# XIII Groupes, anneaux, corps

4 janvier 2022

On remarque que dans des domaines a priori distincts, des similitudes apparaissent, notamment concernant les structures. Pour avoir une théorie générale, on définit des structures algébriques abstraites, on en démontre les propriétés, puis on les applique dans les exemples mathématiques qui vérifient ces structures.
Dans ce chapitre on s'intéresse aux structures algébriques de base : groupes, anneaux et corps. Plus tard, nous étudierons une structure fondamentale : celle d'espace vectoriel.

# 1 Lois de composition internes.

Dans tout ce chapitre, $E$ est un ensemble.

## 1.1 Définition.

**Définition 1.1.1.**
On appelle *loi de composition interne sur $E$* (lci) toute application de $E \times E$ dans $E$.

• Cette définition a déjà été vue, ainsi que des exemples, dans le chapitre IV sur les complexes.

**Remarque 1.1.2.**
On appelle *magma* tout couple constitué d'un ensemble et d'une lci.

**Exemple 1.1.3.**
$(\mathbb{Z}, -)$ est un magma, mais pas $(\mathbb{N}, -)$, car $-4 \notin \mathbb{N}$.

Dans toute la suite, $*$ est une lci sur $E$.

## 1.2 Propriétés usuelles des lci.

**Définition 1.2.1.**
Soit $(E, *)$ un magma.

1. On dit que $E$ est *associatif* si pour tout $x, y, z \in E$, on a : $x * (y * z) = (x * y) * z$. L'élément $x * (y * z) = (x * y) * z$ est alors noté $x * y * z$.
2. On dit que $E$ est *commutatif* si pour tout $x, y \in E$, on a : $x * y = y * x$.
3. Soit $\top$ une seconde lci sur $E$. On dit que dans $E$ $*$ est *distributive* par rapport à $\top$ si pour tout $x, y, z \in E$, on a :
   — $x * (y \top z) = (x * y) \top (x * z)$ ;
   — $(y \top z) * x = (y * x) \top (z * x)$.

**Remarque 1.2.2.**
On dit que dans $E$ $*$ est *distributive à gauche* par rapport à $\top$ si pour tout $x, y, z \in E$, on a : $x * (y \top z) = (x * y) \top (x * z)$.
De même, on a la notion de *distributivié à droite*.

**Exemple 1.2.3.**
• $\mathbb{C}$, $\mathbb{R}$, $\mathbb{Q}$, $\mathbb{Z}$, $\mathbb{N}$ avec $+$ ou $\times$ sont associatifs, mais pas $(\mathbb{Z}, -)$ car $1-(2-3) \neq (1-2)-3$, ni $(\mathbb{R}^3, \wedge)$.
• $\mathbb{C}$, $\mathbb{R}$, $\mathbb{Q}$, $\mathbb{Z}$, $\mathbb{N}$ avec $+$ ou $\times$ sont commutatifs, mais pas $(\mathbb{Z}, -)$ ni $(\mathbb{R}^3, \wedge)$, ni $(\mathscr{F}(\mathbb{R}, \mathbb{R}), \circ)$.
• Sur $\mathbb{C}$, $\mathbb{R}$, $\mathbb{Q}$, $\mathbb{Z}$, $\mathbb{N}$ $\times$ est distributive par rapport à $+$, et sur $\mathscr{P}(E)$, $\cap$ et $\cup$ sont distributives l'une par rapport à l'autre.

**Définition 1.2.4.**
1. Soit $e \in E$. on dit que $e$ est un *élément neutre à gauche* (resp. *à droite*) pour $*$ si pour tout $x \in E$ on a $e * x = x$ (resp. $x * e = x$). On dit que $e$ est un *élément neutre* pour $*$ si c'est un élément neutre à gauche et à droite, i.e. pour tout $x \in E$, $e * x = x * e = x$.
2. Soit $e$ un neutre pour $*$ et soit $x \in E$. On dit que $x$ est *inversible à gauche* (resp. *à droite*) s'il existe un élément $y \in E$ tel que $y * x = e$ (resp. $x * y = e$). Un tel élément $y$ s'appelle *UN inverse à gauche* (resp. *à droite*) de $x$. On dit que $x$ est *inversible* s'il est inversible à gauche et à droite, *i.e.* il existe $y \in E$ tel que $y * x = x * y = e$. Dans ce cas $y$ est *UN inverse de $x$*.

