Groupes, anneaux, corps

1 Notion de loi

1.1 Loi interne

Définition 1.1 Loi interne

Soit E un ensemble. On appelle **loi interne** sur E toute application de $\mathrm{E} \times \mathrm{E}$ dans E.

Notation 1.1

Si $*$ est une loi interne sur E, l'image d'un couple $(x, y) \in \mathrm{E}^2$ par $*$ est notée $x * y$ plutôt que $*(x, y)$.
La notation $(\mathrm{E}, *)$ signifie l'ensemble E **muni** de la loi interne $*$.

Exemple 1.1

- La loi $+$ est une loi interne sur $\mathbb{N}$ mais pas la loi $-$.
- Soit A un ensemble. Les lois $\cup$ et $\cap$ sont des lois internes sur $\mathcal{P}(\mathrm{A})$.
- Le produit vectoriel est une loi interne sur l'ensemble des vecteurs de l'espace mais le produit scalaire n'en est pas une.

Remarque. Un ensemble muni d'une loi interne s'appelle un **magma**.
Si la loi n'est pas une loi usuelle, on appelle souvent l'élément $x * y$ le **produit** de x et y, par analogie avec la multiplication. Bien entendu, si la loi est notée $+$, on parlera plutôt de **somme**.

1.2 Associativité

Définition 1.2 Associativité

Soit $*$ une loi interne sur un ensemble E. On dit que $*$ est **associative** si pour tout $(x, y, z) \in \mathrm{E}^3$:

$$x * (y * z) = (x * y) * z$$

On peut alors noter $x * y * z$ sans parenthèses.

Exemple 1.2

- La multiplication sur $\mathbb{C}$ est une loi interne associative.
- La soustraction sur $\mathbb{Z}$ est une loi interne non associative.

1.3 Commutativité

Définition 1.3 Commutativité

Soit $*$ une loi interne sur un ensemble E. On dit que $*$ est **commutative** si pour tout $(x, y) \in \mathrm{E}^2$:

$$x * y = y * x$$

Remarque. Le symbole $+$ est généralement réservé aux lois commutatives.

Exemple 1.3

- L'addition sur $\mathbb{R}$ est commutative.
- La composition sur E^{E} n'est pas commutative dès que E possède plus de deux éléments.

1.4 Élément neutre et inversibilité

Définition 1.4 Élément neutre

Soit $*$ une loi interne sur un ensemble E. On dit que $e \in \mathrm{E}$ est un élément neutre de $(\mathrm{E}, *)$ si

$$\forall x \in \mathrm{E}, \qquad x * e = e * x = x$$

Théorème 1.1 Unicité de l'élément neutre

Soit $*$ une loi interne sur un ensemble E. Si $(\mathrm{E}, *)$ possède un élément neutre, il est unique.

Remarque. Si la loi est additive (i.e. notée $+$), l'élément neutre est généralement noté 0. Si la loi est multiplicative (i.e. noté $\times$), l'élément neutre est généralement noté 1.

Remarque. Un ensemble muni d'une loi interne associative et possédant un élément neutre est appelé un **monoïde**.

Exemple 1.4

- 1 est l'élément neutre de $(\mathbb{C}, \times)$
- $\varnothing$ est l'élément neutre de $(\mathcal{P}(\mathrm{E}), \cup)$ et E est l'élément neutre de $(\mathcal{P}(\mathrm{E}), \cap)$.
- $(\mathbb{N}^*, +)$ ne possède pas d'élément neutre.
- Id_{E} est l'élément neutre de $(\mathrm{E}^{\mathrm{E}}, \circ)$.

Définition 1.5 Élément inversible

Soit $*$ une loi interne sur un ensemble E possédant un élément neutre e. On dit qu'un élément x de E est **inversible** pour la loi $*$ s'il existe un élément x' tel que

$$x * x' = x' * x = e$$

Un tel x' s'appelle un **inverse** de x.

Remarque. L'élément neutre est toujours inversible et il est inverse de lui-même.

Exemple 1.5

- Tous les éléments non nuls de $(\mathbb{Q}, \times)$ sont inversibles.
- 1 et -1 sont les seuls éléments inversibles de $(\mathbb{Z}, \times)$.
- Les éléments inversibles de $(\mathrm{E}^{\mathrm{E}}, \circ)$ sont les bijections de E dans E.

Tout ce qui suit n'est valable que pour les lois associatives possédant un élément neutre.

