Structures algébriques

« Les êtres mathématiques, en eux-mêmes, importent peu : ce qui compte ce sont leurs *relations*. »
Bourbaki, Algèbre I, Introduction.

1 Philosophie du chapitre

Un ensemble est un tout informe et inorganisé par nature. Chaque élément n'existe que pour ses propriétés propres, indépendamment des autres.
L'objet de ce chapitre est de créer des liens entre les éléments d'un même ensemble : de les faire interagir entre eux. On pourra ainsi *donner forme* à l'ensemble.

Ensuite, c'est le grand ménage : on classe les ensembles en fonction des opérations dont on les a dotés : les groupes, les anneaux, les corps... Puis on analyse chacune de ces structures pour en dégager toutes les règles et théorèmes que l'on peut obtenir.

Cette démarche abstraite, permet d'obtenir des propriétés très générales sur ces ensembles et nous pourrons ensuite les appliquer à des cas particuliers.

Par exemple, on pourrait observer que l'ensemble des polynômes sur $\mathbf{R}$, se comporte, à certains égards, de façon très similaire aux entiers relatifs $\mathbf{Z}$.

- On commence donc par analyser ce qui rapproche ces deux ensembles dans leur définition.
  On en liste un corpus d'axiomes cohérent.
- On cherche et démontre toutes les propriétés qui découlent de ces axiomes, en toute généralité (sans se référer à un ensemble particulier).
- On applique ensuite ces résultats à $\mathbf{R}[X]$ et à $\mathbf{Z}$, mais aussi à tous les autres ensembles dotés des axiomes.

Ainsi, plutôt que de démontrer chaque théorème deux fois : une fois pour $\mathbf{R}[X]$ et une autre fois $\mathbf{Z}$, on les démontre une seule fois, mais de façon plus abstraite et globale.

Il faut garder en mémoire que les opérations définies ici et leurs propriétés prennent appui sur des ensembles « naturels », mais on pourrait ensuite être tentés de construire de nouveaux ensembles en vérifiant d'autres qui nous semblent prometteuses.
Avec un peu d'audace, on résume donc l'algèbre à une vaste opération de nettoyage :

- On met les objets mathématiques dans des boîtes en fonction de leurs propriétés.
- On donne des noms à ces boîtes : groupes, algèbres, espaces vectoriels...
- On démontre chaque théorème une seule fois pour toute la « boîte » et on peut ensuite l'utiliser sans efforts pour chaque élément particulier.

L'idée est donc de travailler un peu plus aujourd'hui pour... travailler moins plus tard.

L'algèbre *linéaire* qui est étudiée de façon plus spécifique cette année consiste en l'étude d'une de ces « boîtes », la plus simple : la linéarité. C'est ce que l'on appelle traditionnellement la proportionnalité.

2 Opération interne

Définition 2.1 *(Opération interne)*

Soit E un ensemble, une **opération interne** $\star$ sur E est une application de E^2 dans E, c'est-à-dire telle que

$$\forall (x,y) \in E^2,\ x \star y \in E.$$

Explications

L'opération est interne pour qu'elle ne nous fasse pas « *sortir* » de l'ensemble E. On travaille en milieu clos sans avoir à se demander à chaque fois « être ou ne pas être dans l'ensemble ? », *that is not the question.*

Remarque : On parle de *magma* pour un ensemble muni d'une loi interne.

Définition 2.2 *(Loi associative, loi commutative)*

Une loi $\star$ sur E est dite **associative** sur E si

$$\forall (x,y,z) \in E^3,\ x \star (y \star z) = (x \star y) \star z.$$

Une loi $\star$ sur E est dite **commutative** sur E si

$$\forall (x,y) \in E^2,\ x \star y = y \star x.$$

Exemple

L'addition sur $\mathbf{Z}$ est associative et commutative.
La multiplication (sur $\mathbf{R}$ ou $\mathbf{C}$) est associative et commutative.
La division sur $\mathbf{R}^*$ n'est ni associative, ni commutative.
La soustraction sur $\mathbf{Z}$ n'est ni associative, ni commutative.
La multiplication matricielle est associative, mais pas commutative.
La composition de fonctions réelles est associative, mais non commutative.

Définition 2.3 *(Élément neutre)*

Une loi $\star$ définie sur E admet un **élément neutre**, s'il existe $e \in E$ tel que

$$\forall x \in E, \qquad x \star e = e \star x = x.$$

e est appelé l'élément neutre.

Propriété 2.4 *(Unicité de l'élément neutre)*

Si l'élément neutre existe, alors il est unique.

Preuve

Si on suppose que e et e' sont des éléments neutres pour $\star$, alors $e = e \star e' = e'$. ■

Exemple

L'élément neutre pour l'addition sur $\mathbf{Z}$ est 0.
L'élément neutre pour le produit sur $\mathbf{Z}$ est 1.

L'élément neutre n'a que peu d'intérêt en lui-même : il ne fait rien.
Par contre, il est utile pour définir le symétrique :

Définition 2.5 *(Symétrique)*

Soit $x \in E$,
x possède un **symétrique** pour la loi $\star$ s'il existe $y \in E$ tel que

$$x \star y = y \star x = e.$$

y est alors appelé le symétrique de x pour $\star$.

⚠ Le symétrique dépend de l'opération choisie. S'il y a plusieurs opérations définies sur l'ensemble, il faut savoir de laquelle on parle.

Exemple

- Le symétrique d'un nombre entier pour l'addition est son opposé.
  -5 est le symétrique de 5 dans $\mathbf{Z}$ pour la loi $+$.
- Sur $\mathbf{N}$ muni de l'addition, seul 0 admet un symétrique.
  L'absence de symétrique est un problème de $\mathbf{N}$: on n'a pas le droit de contracter des dettes. Pour palier à ce problème, on a donc inventé $\mathbf{Z}$.
- Sur $\mathbf{Q}^*$ muni de la multiplication, tous les éléments admettent un symétrique.

Propriété 2.6

L'élément neutre admet toujours un symétrique qui est lui-même.

Propriété 2.7 *(Unicité du symétrique)*

Pour une loi associative,
si un élément admet un symétrique, alors celui-ci est unique.

Preuve

Supposons que x ait deux symétriques y et z, alors $z = z \star (x \star y) = (z \star x) \star y = e \star y = y$.
■

Définition 2.8

- Lorsque la loi $\star$ est une addition, le symétrique est appelé l'**opposé**. L'opposé de x est noté $-x$.
- Lorsque la loi $\star$ est une multiplication, le symétrique est appelé l'**inverse**. L'inverse de x est noté x^{-1}.
- Lorsque la loi $\star$ est une composition, le symétrique est appelé la **réciproque**. La réciproque de f est noté f^{-1}.