**Exemple 1.2.5.**
• 0 est un élément neutre pour $+$ dans $\mathbb{R}$, $\mathbb{C}$, $\mathbb{Q}$, $\mathbb{Z}$, $\mathbb{N}$.
• 1 est un élément neutre pour $\times$ dans $\mathbb{R}$, $\mathbb{C}$, $\mathbb{Q}$.
• Id est un élément neutre pour $\circ$ dans $\mathscr{F}(E, E)$,

et les bijections sont tous les éléments inversibles de cet ensemble.
• Par contre $(\mathbb{R}^3, \wedge)$ n'a pas de neutre. S'il y avait un neutre $u$, on devrait avoir $u \wedge u = u$, mais $u \wedge u = 0$, donc $u = 0$. Mais pour tout $v \neq 0$, on a $u \wedge v = 0$, et non $u \wedge v = v$.

 Être inversible d'un seul côté ne suffit pas pour être inversible tout court : un exemple a été vu dans le TD du chapitre sur les applications (ensemble des applications de $\mathbb{N}$ dans $\mathbb{N}$ muni de $\circ$).

**Remarque 1.2.6.**
Un neutre est toujours inversible et est son propre inverse.

**Proposition 1.2.7.**
Si $*$ admet un neutre, alors ce neutre est unique.

**Démonstration.**
Soient $e$ et $e'$ deux neutres.[1] Alors $e * e' = e$ et $e * e' = e'$, donc $e = e'$. □

**Proposition 1.2.8.**
On suppose la loi $*$ associative, et admettant un neutre $e$. Si un élément est inversible, alors il a un seul inverse.

**Démonstration.**
Soient $y$ et $y'$ deux inverses[2] de $x \in E$. Alors $y * x = e$ et $x * y' = e$. Donc $y * (x * y') = y * e = y$ et $(y * x) * y' = e * y' = y'$, d'où $y = y'$. □

**Remarque 1.2.9.**
On utilise souvent les *notations additives et multiplicatives*.

- En notation additive, $*$ est en général notée $+$, $\underbrace{x + x + \ldots + x}_{n \text{ fois}}$ se note $nx$, et si $x$ est inversible, son inverse se note $-x$. On l'appelle alors plutôt *l'opposé de* $x$. De même, on notera le neutre d'une telle structure 0, ou $0_E$.
- En notation multiplicative, $*$ est en général remplacée par $\times$ (et ce symbole est même souvent omis), $\underbrace{x \times x \times \ldots \times x}_{n \text{ fois}}$ se note $x^n$ et si $x$ est inversible, son inverse se note $x^{-1}$. De même, on notera le neutre d'une telle structure 1, ou $1_E$.

Pour éviter toute erreur, on essaiera au maximum de n'utiliser la notation additive que pour des lois qui ont les mêmes propriétés que la loi + sur $\mathbb{R}$. Par exemple, noter + une lci non commutative peut-être déroutant, ainsi que pour une lci pour laquelle tous les éléments ne sont pas inversibles. La notation + est en général réservée à des lci commutatives et pour lesquelles les éléments sont tous inversibles..

Ce n'est pas le cas pour la notation multiplicative, qui est la plus couramment utilisée pour des lois associatives, mais sans plus. Par exemple il est fréquent d'utiliser $\times$ même pour une lci non commutative et pour laquelle les éléments ne sont pas tous inversibles. Donc faites attention, par défaut on aura $xy \neq yx$, et $x^{-1}$ n'existera pas forcément !

Dans toute la suite, on adoptera la notation multiplicative, et on suppose que $E$ a un neutre noté 1.

1. On pourra remarquer que dans cette démonstration on utilise uniquement le fait que $e$ est neutre à gauche et $e'$ neutre à droite. Donc en fait tout neutre à gauche est égal à tout neutre à droite, d'où l'on déduit d'une part que l'existence d'un neutre à gauche et d'un neutre à droite suffit à assurer l'existence d'un neutre et d'autre part que ce neutre est alors le seul neutre à gauche et le seul neutre à droite. Pour qu'un élément ait plusieurs neutres à gauche, il est donc nécessaire (mais pas suffisant) qu'il n'ait aucun neutre à droite et *vice-versa*.

2. On pourra remarquer que dans cette démonstration on utilise uniquement le fait que $y$ est inverse à gauche et $y'$ inverse à droite. Donc en fait tout inverse à gauche est égal à tout inverse à droite, d'où l'on déduit d'une part que l'existence d'un inverse à gauche et d'un inverse à droite pour $x$ suffit à assurer l'existence d'un inverse et d'autre part que cet inverse est alors le seul inverse à gauche et le seul inverse à droite de $x$. Pour qu'un élément ait plusieurs inverses à gauche, il est donc nécessaire qu'il n'ait aucun inverse à droite et *vice-versa*

**Proposition 1.2.10.**
On suppose la loi $*$ associative. Soient $x, y, z \in E$.

(i) Simplification par un inversible : si $x$ est inversible, alors $x * y = x * z \Leftrightarrow y = z$.