Théorème 1.2 Unicité de l'inverse

Soit E un ensemble muni d'une loi interne **associative** possédant un élément neutre. Tout élément inversible possède un unique inverse.

Notation 1.2

L'inverse est généralement noté x^{-1} ou encore x^{*-1} s'il y a un risque d'ambiguïté sur la loi interne. Si la loi est notée $+$, on parle **d'opposé** plutôt que d'inverse et on le note $-x$ plutôt que x^{-1}.

Théorème 1.3 Propriétés de l'inverse

Soit E un ensemble muni d'une loi interne **associative** possédant un élément neutre.

(i) Soit $x \in \mathrm{E}$ inversible. Alors x^{-1} est inversible et $\left(x^{-1}\right)^{-1} = x$.

(ii) Soit $(x, y, z) \in \mathrm{E}^3$ avec x inversible. Alors

$$(x * y = x * z \text{ ou } y * x = z * x) \implies y = z$$

(iii) Soit $(x, y) \in \mathrm{E}^2$. Si x et y sont inversibles, alors $x * y$ est inversible et $(x * y)^{-1} = y^{-1} * x^{-1}$.

Remarque. La deuxième propriété signifie que l'on peut simplifier à gauche et à droite.

Attention ! L'inverse de $x * y$ **n'est pas** $x^{-1} * y^{-1}$ mais bien $y^{-1} * x^{-1}$.

1.5 Puissances

Notation 1.3 Puissance

Soit E un ensemble muni d'une loi interne associative $*$ et d'un élément neutre e.
Soient x un élément de E et $n \in \mathbb{N}^*$.

- L'élément $\underbrace{x * x * \cdots * x}_{n \text{ fois}}$ se note x^{*n} ou encore x^n s'il n'y a pas d'ambiguïté sur la loi.
- Par convention, on pose $x^0 = e$.
- Si x est inversible, on pose $x^{-n} = (x^{-1})^n = (x^n)^{-1}$.

Remarque. Si la loi est noté additivement $+$, on parle plutôt de **multiple** que de puissance et le «multiple $k^{\text{ème}}$» de x s'écrit kx plutôt que x^{+k}.

Proposition 1.1 Règles de calcul

Soit E un ensemble muni d'une loi interne associative $*$ et d'un élément neutre e.
Soient x un élément de E.

1. Pour tout $(n,p) \in \mathbb{N}^2$, $x^n * x^p = x^{n+p}$.
2. Si x est inversible, alors pour tout $(n,p) \in \mathbb{Z}^2$, $x^n * x^p = x^{n+p}$.

Attention ! En général $(x * y)^n \neq x^n * y^n$, à moins d'avoir commutativité de $*$.

1.6 Distributivité

Définition 1.6 Distributivité

Soit E un ensemble et $*$ et $\top$ deux lois internes sur E. On dit que la loi $*$ est distributive par rapport à $\top$ si :

$$\forall (x,y,z) \in \mathrm{E}^2, \qquad x * (y \top z) = (x * y) \top (x * z) \qquad \text{et} \qquad (y \top z) * x = (y * x) \top (z * x)$$

Exemple 1.6

- La loi $\times$ est distributive sur la loi $+$ dans $\mathbb{Z}$.
- Pour tout ensemble E, l'union $\cup$ et l'intersection $\cap$ sont deux lois distributives l'une sur l'autre dans $\mathcal{P}(\mathrm{E})$.

2 Groupes

2.1 Définition

Définition 2.1

On appelle **groupe** tout ensemble G muni d'une loi interne $*$ vérifiant les conditions suivantes :

(i) $*$ est associative,

(ii) $(\mathrm{E}, *)$ possède un élément neutre,

(iii) tout élément est inversible.

Remarque. Il peut arriver qu'on parle d'un groupe sans préciser sa loi. Le produit de deux éléments x et y de G se notera alors simplement xy.

Définition 2.2 Groupe commutatif

Soit $(\mathrm{G}, *)$ un groupe. Si la loi $*$ est commutative, on dit que le groupe $(\mathrm{G}, *)$ est **commutatif** ou **abélien**.

2.2 Groupes classiques

Proposition 2.1 Ensembles de nombres

- $(\mathbb{Z}, +)$, $(\mathbb{Q}, +)$, $(\mathbb{R}, +)$ et $(\mathbb{C}, +)$ sont des groupes commutatifs d'élément neutre 0.
- $(\mathbb{Q}^*, \times)$, $(\mathbb{R}^*, \times)$ et $(\mathbb{C}^*, \times)$ sont des groupes commutatifs d'élément neutre 1.