Reste à savoir ce qu'est une addition, une multiplication ou une composition...
C'est une question d'usage :

- L'addition et la multiplication[1], sont souvent définis l'un par rapport à l'autre. Nous allons voir un peu plus loin la structure d'anneau qui est munie de deux opérations. Celle qui forme le groupe est l'addition et l'autre la multiplication.
- Le terme de composition est utilisé à la place de la multiplication lorsque l'on traite d'applications.

Propriété 2.9 *(Inversibilité du produit)*

Soit E muni d'une loi de composition multiplicative interne $\star$ et associative.
Soit $(x, x') \in E$.
Si x et x' admettent tous deux des inverses (symétriques) dans E pour la loi $\star$, alors $x \star x'$ admet aussi un inverse dans E égal à $x'^{-1} \star x^{-1}$.

Preuve

On note x^{-1} et x'^{-1} les inverses respectifs de x et x'.

$$\begin{aligned}(x \star x') \star (x'^{-1} \star x^{-1}) &= x \star (x' \star x'^{-1}) \star x^{-1} \qquad \text{(associativité)}\\ &= x \star (e) \star x^{-1}\\ &= x \star x^{-1} = e.\end{aligned}$$

On a de même $(x \star x') \star (x'^{-1} \star x^{-1}) = e$.
Ainsi $x \star x'$ admet un inverse qui vaut $x'^{-1} \star x^{-1}$. ■

Exemple

Écrire la même propriété en notation additive.

1. La somme est le résultat d'une addition, de même que le produit est le résultat d'une multiplication.

Définition 2.10 *(Élément régulier)*

Un élément $a \in E$ est dit **régulier à gauche** pour la loi $\star$ interne et associative si

$$\forall (x, y) \in E,\ a \star x = a \star y \Rightarrow x = y.$$

Il est dit **régulier à droite** si

$$\forall (x, y) \in E,\ x \star a = y \star a \Rightarrow x = y.$$

Il est dit **régulier** s'il est à la fois régulier à gauche et à droite.

Exemple

Un élément neutre est toujours régulier.

Définition 2.11 *(Partie stable)*

Soit E muni de la loi interne $\star$.
Une partie $E' \subset E$ est dite **stable** par $\star$, si

$$\forall (x, x') \in E',\ x \star x' \in E'.$$

C'est-à-dire si la loi $\star$ est interne dans E'.

Exemple

Si E admet un élément neutre e pour la loi $\star$, alors $\{e\}$ est stable par $\star$.

3 Groupes

Définition 3.1 *(Groupe)*

Un **groupe** est un ensemble G muni d'une loi *interne* $\star$ tel que :

- la loi $\star$ est associative,
- G contient un élément neutre e pour la loi $\star$,
- tout élément x de G admet un symétrique pour $\star$.

Lorsque la loi $\star$ est commutative, on dit que le groupe est commutatif, ou *abélien*.

En fonction des groupes étudiés, on adoptera parfois la notation multiplicative, parfois la notation additive.
Les résultats sont les mêmes, mais il faut être à l'aise avec les deux notations.
Usage : on réserve la notation additive pour les lois commutatives.

Exemple *(Groupes additifs)*

- $(\mathbf{N}, +)$ n'est pas un groupe car ses éléments non nuls n'admettent pas d'inverse.

- $(\mathbf{Z}, +)$ est un groupe commutatif.
- $(\mathbf{Q}, +)$, $(\mathbf{R}, +)$ et $(\mathbf{C}, +)$ sont des groupes commutatifs.
- $(\mathscr{M}_{n,p}(\mathbf{K}), +)$ est un groupe commutatif.

Exemple *(Groupes multiplicatifs)*

Pour avoir un groupe multiplicatifs sur les ensembles de nombres, il est nécessaire de retirer le 0 qui n'admet par d'inverse pour le produit.

- $(\mathbf{Z}^*, \times)$ n'est pas un groupe.
- $(\mathbf{Q}^*, \times)$, $(\mathbf{R}^*, \times)$ et $(\mathbf{C}^*, \times)$ sont des groupes commutatifs.
- $(\mathbf{U}, \times)$, l'ensemble des nombres complexes de module 1, muni du produit est un groupe commutatif.
- L'ensemble des rotations de centre O, muni de la loi de composition est un groupe.
- $(\mathrm{GL}_n(\mathbf{K}), \times)$ est un groupe non commutatif $(n \geqslant 2)$.

Exemple *(Un petit détour amusant)*

Le but de cet exemple est de montrer que l'associativité et la commutativité sont bien des notions distinctes. Les matrices donnent un exemple de loi qui est associative sans être commutative. L'idée ici est de trouver une loi commutative mais non associative.
Plutôt que de travailler avec les nombres, nous allons travailler avec des objets beaucoup plus simples (il n'y en aura que trois) que l'on nommera p comme « pierre », f comme « feuille » et c comme « ciseaux ».
Sur cet ensemble, nous définissons une opération $\star$ inspirée du jeu « pierre-feuille-ciseaux ». L'opération entre deux « actions » donne pour résultat le vainqueur[2].
Par exemple, pour $p \star f$, le résultat est f car c'est la feuille qui gagne contre la pierre. Dans le cas où les deux « actions » sont identiques, alors l'opération renvoie l'action elle-même).
On note $M = \{p, f, c\}$, l'ensemble de travail. On peut alors résumer la loi avec une *table de Cayley* :

$\star$	p	f	c
p	p	f	p
f	f	f	c
c	p	c	c

Ce tableau se lit ainsi : pour calculer $p \star f$, on prend la ligne p et la colonne f et on lit le résultat : $p \star f = f$.
Cela correspond bien au jeu : entre la pierre et la feuille, c'est la feuille qui gagne.
L'opération sur M est *interne*. En effet, $\forall (x, y) \in M^2$, $x \star y \in M$ (le résultat d'une opération est toujours un des trois éléments p, f ou c).
L'opération est clairement *commutative* : $\forall (x, y) \in M^2$, $x \star y = y \star x$ (l'ordre n'a pas d'importance entre les deux joueurs).
Par contre, cette opération n'admet *pas d'élément neutre* (tout élément agit de façon non triviale sur les autres) : la structure $(M, \star)$ n'est pas un groupe. On dit que c'est un *magma* commutatif (une façon de dire que ce n'est pas très ordonné...).
Ce magma n'est pas non plus *associatif*.
Prenons un exemple :

$$p \star (f \star c) = p \star c = p \qquad \text{et} \qquad (p \star f) \star c = f \star c = c.$$

On voit donc que

$$p \star (f \star c) \neq (p \star f) \star c.$$

C'est simplement une façon mathématique de dire que l'on ne peut pas jouer à ce jeu à trois en même temps.
Si on voulait avoir un élément neutre, il faudrait rajouter un élément qui perd à chaque fois.
On pourrait l'appeler n de tel sorte que $\forall x \in M \ : n \star x = x$.
Grâce à cet élément neutre, on peut construire un symétrique pour chaque élément de M en imposant que $\forall x \in M$, $x \star x = n$.
Ainsi, chaque élément est son propre symétrique.
On modifie donc les règles du jeu et on obtient une nouvelle table de Cayley :

$\star$	n	p	f	c
n	n	p	f	c
p	p	n	f	p
f	f	f	n	c
c	c	p	c	n

On n'est pas très loin d'un groupe, mais il manque, encore et toujours l'associativité !

