut définir une multiplication sur $\mathbb{Z}/n\mathbb{Z}$. Soient donc $x, y \in \mathbb{Z}/n\mathbb{Z}$.
- On écrit
$$x = \overline{a} \quad \text{et} \quad y = \overline{b}.$$
avec $a, b \in \mathbb{Z}$.
- On aimerait poser
$$x \times y \coloneqq \overline{ab}. \tag{$**$}$$
- Pour cela, il faut vérifier que si on avait écrit également
$$x = \overline{a'} \quad \text{et} \quad y = \overline{b'}$$
alors on aurait $\overline{ab} = \overline{a'b'}$.
- C'est exactement ce que montre le lemme précédent.
- Ainsi, la formule $(**)$ est bien définie.

c) propriétés de la multiplication

Fait ANN.**37**
Soient $x, y, z \in \mathbb{Z}/n\mathbb{Z}$. *Alors,*

1) $(x \times y) \times z = x \times (y \times z)$;
2) $x \times y = y \times x$;
3) $x \times \overline{1} = \overline{1} \times x = x$;

Démonstration. — Elle est laissée au lecteur à titre d'entraînement. ■
Autrement dit, on a montré que

Fait ANN.**38**
Le triplet $\left(\mathbb{Z}/n\mathbb{Z}, \times, \overline{1}\right)$ *est un monoïde commutatif.*

4) Structure d'anneau

a) $\mathbb{Z}/n\mathbb{Z}$ est un anneau

Théorème ANN.**39**
Le 5-uplet $\left(\mathbb{Z}/n\mathbb{Z}, +, \times, \overline{0}, \overline{1}\right)$ *est un anneau commutatif.*

Démonstration. — .....

.....

.....

.....

.....

..... ■

b) la projection canonique est un morphisme

Fait ANN.**40**
L'application

$$\pi_n : \begin{cases} \mathbb{Z} \longrightarrow \mathbb{Z}/n\mathbb{Z} \\ a \longmapsto \overline{a}. \end{cases}$$

est un morphisme d'anneaux.

Démonstration. — .....

.....

.....

.....

.....

..... ■

5) Les $\mathbb{Z}/p\mathbb{Z}$ sont des corps

♛ **Théorème** ANN.**41**
On a

$$\mathbb{Z}/n\mathbb{Z} \text{ corps} \iff n \text{ est premier.}$$

Démonstration. — .....

.....

.....

■