Remarque. Quand on parle du groupe $\mathbb{R}$ sans préciser la loi, on parle toujours du groupe additif $(\mathbb{R}, +)$. De même, quand on parle du groupe $\mathbb{C}^*$ sans préciser la loi, on parle toujours du groupe multiplicatif $(\mathbb{C}^*, \times)$.

Proposition 2.2 Groupe symétrique

Soit E un ensemble. L'ensemble des bijections de E sur E est noté $\mathfrak{S}(\mathrm{E})$. $(\mathfrak{S}(\mathrm{E}), \circ)$ est un groupe d'élément neutre Id_E.

Proposition 2.3 Ensembles de transformations du plan

On note P le plan. Les ensembles suivants munis de la loi de composition sont des groupes d'élément neutre Id_P :

- l'ensemble des homothéties du plan de rapport non nul,
- l'ensemble des translations du plan,
- l'ensemble des rotations du plan,
- l'ensemble des similitudes directes du plan de rapport non nul,
- l'ensemble des similitudes du plan de rapport non nul.

Remarque. Les éléments inversibles d'un monoïde forment un groupe.

2.3 Sous-groupes

Définition 2.3 Sous-groupe

Soient $(\mathrm{G}, *)$ un groupe et H un ensemble. On dit que H est un **sous-groupe** de G si :

(i) $\mathrm{H} \subset \mathrm{G}$

(ii) H contient l'élément neutre,

(iii) H est stable pour la loi $*$ i.e. $\forall (h, h') \in \mathrm{H}^2,\ h * h' \in \mathrm{H}$,

(iv) H est stable par passage à l'inverse i.e. $\forall h \in \mathrm{H},\ h^{-1} \in \mathrm{H}$.

Exemple 2.1

Soit G un groupe d'élément neutre e. Alors G et $\{e\}$ sont des sous-groupes de G.

Remarque. Si H est un sous-groupe d'un groupe $(\mathrm{G}, *)$. Alors pour tout $(h, n) \in \mathrm{H} \times \mathbb{Z}$, $h^n \in \mathrm{H}$.

Proposition 2.4

Soient $(\mathrm{G}, *)$ un groupe et H un sous-groupe de G. Alors $(\mathrm{H}, *)$ est un groupe. De plus,

(i) l'élément neutre de $(\mathrm{H}, *)$ est l'élément neutre de $(\mathrm{G}, *)$;

(ii) si $h \in \mathrm{H}$, l'inverse de h en tant qu'élément du groupe $(\mathrm{H}, *)$ est égal à son inverse en tant qu'élément du groupe $(\mathrm{G}, *)$.

Remarque. Si on voulait être rigoureux, il faudrait munir H de la restriction de $*$ à H.

Remarque. Si K est un sous-groupe de H qui est un sous-groupe de G, alors K est un sous-groupe de G.

Théorème 2.1 Caractérisation des sous-groupes

Soient $(\mathrm{G}, *)$ un groupe d'élément neutre e et H un ensemble. Alors H est un sous-groupe si et seulement si

(i) $\mathrm{H} \subset \mathrm{G}$;

(ii) H contient l'élément neutre ;

(iii) $\forall (h, k) \in \mathrm{H}^2, h * k^{-1} \in \mathrm{H}$.

Méthode **Sous-groupes en pratique**

Il est souvent plus facile de montrer qu'un ensemble muni d'une loi interne est un groupe en montrant qu'il est un sous-groupe d'un groupe connu.

Exemple 2.2

- $(\mathbb{Z}, +)$ est un sous-groupe de $(\mathbb{Q}, +,)$ qui est un sous-groupe de $(\mathbb{R}, +)$ qui est un sous-groupe de $(\mathbb{C}, +)$.
- $(\mathbb{Q}^*, \times)$ est un sous-groupe de $(\mathbb{R}^*, \times)$ qui est un sous-groupe de $(\mathbb{C}^*, \times)$.
- Soit $n \in \mathbb{N}^*$. $(\mathbb{U}_n, \times)$ est un sous-groupe de $(\mathbb{U}, \times)$ qui est un sous-groupe de $(\mathbb{C}^*, \times)$.
- Les homothéties de rapport non nul, les translations, les rotations et les similitudes directes forment des sous-groupes du groupe des similitudes.
- Soient E un ensemble et $a \in \mathrm{E}$. Les éléments de $\mathfrak{S}(\mathrm{E})$ fixant a forment un sous-groupe de $\mathfrak{S}(\mathrm{E})$.