Définition 3.2 *(Sous-groupe)*

Soit $(G, \star)$ un groupe.
Un **sous-groupe** de $(G, \star)$ est un groupe $(G', \star)$ avec G' une partie stable de G pour la loi $\star$.

Théorème 3.3 *(Caractérisation des sous-groupes)*

Soit $(G, \star)$ un groupe et $G' \subset G$.
$(G', \star)$ est un sous-groupe de $(G, \star)$ si, et seulement si

1. G' contient l'élément neutre de G.
2. $\forall (x, x') \in (G')^2$, $x \star x'^{-1} \in G'$.

2. Honte à ceux qui ne connaissent pas ce jeu !

Remarques :

- On peut remplacer $e \in G'$ par G' non vide, car alors le second point nous donne $e = x \star x^{-1} \in G'$ pour un certain x.
  Le second point peut être vérifié en deux étapes :
  1. stabilité par produit,
  2. stabilité par passage à l'inverse.

Preuve

Le sens direct est trivial.
Pour le sens réciproque,

- Contient l'élément neutre par hypothèse.
- Contient l'inverse de tout élément (en prenant $x = e$).
- Stable par produit car si, $(x, x') \in (G')^2$ alors, d'après le point précédent ${x'}^{-1} \in G'$, donc en appliquant la formule à $(x, {x'}^{-1})$, on obtient $x \star x' \in G'$.
  La loi est donc bien interne.
- L'associativité est directement héritée de G.

■

Exemple

$\left(\mathbf{Q}_+^*, \times\right)$ est-il un groupe ? Même question pour $\mathbf{R}_+^*$.
Solution :
Oui, ce sont des sous-groupes de $(\mathbf{Q}^*, \times)$ et $(\mathbf{R}^*, \times)$.

Exemple

Montrer que l'ensemble des racines n-ièmes de l'unité $\mathbf{U}_n = \left\{ \mathrm{e}^{\frac{2ik\pi}{n}} \right\}_{k \in [\![0, n-1]\!]}$ muni du produit est un groupe.

Exemple

Montrer que tout élément d'un groupe est régulier.
Solution :
Soit G le groupe (noté multiplicativement).
Soit $x \in G$, montrons que x est régulier.
Soient $(y, z) \in G^2$ tels que $xy = xz$, alors en multipliant par x^{-1} à gauche, on trouve $y = z$.
Ainsi x est régulier à gauche, on montre de même qu'il est régulier à droite en multipliant à droite par x^{-1}. Ceci prouve que x est régulier.

Exemple

Montrer que si G' est un sous-groupe de G, alors son complémentaire dans G n'en est pas un.
Solution :
Il ne contient pas l'élément neutre.

Propriété 3.4 *(Puissances)*

Soit $(G, \star)$ un groupe (notation multiplicative).
Soit $x \in G$.
On définit par récurrence les puissances de x avec

$$\begin{cases} x^0 = e, \\ \forall n \in \mathbf{N},\ x^{n+1} = x^n \star x = x \star x^n, \\ \forall n \in \mathbf{N},\ x^{-n} = \left(x^{-1}\right)^n = \left(x^n\right)^{-1}. \end{cases}$$

On a alors :

- $\forall x \in G,\ \forall n \in \mathbf{Z},\ x^n \in G$.
- $\forall (n, p) \in \mathbf{Z},\ x^{n+p} = x^n \star x^p$.

⚠ En général $(x \star y)^n \neq x^n \star y^n$ (sauf si G est un groupe commutatif).

Preuve

- G est un groupe, donc il admet bien un élément neutre que l'on peut noter e.
  La définition de x^0 est donc correcte.
- On montre par récurrence sur $n \in \mathbf{N}$ que $x^n \in G$ et $x^n \star x = x \star x^n$.
  L'initialisation est immédiate.
  Pour l'hérédité, $x^n \in G$ et $x \in G$, donc $x^{n+1} \in G$ car la loi est interne.
  De plus, $x^{n+1} \star x = (x \star x^n) \star x = x \star (x^n \star x) = x \star (x \star x^n) = x \star x^{n+1}$.
- Pour x^{-n}, on remarque déjà que si $x \in G$, alors $x^{-1} \in G$ et d'après le résultat précédent, pour tout $n \in \mathbf{N}$, $(x^{-1})^n \in G$.
  On montre ensuite l'égalité par récurrence.
  Initialisation : $x^{-0} = x^0 = e = e^{-1} = \left(x^{-1}\right)^0$.
  Hérédité : on suppose l'égalité au rang $n \in \mathbf{N}$, alors $\left(x^{n+1}\right) \star \left(x^{-1}\right)^{n+1} = x \star x^n \star \left(x^{-1}\right)^n \star x^{-1}$.
  Et par hypothèse de récurrence, $\left(x^{-1}\right)^n = (x^n)^{-1}$ donc $x^n \star \left(x^{-1}\right)^n = e$ et on obtient donc $\left(x^{n+1}\right) \star \left(x^{-1}\right)^{n+1} = x \star e \star x^{-1} = e$.
  (on fait le même raisonnement pour le calcul dans l'autre ordre).
  Ceci prouve donc l'hérédité.
- Pour montrer que $x^{n+p} = x^n \star x^p$, on procède par récurrence sur $p \in \mathbf{N}$.
  Pour $p = 0$, l'égalité et vraie pour tout $n \in \mathbf{Z}$ car $x^p = x^0 = e$.
  On suppose l'égalité pour un rang $p \in \mathbf{N}$ fixé, alors $x^{n+p+1} = x^{(n+1)+p}$ et on applique l'hypothèse de récurrence avec $n+1$ ce qui donne $x^{n+p+1} = x^{n+1} \star x^p = x^n \star x \star x^p = x^n \star x^{p+1}$ en utilisant les résultats montrés aux points précédents.
  Ceci prouve l'égalité pour tout $p \in \mathbf{N}$.
  Pour $p < 0$, on passe simplement à l'inverse en utilisant les résultats déjà démontrés.