2.4 Morphismes de groupes (hors-programme)

Définition 2.4 Morphisme de groupes

Soient $(\mathrm{G}, *)$ et $(\mathrm{G}', .)$ deux groupes. On appelle **morphisme (de groupes)** de G dans G′ toute application f de G dans G′ telle que :

$$\forall (x, y) \in \mathrm{G}^2, f(x * y) = f(x).f(y)$$

On appelle **endomorphisme (de groupe)** de G tout morphisme de G dans G.

Exemple 2.3

- L'exponentielle est un morphisme de $(\mathbb{R}, +)$ dans $(\mathbb{R}^*, \times)$.
- Le logarithme est un morphisme de $(\mathbb{R}^*, \times)$ dans $(\mathbb{R}, +)$.
- Le module est un morphisme de $(\mathbb{C}^*, \times)$ dans $(\mathbb{R}^*, \times)$.
- La valeur absolue est un endomorphisme de $(\mathbb{R}^*, \times)$.

Proposition 2.5 Morphisme, élément neutre et inverse

Soit f un morphisme de $(\mathrm{G}, *)$ dans $(\mathrm{G}', .)$. On note e et e' les éléments neutres respectifs de G et G′. Alors

(i) $f(e) = e'$,

(ii) $\forall x \in \mathrm{G}$, $f(x^{-1}) = f(x)^{-1}$.

(iii) $\forall x \in \mathrm{G}, \forall n \in \mathbb{Z}$, $f(x^n) = f(x)^n$.

Proposition 2.6 Morphisme et composition

Soient $f : \mathrm{G} \to \mathrm{G}'$ et $g : \mathrm{G}' \to \mathrm{G}''$ deux morphismes de groupes. Alors $g \circ f : \mathrm{G} \to \mathrm{G}''$ est un morphisme de groupes.

Proposition 2.7 Images directe et réciproque d'un sous-groupe par un morphisme de groupes

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

(i) Si H est un sous-groupe de G, alors $f(\mathrm{H})$ est un sous-groupe de G′.

(ii) Si K est un sous-groupe de G′, alors $f^{-1}(\mathrm{K})$ est un sous-groupe de G.

Définition 2.5 Noyau et image d'un morphisme

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

(i) On appelle **noyau** de f l'ensemble $\operatorname{Ker} f = f^{-1}(\{e'\}) = \{x \in \mathrm{G} \mid f(x) = e'\}$.

(ii) On appelle **image** de f l'ensemble $\operatorname{Im} f = f(\mathrm{G}) = \{f(x), x \in \mathrm{G}\}$.

Remarque. L'image du morphisme f n'est autre que l'image de l'application f.

Théorème 2.2

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

(i) $\operatorname{Ker} f$ est un sous-groupe de G.

(ii) $\operatorname{Im} f$ est un sous-groupe de G′.

Exemple 2.4

Le module est un morphisme de $(\mathbb{C}, *)$ dans $(\mathbb{R}, *)$. Par définition, son noyau est $\mathbb{U}$ qui est donc un sous-groupe de $(\mathbb{C}, *)$. De même, $\{-1, 1\}$ est un sous-groupe de $\{\mathbb{R}^*, \times\}$ puisque c'est le noyau de l'endomorphisme «valeur absolue» de $(\mathbb{R}^*, \times)$.

Proposition 2.8

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

(i) f est injectif si et seulement si $\operatorname{Ker} f = \{e\}$.

(ii) f est surjectif si et seulement si $\operatorname{Im} f = \mathrm{G}'$.

Remarque. En ce qui concerne la première proposition, pour prouver l'injectivité de f, il suffit de montrer que $\operatorname{Ker} f \subset \{e\}$ puisque $\operatorname{Ker} f$, étant un sous-groupe, contient nécessairement e.

Méthode Injectivité en pratique

Pour prouver l'injectivité d'un morphisme de groupes $f : \mathrm{G} \to \mathrm{G}'$, on commence la démonstration par : «Soit $x \in \mathrm{G}$ tel que $f(x) = e'$» et on montre que $x = e$.

Définition 2.6 Isomorphisme, automorphisme

Soient G et G′ deux groupes.
On appelle **isomorphisme** de G sur G′ tout morphisme bijectif de G dans G′.
On appelle **automomorphisme** de G tout endomorphisme bijectif de G. On dit que G est **isomorphe** à G′ s'il existe un isomorphisme de G sur G′.

Remarque. Dire que deux groupes sont isomorphes veut dire qu'ils ont la même structure. Si on connaît l'un, on connaît l'autre. Toute propriété liée à la structure de groupe qui est vraie dans un groupe est aussi vraie dans un groupe qui lui est isomorphe.

Exemple 2.5

- $(\mathbb{C}, +)$ et $(\mathbb{R}^2, +)$ sont isomorphes.
- Notons $\overrightarrow{\mathrm{P}}$ et $\overrightarrow{\mathrm{E}}$ le plan et l'espace vectoriel. Alors $(\overrightarrow{\mathrm{P}}, +)$ et $(\overrightarrow{\mathrm{E}}, +)$ sont respectivement isomorphes à $(\mathbb{R}^2, +)$ et $(\mathbb{R}^3, +)$.

Théorème 2.3 Réciproque d'un isomorphisme

Soit f un isomorphisme de groupes de G sur G′. Alors f^{-1} est un isomorphisme de groupes de G′ sur G.

Théorème 2.4 Groupe des automorphismes

Soit G un groupe. L'ensemble des automorphismes de G, noté $\mathrm{A}ut(\mathrm{G})$, est un sous-groupe de $(\mathfrak{S}(\mathrm{G}), \circ)$.

3 Anneaux

3.1 Définition et premières propriétés

Définition 3.1 Anneau

On appelle **anneau** tout triplet $(\mathrm{A}, +, \times)$ où A est un ensemble et $+$ et $\times$ sont des lois internes sur A vérifiant les conditions suivantes :

(i) $(\mathrm{A}, +)$ est un groupe commutatif dont l'élément neutre est généralement noté 0_{A} ou 0,

(ii) $\times$ est associative,

(iii) A possède un élément neutre pour $\times$ généralement noté 1_{A} ou 1,

(iv) $\times$ est distributive sur $+$.

Si $\times$ est commutative, on dit que l'anneau $(\mathrm{A}, +, \times)$ est commutatif.

Exemple 3.1

- $(\mathbb{Z}, +, \times)$, $(\mathbb{Q}, +, \times)$, $(\mathbb{R}, +, \times)$ et $(\mathbb{C}, +, \times)$ sont trois exemples d'anneaux commutatifs.
- $(\mathbb{R}^n, +, \times)$ est un anneau commutatif (l'addition et la multiplication s'effectuant composante par composante).
- $(\mathbb{R}^{\mathbb{R}}, +, \times)$ est un anneau commutatif.
- L'ensemble des polynômes à coefficients dans $\mathbb{R}$ (noté $\mathbb{R}[X]$) est aussi un anneau commutatif.

Notation 3.1

Soit A un anneau. On note A^* l'ensemble des éléments inversibles de A.

Proposition 3.1

Si $(\mathrm{A}, +, \times)$ est un anneau, $(\mathrm{A}^*, \times)$ est un groupe.

Théorème 3.1 Règle de calcul dans les anneaux

Soient $(\mathrm{A}, +, \times)$ un anneau, $(a, b) \in \mathrm{A}^2$ et $n \in \mathbb{Z}$.

(i) $0_{\mathrm{A}} \times a = a \times 0_{\mathrm{A}} = 0_{\mathrm{A}}$,

(ii) $n(a \times b) = (na) \times b = a \times (nb)$,

Remarque. On peut avoir $1_{\mathrm{A}} = 0_{\mathrm{A}}$ mais il est facile de voir que, dans ce cas, tout élément de A est nul i.e. $\mathrm{A} = \{0\}$. On appelle cet anneau l'**anneau nul**.

Définition 3.2 Anneau intègre

On dit qu'un anneau A est intègre s'il est **non nul** et s'il vérifie la propriété suivante :

$$\forall (a, b) \in \mathrm{A}^2, \qquad ab = 0 \Rightarrow (a = 0 \text{ ou } b = 0)$$

Remarque. On peut généraliser à un produit de plus de deux facteurs.