$$x^{n+p} = \left(x^{-1}\right)^{-n-p} = \left(x^{-1}\right)^{-n} \star \left(x^{-1}\right)^{-p} = x^n \star x^p.$$

■

Propriété 3.5 *(Notation additive)*

En notation additive, pour le groupe $(G, +)$, la propriété précédente s'écrit :

$$\begin{cases} 0x = e. \\ \forall n \in \mathbf{N},\ (n+1)x = nx + x = x + nx. \\ \forall n \in \mathbf{N},\ (-n)x = -(nx) = n(-x). \end{cases}$$

On a alors :

- $\forall x \in G,\ \forall n \in \mathbf{Z},\ nx \in G.$
- $\forall (n, p) \in \mathbf{Z},\ (n+p)x = nx + px.$

Exemple

Soit $P \in \mathbf{K}[X]$, on note E l'ensemble des racines de P dans $\mathbf{K}$.
L'ensemble E, muni de la multiplication est-il un groupe ?
Exercice relativement facile sur $\mathbf{R}$*, mais difficile sur* $\mathbf{C}$.

Solution :

Analyse : Si P n'admet aucune racine, ce n'est pas un groupe car E est vide.
Donc P admet au moins une racine $\alpha \in \mathbf{K}$.

- Si $|\alpha| > 1$, alors $\{\alpha^n,\ n \in \mathbf{Z}\}$ forme une famille de scalaires deux à deux distincts (modules distincts). Donc E qui contient cette famille (stabilité) est infini.
  Donc P possède une infinité de racines, donc P est nul.
- Si $|\alpha| \in]0,\ 1[$, c'est la même chose avec $\frac{1}{\alpha} \in E$.
- Si $\alpha = 0$. Cela suppose que 0 soit inversible pour le produit.
  Ce n'est évidemment pas le cas, car pour tout $x \in \mathbf{K}$, $x \times 0 = 0$.
  Mais on peut faire preuve d'audace et supposer que $0 = 1$, pour obtenir l'inversibilité.
  Il est alors immédiat que l'ensemble peut former un groupe à la seule condition d'être réduit à un seul point. Alors $\alpha = 0$ est la seule racine et P s'écrit sous la forme $X^n R$ avec $n \in \mathbf{N}^*$ et R un polynôme sans racines.

Avant de traiter le cas $|\alpha| = 1$, on peut rédiger une synthèse partielle :
Synthèse « partielle » :
Si P est nul, alors 1 est l'élément neutre, mais $0 \in E$ n'admet pas d'inverse, donc E n'est pas un groupe.
S'il existe $n \in \mathbf{N}^*$ et $\mathbf{R} \in \mathbf{K}[X]$ sans racines tel que $P = X^n R$.
Alors $E = \{0\}$ que l'on peut considérer comme un groupe d'élément neutre 0 pour la loi $\times$.
Ainsi pour $\mathbf{K} = \mathbf{C}$ on a nécessairement $R = \lambda \in \mathbf{K}^*$ (ce qui est aussi suffisant).
Pour $\mathbf{K} = \mathbf{R}$, R s'écrit sous forme de produit de polynômes de degré 2 à discriminants strictement négatifs.
Dernière situation et non des moindres.
Supposons qu'il existe une racine α de module 1.
D'après les derniers cas, on sait que toute racine est alors nécessairement de module 1.

- Si $\mathbf{K} = \mathbf{R}$, alors $\alpha = 1$ ou $\alpha = -1$ et on peut écrire $P = (X-1)^p (X+1)^q R$ avec $(p, q) \in \mathbf{N}^2$ et R sans racines.
  - Si 1 est la seule racine, alors $E = \{1\}$ qui est bien un groupe pour $\times$.
  - Si -1 est racine, $1 = (-1)^2$ est aussi racine et $E = \{-1, 1\}$ qui est bien un groupe pour $\times$.

  On a donc $p \geqslant 1$ et $q \in \mathbf{N}$.
- Si $\mathbf{K} = \mathbf{C}$, on note $\alpha = \mathrm{e}^{i\theta}$.
  Comme E est stable par produit et qu'on suppose P non nul on a donc $\{\alpha^n,\ n \in \mathbf{Z}\}$ qui est un ensemble fini, donc il existe $p > q$ tel que $\mathrm{e}^{ip\theta} = \mathrm{e}^{iq\theta}$.
  Donc $(p-q)\theta \equiv 0\ [2\pi]$.
  Ainsi θ s'écrit sous la forme $\theta = \frac{2k\pi}{n}$ (avec $n = p - q > 0$).
  Comme l'angle est égal à 2π près, on peut choisir $k \in [\![0,\ n-1]\!]$ et également supposer la fraction irréductible.
  On sait que $\mathrm{e}^{i\theta} \in E$ et pour tout $u \in \mathbf{Z}$, $\mathrm{e}^{i\theta u} \in E$ par stabilité avec la puissance.
  Or $k \wedge n = 1$ (fraction irréductible) donc on peut trouver $(u, v) \in \mathbf{Z}^2$ tel que $ku + nv = 1$, donc
  $$\mathrm{e}^{i\theta u} = \mathrm{e}^{2i\pi \frac{ku}{n}} = \mathrm{e}^{2i\pi \frac{1-nv}{n}} = \mathrm{e}^{\frac{2i\pi}{n}} \in E.$$
  Ainsi E contient les racines n-ièmes de l'unité.
  On voit que réciproquement, $\alpha = \mathrm{e}^{i\theta} = \mathrm{e}^{\frac{2ik\pi}{n}} \in \mathbf{U}_n$.
  Donc toute racine de P est nécessairement racine n-ième de l'unité et si pour $n \in \mathbf{N}^*$ fixé, une racine n-ième est dans E, alors toutes les racines n-ièmes (pour le même n) le sont aussi.
  On peut donc écrire P sous la forme
  $$P = \lambda \prod_{\alpha \in U} (X - \alpha)^{m_\alpha}$$
  où U désigne une union finie d'ensembles $\mathbf{U}_n$ $n \in \mathbf{N}^*$ et pour tout $\alpha \in U$, $m_\alpha \geqslant 1$.
  On peut note $U = \bigcup_{n \in I} \mathbf{U}_n$ avec I un sous-ensemble fini non vide de $\mathbf{N}^*$.
  Reste à s'assurer que E est stable par produit.
  Cela suppose que si $p \in I$ et $q \in I$, alors pour tout $(k, k') \in \mathbf{Z}^2$ $\mathrm{e}^{2i\pi\left(\frac{k}{p} + \frac{k'}{q}\right)} \in E$.
  En écrivant $p = dp'$ et $q = dq'$ pour $d = p \wedge q$, alors on obtient $\mathrm{e}^{2i\pi \frac{kq' + k'p'}{dpq'}} \in E$.
  On a $p' \wedge q' = 1$ et d'après Bezout, on peut donc choisir $kq' + k'p' = 1$ pour les bonnes valeurs de k et k'.
  On remarque alors que $dp'q' = p \vee q \in I$, ainsi I doit être stable par passage au PPCM.
  Mais, toute racine p-ième de l'unité est aussi racine $(p \vee q)$-ième de l'unité, de même pour les racines q-ièmes et on a donc $\mathbf{U}_p \cup \mathbf{U}_q \subset \mathbf{U}_{p \vee q}$.
  Ainsi, en prenant le PPCM de tous les éléments de I que l'on peut noter n on obtient que $U = \mathbf{U}_n$.
  Réciproquement, il est évident que cela convient et P s'écrit
  $$P = \lambda \prod_{\alpha \in \mathbf{U}_n} (X - \alpha)^{m_\alpha}$$
  avec $\lambda \in \mathbf{C}^*$, $n \in \mathbf{N}^*$ et pour tout $\alpha \in \mathbf{U}_n$, $m_\alpha \in \mathbf{N}^*$.