Exemple 3.2

Les anneaux $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ et $\mathbb{C}$ sont intègres.
Les anneaux $(\mathbb{R}^{\mathbb{R}}, +, \times)$ et $(\mathbb{R}^n, +, \times)$ pour $n \geq 2$ ne sont pas intègres.

Attention ! Tous les anneaux ne sont pas intègres. Nous verrons par exemple dans le cadre de l'algèbre linéaire des anneaux non intègres.

3.2 Formules

Définition 3.3

Soient $(\mathrm{A}, +, \times)$ un anneau et $(a, b) \in \mathrm{A}^2$. On dit que a et b commutent si $a \times b = b \times a$.

Proposition 3.2

Soient $(\mathrm{A}, +, \times)$ un anneau et $(a, b) \in \mathrm{A}^2$ tels que a et b **commutent**. Alors

(i) $\forall n \in \mathbb{N}^*$, $a^n - b^n = (a-b)\sum_{k=0}^{n-1} a^k b^{n-1-k} = \left[\sum_{k=0}^{n-1} a^k b^{n-1-k}\right](a-b)$,

(ii) $\forall n \in \mathbb{N}$, $(a+b)^n = \sum_{k=0}^{n} \binom{n}{k} a^k b^{n-k}$.

En particulier, ces formules sont toujours vraies dans un anneau commutatif.

3.3 Sous-anneaux

Définition 3.4 Sous-anneau

Soient $(\mathrm{A}, +, \times)$ un anneau et B un ensemble. On dit que B est un sous-anneau de $(\mathrm{A}, +, \times)$ si :

(i) $(\mathrm{B}, +)$ est un sous-groupe de $(\mathrm{A}, +)$;

(ii) $1_{\mathrm{A}} \in \mathrm{B}$;

(iii) B est stable par $\times$.

Proposition 3.3

Si B est un sous-anneau de $(\mathrm{A}, +, \times)$, alors $(\mathrm{B}, +, \times)$ est un anneau. De plus, $1_{\mathrm{B}} = 1_{\mathrm{A}}$.

Proposition 3.4 Caractérisation des sous-anneaux

Soient $(A, +, \times)$ un anneau et B un ensemble. B est un sous-anneau de $(A, +, \times)$ si et seulement si :

(i) $B \subset A$;

(ii) $1_A \in B$;

(iii) $\forall (a, b) \in B^2, a - b \in B$;

(iv) $\forall (a, b) \in B^2, a \times b \in B$.

Méthode **Sous-anneaux en pratique**

Il est souvent plus facile de montrer qu'un triplet $(A, +, \times)$ est un anneau en montrant qu'il est un sous-anneau d'un anneau connu.

Exemple 3.3

$(\mathbb{Z}, +, \times)$ est un sous-anneau de $(\mathbb{Q}, +, \times)$ qui est un sous-anneau de $(\mathbb{R}, +, \times)$ qui est un sous-anneau de $(\mathbb{C}, +, \times)$.

Exercice 3.1 **Entiers de Gauss**

Montrer que $\mathbb{Z}[i] = \{a + ib, (a, b) \in \mathbb{Z}^2\}$ est un sous-anneau de $\mathbb{C}$.

Exercice 3.2

Soit $d \in \mathbb{N}$ qui ne soit pas un carré d'entier. Montrer que $\mathbb{Z}[\sqrt{d}]$ est un sous anneau de $\mathbb{R}$.

Exercice 3.3

Montrer que $\mathbb{Z}$ est le seul sous-anneau de $\mathbb{Z}$.

3.4 Morphismes d'anneaux (hors-programme)

Définition 3.5 Morphisme d'anneaux

Soient $(A, +, \times)$ et $(B, \oplus, \otimes)$ deux anneaux. On appelle **morphisme d'anneaux** de A dans B toute application $f : A \to B$ telle que :

(i) $f(1_A) = 1_B$,

(ii) $\forall (a, b) \in A^2, f(a + b) = f(a) \oplus f(b)$,

(iii) $\forall (a, b) \in A^2, f(a \times b) = f(a) \otimes f(b)$,

Remarque. En particulier, f est un morphismes de groupes de $(A, +)$ dans $(B, \oplus)$. On peut donc définir le noyau et l'image d'un morphisme d'anneaux.

Remarque. On peut également définir des notions d'**endomorphisme**, d'**isomorphisme** et d'**automorphisme** d'anneaux.