Théorème 3.6 *(Groupe symétrique)*

Soit X un ensemble non vide.
L'ensemble des bijections (*permutations*) sur X muni de la composition forme un groupe, appelé **groupe symétrique** ou **groupe des permutations**
On le note S_X.
Son élément neutre est l'application identité.

Si $X = [\![1, n]\!]$, alors on note l'ensemble S_n.

Preuve

$\mathrm{Id}_X \in S_X$, la composée de deux bijections est une bijection, et la réciproque d'une bijection est une bijection.
Enfin, la composition est associative. ■

Une fonction de n variable est dite *symétrique*, lorsqu'elle est invariante par permutation de ses variables. C'est la raison pour laquelle, le groupe correspondant aux dites permutations est appelé groupe symétrique.

4 Morphismes des groupes

Définition 4.1 *(Morphisme de groupes)*

Soient $(G, \times)$ et $(G', \star)$ deux groupes (notés multiplicativement).
Soit $f : G \to G'$ une application.
f est un **morphisme de groupe**, si, et seulement si

$$\forall (x, x') \in G^2,\ f(x \times x') = f(x) \star f(x').$$

Définition 4.2 *(Endomorphisme)*

Définition hors programme, mais usuelle.
Si $G' = G$ dans les notations de la définition précédente, alors on dit que f est un **endomorphisme (de groupe).**

Remarque : Il existe autant de type de morphismes que de structures algébriques. Nous en verrons donc d'autres ailleurs.
C'est la raison pour laquelle, nous précisons que c'est un morphisme *de groupes.*
Cependant, lorsqu'il n'y a pas d'ambigüité sur la structure concernée, on parlera simplement de morphisme.

Explications

Un morphisme entre les groupes G et G' est une application compatible avec les opérations des groupes.
Ainsi, lorsque l'on réalise une opération sur G, cela revient à réaliser la même opération sur les images.
Les morphismes de groupes permettent en particulier de transporter la structure et donc d'obtenir que des résultats démontrés sur G soient directement valables sur G'.

Propriété 4.3

Soit $f : G \to G'$ un morphisme de groupe. Si e est l'élément neutre de G et e' celui de G', alors

- $f(e) = e'$.
- $\forall x \in G,\ f\left(x^{-1}\right) = (f(x))^{-1}$.

En utilisant les notations multiplicatives.

Preuve

- $f(e) = f\left(e^2\right) = (f(e))^2$.
  Or $f(e) \in G'$ admet un inverse, et donc en multipliant l'égalité du dessus par cet inverse on obtient
  $$e' = f(e).$$
- Soit $x \in G$ $e' = f(xx^{-1}) = f(x) f\left(x^{-1}\right)$ et $e' = f(x^{-1}x) = f\left(x^{-1}\right) f(x)$.
  Donc $f\left(x^{-1}\right) = (f(x))^{-1}$.

■

Exemple

Soient G et G' deux groupes (multiplicatifs) et e' l'élément neutre de G'.
Soit $f : G \to G'$, défini par

$$\forall x \in G,\ f(x) = e'.$$

Montrer que f est un morphisme de groupe.

Exemple

Soit $f : \mathbf{Z} \to G'$ un morphisme de groupes.

1. Montrer que la donnée de $f(1)$ détermine complètement le morphisme.
2. En déduire tous les morphismes de groupes de $\mathbf{Z}$ dans $(\mathbf{Q}, +)$.

Définition 4.4 *(Noyau et image)*

Soit $f : G \to G'$ un morphisme de groupes.
On note e' l'élément neutre de G'.

- L'**image** de f, notée $\mathrm{Im}(f)$ est l'image directe de G par f :
  $$\mathrm{Im}(f) = f(G) = \{f(x),\ x \in G\} \subset G'.$$
- Le **noyau** de f, noté $\ker(f)$ est l'image réciproque de $\{e'\}$ par f :
  $$\ker(f) = f^{-1}(\{e'\}) = \{x \in G,\ f(x) = e'\} \subset G.$$

Théorème 4.5

Soit $f : G \to G'$ un morphisme de groupe.
$\ker(f)$ et $\mathrm{Im}(f)$ sont des sous groupes respectifs de G et G'.
Plus généralement, si

- H est un sous groupe de G alors $f(H)$ est un sous groupe de G'.
- H' est un sous groupe de G' alors $f^{-1}(H')$ est un sous groupe de G.

Preuve

On montre directement le cas général.
L'image est le noyau n'en sont que des cas particuliers. En effet $\mathrm{Im}(f) = f(G)$ avec G sous groupe de lui-même et $\ker(f) = f^{-1}(\{e'\})$ où $\{e'\}$ est bien un sous groupe de G'.