Proposition 3.5 Images directe et réciproque d'un sous-anneau par un morphisme d'anneaux

Soit $f : A \to B$ un morphisme d'anneaux.

(i) Si C est un sous-anneau de A, alors $f(C)$ est un sous-anneau de B.

(ii) Si D est un sous-anneau de B, alors $f^{-1}(D)$ est un sous-anneau de A.

4 Corps

4.1 Définition et premières propriétés

Définition 4.1 Corps

On appelle corps tout anneau **commutatif** $(K, +, \times)$ dans lequel tout élément non nul est inversible pour $\times$.

Remarque. En particulier, un corps est un anneau.
Pour tout corps K, $K^* = K \setminus \{0_K\}$.

Théorème 4.1 Corps et intégrité

Tout corps est **intègre**.

Remarque. On peut donc calculer dans un corps quelconque comme on calculerait dans $\mathbb{Q}$, $\mathbb{R}$ ou $\mathbb{C}$.

Exemple 4.1

$\mathbb{Q}$, $\mathbb{R}$ et $\mathbb{C}$ sont des corps.

4.2 Sous-corps

Définition 4.2 Sous-corps

Soit $(K, +, \times)$ un corps et L un ensemble. On dit que L est un sous-corps de $(K, +, \times)$ si

(i) L est un sous-anneau de $(K, +, \times)$;

(ii) L est stable par inversion i.e. $\forall x \in L \setminus \{0_K\}, x^{-1} \in L$.

Proposition 4.1

Soient $(K, +, \times)$ un corps et L un sous-corps de $(K, +, \times)$. Alors $(L, +, \times)$ est un corps.

Proposition 4.2 Sous-corps

Soit $(\mathrm{K}, +, \times)$ un corps et L un ensemble. L est un sous-corps de $(\mathrm{K}, +, \times)$ si et seulement si

(i) $\mathrm{L} \subset \mathrm{K}$;

(ii) $1_{\mathrm{K}} \in \mathrm{L}$;

(iii) $\forall (x, y) \in \mathrm{L}^2, x - y \in \mathrm{L}$;

(iv) $\forall (x, y) \in \mathrm{L} \times (\mathrm{L} \setminus \{0_{\mathrm{K}}\}), x \times y^{-1} \in \mathrm{L}$.

Méthode Sous-corps en pratique

Il est souvent plus facile de montrer qu'un triplet $(\mathrm{K}, +, \times)$ est un corps en montrant qu'il est un sous-corps d'un corps connu.

Exemple 4.2

$(\mathbb{Q}, +, \times)$ est un sous-corps de $(\mathbb{R}, +, \times)$ qui est un sous-corps de $(\mathbb{C}, +, \times)$. $\mathbb{Q}$ est le plus petit sous-corps de $\mathbb{C}$.

Remarque. Un sous-corps est un sous-anneau mais un sous-anneau d'un corps n'est pas forcément un sous-corps. Par exemple, $\mathbb{Q}$ est bien un sous-anneau de $\mathbb{R}$ car $\mathbb{Q}$ est un sous-corps de $\mathbb{R}$. Mais $\mathbb{Z}$ n'est pas un sous-corps de $\mathbb{Q}$ bien qu'il soit un sous-anneau de $\mathbb{Q}$ et que $\mathbb{Q}$ soit un corps.

Exercice 4.1

Montrer que $\mathbb{Q}[i] = \{a + ib, (a, b) \in \mathbb{Q}^2\}$ est un sous-corps de $\mathbb{C}$.

Exercice 4.2

Soit $d \in \mathbb{N}$ qui ne soit pas un carré d'entier. Montrer que $\mathbb{Q}[\sqrt{d}]$ est un sous-corps de $\mathbb{C}$.

4.3 Morphismes de corps (hors-programme)

Définition 4.3 Morphisme de corps

Soient $(\mathrm{K}, +, \times)$ et $(\mathrm{L}, \oplus, \otimes)$ deux corps. On appelle **morphisme de corps** de K dans L tout morphisme d'anneaux de K dans L.

Proposition 4.3

Soit $f : \mathrm{K} \to \mathrm{L}$ un morphisme de corps. Alors

1. $\forall x \in \mathrm{K}^*, f(x) \in \mathrm{K}^*$ et $f(x^{-1}) = f(x)^{-1}$.
2. f est injectif.

On peut également définir des notions d'**endomorphisme**, d'**isomorphisme** et d'**automorphisme** de corps.

Exemple 4.3

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