- On considère donc H sous groupe de G.
  Montrons que $H' = f(H)$ est un sous-groupe de G'.
  Il est tout d'abord évident que $H' \subset G'$ par définition de f.
  - $e \in H$, car c'est un sous groupe de G et $f(e) = e'$, donc $e' \in H'$.
  - Soit $(y, y') \in H'^2$, alors par définition de H', il existe $(x, x') \in H^2$ tel que $y = f(x)$ et $y' = f(x')$.
    Or $xx'^{-1} \in H$ (groupe) et $f\left(xx'^{-1}\right) = f(x)\left(f(x')\right)^{-1}$ (morphisme de groupes).
    Donc $yy'^{-1} = f\left(xx^{-1}\right) \in f(H) = H'$.

  H' est donc bien un sous groupe de G'.
- On considère à présent H' que l'on suppose un sous groupe de G' (sans lien avec les notations utilisées pour la preuve de l'image directe), et on note $H = f^{-1}(H')$.
  Montrons que H est un sous-groupe de G.
  Il est déjà évident, par définition, que $H \subset G$.
  - $f(e) = e' \in H'$ car H' est un sous-groupe de G' et f un morphisme de groupes.
    Donc $e \in f^{-1}(H') = H$.
  - Soit $(x, x') \in H^2$.
    Par définition $f(x) \in H'$ et $f(x') \in H'$ donc $f\left(xx'^{-1}\right) = f(x)\left(f(x')\right)^{-1} \in H'$ donc $xx'^{-1} \in H$.

  Ce qui prouve donc bien que H est un sous groupe de G.

■

Théorème 4.6

Soit $f : G \to G'$ un morphisme de groupes.

$$f \text{ est injectif si, et seulement si } \ker(f) = \{e\}.$$

Où e désigne l'élément neutre de G.

Preuve

Si f est injective, alors e' l'élément neutre de G' admet au plus un antécédent par f.
Or $f(e) = e'$, donc e est l'unique antécédent de e' par f.
Donc $\ker(f) = \{e\}$.
Réciproquement : si $\ker(f) = \{e\}$ alors on considère $(x, x') \in G^2$ tel que $f(x) = f(x')$.
Ainsi $f(x)\left(f(x')\right)^{-1} = e'$ donc $f\left(xx'^{-1}\right) = e'$.
Donc $xx^{-1} \in \ker(f) = \{e\}$ donc $x = x'$ ce qui prouve bien que le morphisme est injectif.

■

Définition 4.7 *(Isomorphisme)*

Soit $f : G \to G'$ un morphisme de groupe.
f est un **isomorphisme** (de groupe) si f est bijective.
Hors programme, mais d'usage courant :
Si de plus, f est un endomorphisme de groupes, alors on dit que f est un **automorphisme.**
On note $\mathrm{Aut}(G)$ l'ensemble des automorphismes sur G.

Exemple

L'application identité de $G \to G$ est un isomorphisme de groupe.
Comme le groupe de départ et le groupe d'arrivée sont les même, on peut dire que c'est un automorphisme.

⚠ Pour montrer que f est un isomorphisme, il ne suffit pas en général de montrer que l'application est bijective. Il ne faut pas oublier de montrer que c'est un morphisme.

Propriété 4.8

Si $f : G \to G'$ est un isomorphisme, alors sa réciproque, f^{-1} est aussi un isomorphisme.

Preuve

Ce n'est pas le caractère bijectif de f^{-1} qui nous intéresse ici (c'est une trivialité), mais le fait que f^{-1} soit lui-même un morphisme de groupes.
Soit $(y, y') \in (G')^2$, alors, $f\left(f^{-1}(y)f^{-1}(y')\right) = f\left(f^{-1}(y)\right) f\left(f^{-1}(y')\right) = yy'$.
Donc $f^{-1}(y)f^{-1}(y')$ est un antécédente de yy' par f, et par injectivité de f, il est donc égal à $f^{-1}(yy')$, ce qui prouve bien que

$$f^{-1}(yy') = f^{-1}(y)f^{-1}(y').$$

■

Méthode

Pour montrer qu'un endomorphisme d'un groupe *fini* est un automorphisme, il suffit de montrer qu'il est injectif : son noyau est réduit à l'élément neutre.

Exemple *(Fondamental)*

Soit G un groupe, et $g \in G$. On définit

$$f_g : \left\{ \begin{array}{ccc} G & \to & G \\ x & \mapsto & gxg^{-1}. \end{array} \right.$$

1. Montrer que f est un automorphisme.

2. On note Z l'ensemble des $g \in G$ tel que l'automorphisme f_g correspondant soit l'application identité.
Montrer que Z est un sous-groupe de G.
Comment décrire simplement ses éléments ?

Solution :

1. f est un morphisme, car $\forall (x, y) \in G^2$, $f(xy) = gxyg^{-1} = gxg^{-1}gyg^{-1} = f(x)f(y)$.
$f_{g^{-1}}$ est clairement le morphisme réciproque de f donc f est un isomorphisme.
2. $g \in Z \iff \forall x \in G,\ gxg^{-1} = x \iff \forall x \in G,\ gx = xg$.
Ainsi Z est l'ensemble des éléments qui commutent avec tous les autres. On dit que Z est le *centre* de G.
On a clairement $e \in Z$, avec e l'élément neutre.
Si $x \in Z$, alors $\forall g \in G$, $gx^{-1} = x^{-1}xgx^{-1}$.
Or $xg = gx$, donc $gx^{-1} = x^{-1}gxx^{-1} = x^{-1}g$, donc $x^{-1} \in Z$.
Si $(x, y) \in Z^2$, alors $\forall g \in G$, $gxy = xgy = xyg$, donc $xy \in Z$.
Ce qui prouve bien que Z est un sous-groupe de G.
On peut aussi voir $\mathbf{Z}(G)$ comme le noyau de l'application

$$\varphi : \left\{ \begin{array}{ccc} G & \to & S_G \\ g & \mapsto & (x \mapsto gxg^{-1}) \end{array} \right.$$

5 Anneaux et corps

Définition 5.1 *(Anneau)*

$(A, +, \times)$ est un **anneau** si

1. $(A, +)$ est un groupe commutatif.
2. La loi $\times$ vérifie :
   (a) $\times$ est une loi *interne* : $\forall (x, x') \in A^2$, $x \times x' \in A$,
   (b) $\times$ est *associative* : $\forall (x, x', y) \in A^3$, $(x \times x') \times y = x \times (x' \times y)$,
   (c) $\times$ est distributive par rapport à $+$:
   $\forall (x, x', y) \in A^3$, $(x + x') \times y = x \times y + x' \times y$.
   (d) $\times$ admet un élément neutre (souvent noté 1 ou 1_A) et appelé élément **unité** :
   $\forall x \in A$, $x \times 1_A = 1_A \times x = x$.

Si, de plus $\times$ est commutative, alors, l'anneau est commutatif.

Définition 5.2 *(Corps)*

$(K, +, \times)$ est un **corps** (commutatif) si

1. $(A, +, \times)$ est un anneau commutatif non réduit à $\{0\}$.
2. tout élément de $K^* = K \setminus \{0\}$ admet un symétrique pour la loi $\times$.

$$\forall x \in K \setminus \{0\},\ \exists x' \in K,\ \text{tel que } x \times x' = 1.$$

x' est appelé l'**inverse** de x et noté $x^{-1} = \frac{1}{x}$.

Remarque : Pour utiliser la notation $\frac{1}{x}$ et travailler avec des fractions, il est nécessaire que l'opération soit commutative.
Dans le cadre du programme, tout corps est supposé commutatif.
On verra plus loin que la condition $K \neq \{0\}$ peut s'écrire aussi $0_K \neq 1_K$.

Exemple

- $(\mathbf{Z}, +, \times)$ est un anneau (commutatif).
- $(\mathbf{Q}, +, \times)$ est un corps.
- $(\mathscr{M}_n(\mathbf{R}), +, \times)$ est un anneau (non commutatif).
- $(\mathbf{R}, +, \times)$ est un corps.
- $(\mathbf{C}, +, \times)$ est un corps.

Propriété 5.3 *(Règles de calcul)*

Soit $(A, +, \times)$ un anneau.
$\forall (a, b) \in A^2$,

1. 0_A est absorbant : $a \times 0_A = 0_A \times a = 0_A$.
2. $-a = (-1_A) \times a = a \times (-1_A)$.
3. $\forall n \in \mathbf{Z}$, $n(a \times b) = (na) \times b = a \times (nb)$.
4. $(-a) \times (-b) = a \times b$.

Preuve

1. $a \times 0_A = a \times (0_A + 0_A) = a \times 0_A + a \times 0_A$.
Donc en soustrayant $a \times 0_A$, on obtient le résultat voulu.
2. $a + (-1_A \times a) = 1_A \times a + (-1_A) \times a = (1 - 1_A) \times a = 0_A$.
On a donc bien $-1_A \times a = -a$.
3. On montre d'abord la propriété par récurrence sur $n \in \mathbf{N}$.
Initialisation : pour $n = 0$, on a $0(ab) = 0_A$ car on a montré que 0_A est absorbant.
Or $(0_A a) \times b = 0_A \times b = 0_A$ et de même $a \times (0_A b) = 0_A$ ce qui donne donc l'égalité

cherchée.
Hérédité : on suppose la relation vraie au rang $n \in \mathbf{N}$.

$$\begin{aligned}
\text{Alors } (n+1)(a\times b) &= n(a\times b)+a\times b && (n+1)x = nx+x \text{ avec } x = a\times b\\
&= (na)\times b + a\times b && \text{H.R.}\\
&= (na+a)\times b && \text{distributivité}\\
&= ((n+1)a)\times b && (n+1)x = nx+x \text{ avec } x = a.
\end{aligned}$$

$$\begin{aligned}
\text{De même } (n+1)(a\times b) &= n(a\times b)+a\times b && (n+1)x = nx+x \text{ avec } x = a\times b\\
&= a\times (nb)+a\times b && \text{H.R.}\\
&= a\times (nb+b) && \text{distributivité}\\
&= a\times ((n+1)b) && (n+1)x = nx+x \text{ avec } x = b.
\end{aligned}$$

Ce qui prouve bien l'hérédité.
La propriété est donc vraie pour tout $n \in \mathbf{N}$.
Pour $-n \leqslant 0$, on écrit :

$$\begin{aligned}
(-n)(a\times b) &= -(n(a\times b) && (-n)x = -(nx) \text{ avec } x = a\times b\\
&= -((na)\times b) && \text{cas précédent } n \geqslant 0\\
&= (-(na)\times b) && \text{car } (-x)\times y + (x\times y) = 0\\
&= ((-n)a)\times b && \text{car } -nx = (-n)x.
\end{aligned}$$

On fait de même avec b.

4. On utilise les points précédents : $(-a)\times(-b) = -(a\times(-b)) = -(-(a\times b)) = a\times b$.

■

Exemple

Un anneau A contient donc au moins 0 l'élément neutre du groupe, et 1 l'élément unité (neutre du produit).
Donner une condition nécessaire et suffisante sur A pour que $0 \neq 1$.
Solution :
Si $0 = 1$, alors d'après le caractère absorbant du 0, pour tout $x \in A$, $x = 1\times x = 0\times x = 0$.
Donc $A = \{0\}$.
La réciproque est évidente (on vérifie bien que $\{0\}$ est un anneau).

Définition 5.4 *(Anneau intègre)*

On dit qu'un anneau non nul $(A, +, \times)$ est **intègre**, s'il est commutatif et si

$$\forall (x, x') \in A^2,\ x\times x' = 0_A \Rightarrow x = 0_A \text{ ou } x' = 0_A.$$

Exemple

$(\mathbf{Z}, +, \times)$ est un anneau intègre.
$(\mathbf{R}[X], +, \times)$ est aussi un anneau intègre.
$(\mathscr{M}_n(\mathbf{R}), +, \times)$ est un anneau non intègre $(n \geqslant 2)$.
Tout corps est un anneau intègre.

Exemple *(À connaître)*

Montrer que tout anneau fini intègre est un corps.
On appelle anneau fini, un anneau qui ne contient qu'un nombre fini d'éléments.

Solution :
Cela revient à montrer que tout élément non nul de l'anneau admet un inverse.
Soit $x \in A^*$, on considère $E = \{x\times x', \text{pour } x' \in A\}$.
E est un sous-ensemble de A car $\times$ est une loi interne. Les éléments de E sont deux à deux distincts. En effet si $x\times x' = x\times x''$, alors $x\times x' - x\times x'' = 0$ (A est un groupe pour la loi $+$, donc les éléments admettent un symétrique).
Et par distributivité $x\times(x' - x'') = 0$.
Or l'anneau est intègre et $x \neq 0$, donc $x' - x'' = 0$, donc $x = x''$.
Ainsi E contient autant d'éléments que A et il est inclus dans A.
Donc $E = A$.
En particulier $1 \in E$, donc $\exists x' \in A$ tel que $x\times x' = 1$.
Donc x admet un inverse dans A.
Autre rédaction :
Pour $x \neq 0_1$, on définit l'application

$$\varphi_x : \left\{ \begin{array}{ccc} A & \to & A \\ y & \mapsto & x\times y. \end{array} \right.$$

φ_x est injective (par régularité de x) entre deux ensembles finis de même cardinal, donc elle est surjective.
On en conclut qu'il existe $y \in A$ tel que $\varphi(y) = 1$, donc $y = x^{-1}$ ce qui prouve bien l'existence de l'inverse.

Remarque : Pour $n \geqslant 2$, $(\mathbf{R}_n[X], +, \times)$ n'est pas un corps, bien qu'il soit intègre.

Théorème 5.5 *(Groupe des inversibles)*

Soit $(A, +, \times)$ un anneau.
On note A^* l'ensemble des inversibles de A.
$(A^*, \times)$ forme un groupe, appelé groupe des inversibles.

Preuve

- 1_A est inversible, car $1_A\times 1_A = 1_A$. C'est l'élément neutre.
- On a vu que le produit de deux inversible est inversibles (donc la loi est interne).
- La loi est associative par héritage.
- Par définition, tout élément de A^* est inversible dans A^*.

■

Exemple

Le groupe des inversibles de $(\mathbf{R}, +, \times)$ est $(\mathbf{R}^*, \times)$ avec $\mathbf{R}^* = \mathbf{R}\setminus\{0\}$.
On voit donc que la notation est cohérente.

Exemple

Le groupe des inversibles de $\mathscr{M}_n(\mathbf{K})$ est $\mathrm{GL}_n(\mathbf{K})$.

Exemple

Déterminer le groupe des inversibles d'un corps.

Solution :
C'est simplement $\mathbf{K} \setminus \{0_K\}$ muni du produit.

Propriété 5.6 *(Binôme de Newton et formule de Bernoulli)*

Soit $(A, +, \times)$ un anneau.
Soit $(a, b) \in A^2$ deux éléments qui **commutent.**
$\forall n \in \mathbf{N}$,

$$(a+b)^n = \sum_{k=0}^{n} \binom{n}{k} a^k b^{n-k}, \qquad a^{n+1} - b^{n+1} = (a-b) \sum_{k=0}^{n} a^k b^{n-k}.$$

Preuve
Même preuve que sur $\mathbf{R}$. ■

Définition 5.7 *(Sous-anneau)*

Soit $(A, +, \times)$ un anneau.
Un **sous-anneau** de $(A, +, \times)$ est un anneau $(A', +, \times)$ avec A' une partie stable de A pour les lois $+$ et $\times$.

Théorème 5.8 *(Caractérisation des sous-anneaux)*

Soit $(A, +, \times)$ un anneau et $A' \subset A$.
$(A', +, \times)$ est un sous-anneau de $(A, +, \times)$ si, et seulement si

1. A' contient **l'élément unité** de A,
2. A' est stable par différence : $\forall (x, x') \in (A')^2$, $x - x' \in A'$,
3. A' est stable par produit : $\forall (x, x') \in (A')^2$, $x \times x' \in A'$.

Définition 5.9 *(Morphismes d'anneaux)*

Soient $(A, +, \times)$ et $(A', \dot{+}, \dot{\times})$ deux anneaux.
Soit $f : A \to A'$.
f est un **morphisme d'anneaux** si, et seulement si f est compatible avec les deux opérations sur l'anneau :

- f est un morphisme de groupes entre $(A, +)$ et $(A', \dot{+})$:
- $\forall (x, x') \in A^2$, $f(x \times x') = f(x) \dot{\times} f(x')$.
- $f(1_A) = f(1_{A'})$.

ou de façon équivalente :

$\forall (x, x') \in A^2$, $f(x+x') = f(x) \dot{+} f(x')$, $\quad f(x \times x') = f(x) \dot{\times} f(x')$, et $f(1_A) = f(1_{A'})$.

Remarque : Pour un morphisme d'anneaux, on a besoin de vérifier l'image de l'élément unité, contrairement au morphisme de groupe où l'image de l'élément neutre s'obtient comme conséquence.
Cela vient du fait que les éléments ne possèdent en général pas d'inverse pour la loi multiplicative.

Définition 5.10 *(Morphisme de corps)*

Soient $(k, +, \times)$ et $(k', \dot{+}, \dot{\times})$ deux corps.
Soit $f : k \to k'$.
f est un **morphisme de corps** si, et seulement si c'est un morphisme entre les anneaux k et k'.
C'est équivalent au fait que ce soit un morphisme de groupe pour les deux lois (additive et multiplicative) du corps.

Remarque : Ici, on n'a pas besoin de vérifier $f(1_k) = f(1_{k'})$, même si ce n'est pas faux.

Propriété 5.11

- L'image d'un anneau par un morphisme d'anneau est un anneau.
- L'image *réciproque* d'un anneau par un morphisme d'anneau est un anneau.
- L'image d'un corps par un morphisme de corps est un corps.
- L'image *réciproque* d'un corps par un morphisme de corps est un corps.

Preuve
Comme pour le groupe. ■

Exemple
Soit A un anneau.

$$f : \left\{ \begin{array}{ccc} \mathbf{Z} & \to & A \\ k & \mapsto & k1_A. \end{array} \right.$$

1. f est un morphisme d'anneau.
2. $f(\mathbf{Z})$ est le plus petit sous-anneau de A.
3. Si A est fini, alors f n'est pas injectif.

Solution :

1. On remarque déjà que $\mathbf{Z}$ est un anneau pour les lois usuelles.
   $\forall (k, k') \in \mathbf{Z}^2$, $f(k+k') = (k+k')1_A = k1_A + k'1_A = f(k) + f(k')$.
   De même $f(kk') = f(k)f(k')$.
2. $f(\mathbf{Z})$ est l'image d'un anneau par un morphisme d'anneau, donc est lui-même un sous anneau de A.

Si A' est un sous-anneau de A alors, A' contient 1_A, donc par stabilité par somme, A' contient $\mathbf{Z}1_A = f(\mathbf{Z})$.
Ce qui prouve bien que $f(\mathbf{Z})$ est le plus petit sous-anneau de A.

3. Si f est injectif, alors $f(\mathbf{Z})$ est infini, donc A qui contient $f(\mathbf{Z})$ est lui-même infini.
On obtient donc la propriété énoncée par contraposée.

⚠ $\ker f$ n'est pas un sous-anneau de l'anneau se départ.
En effet, $\{0\}$ n'est pas un anneau, mais seulement en groupe, et $\ker f$ est bien un groupe, mais pas un anneau ($1 \notin \ker f$).
Ce groupe a cependant des propriétés assez fortes que l'on a rassemblées sous la définition *d'idéal.* Notion qui sera étudiée en deuxième année.