(ii) Inverse d'un produit : si $x$ et $y$ sont inversibles alors $x * y$ l'est aussi et $(x * y)^{-1} = y^{-1} * x^{-1}$. **Attention :** l'inverse de $x * y$ n'a aucune raison d'être $x^{-1} * y^{-1}$.

(iii) Puissances négatives : si $x$ est inversible, on pose pour $n \in \mathbb{N}^*$, $x^{-n} = (x^{-1})^n$. Alors $x^{-n} = (x^n)^{-1}$.

(iv) Inverse d'un inverse : si $x$ est inversible, $x^{-1}$ l'est aussi et $(x^{-1})^{-1} = x$.

**Démonstration.** (iii) Par récurrence. Vrai si $n = 0$ ou 1. Si vrai pour $n$, alors $x^{n+1} * x^{-n-1} = x^n * x * x^{-1} * x^{-n} = x^n * e * x^{-n} = x^n * x^{-n} = e$.

(iv) Vrai par unicité de l'inverse.

□

**Définition 1.2.11.**
Soit $(E, *)$ un magma et $F$ une partie de $E$. On dit que $F$ est une *partie stable* (de $E$ par $*$) si pour tous $x, y \in F$, $x * y \in F$.

**Exemple 1.2.12.**
$\{-1, 1\}$ est une partie stable de $(\mathbb{R}, \times)$, mais pas $\{-2, 2\}$.

# 2 Structure de groupe.

## 2.1 Définition et exemples.

**Définition 2.1.1.**
On appelle *groupe* tout ensemble muni d'une loi de composition interne associative, ayant un élément neutre, et dont tout élément est inversible.

Si un groupe est *commutatif* (ce qui signifie en fait que sa loi est commutative), il est dit *abélien*.

Par défaut on utilise la notation multiplicative pour un groupe, sauf pour les groupes abéliens pour lesquels on utilise la notation additive.

**Exemple 2.1.2.**
• $\mathbb{C}$, $\mathbb{R}$, $\mathbb{Q}$, $\mathbb{Z}$ sont des groupes avec la loi $+$, mais pas avec la loi $\times$.
• Pour $n \in \mathbb{N}^*$, $\mathbb{C}^n$, $\mathbb{R}^n$, $\mathbb{Q}^n$, $\mathbb{Z}^n$ sont des groupes avec la loi $+$.
• $\mathbb{C}\setminus\{0\}$, $\mathbb{R}\setminus\{0\}$, $\mathbb{Q}\setminus\{0\}$, sont des groupes avec la loi $\times$.
• $\mathbb{N}$ n'est un groupe ni avec la loi $+$ ni avec la loi $\times$.

**Exemple 2.1.3.**
En spé, vous manipulerez le groupe $(\mathbb{Z}/n\mathbb{Z}, +)$, que l'on peut voir comme « l'ensemble des congruences modulo $n$ », avec $n \in \mathbb{N}^*$.

**Définition 2.1.4.**
Soit $X$ un ensemble non vide. On appelle *groupe des permutations de $X$* l'ensemble des bijections de $X$ dans $X$. Comme son nom l'indique, c'est un groupe, si on le munit de la loi de composition $\circ$. On le note $S_X$ (on trouvera parfois la notation $\mathfrak{S}(X)$).

**Démonstration.**
L'application identité, Id : $X \to X$, $x \mapsto x$, est évidemment une bijection de $X$, donc $S_X$ est non vide.
On sait déjà que la composée de deux bijections est une bijection, donc $\circ$ est une lci sur $S_X$. Il est évident que Id en est le neutre. On sait également que cette loi est associative, et que la réciproque d'une bijection est encore une bijection. Cela assure que $(S_X, \circ)$ est un groupe. □

## 2.2 Sous-groupes.

**Dans toute la suite, $(G, *)$ est un groupe de neutre $e$. On adopte la notation multiplicative.**

**Définition 2.2.1.**
On appelle *sous-groupe* de $G$ tout ensemble $H$ vérifiant les propriétés suivantes :

(i) $H \subset G$ ;

(ii) $e \in H$ ;

(iii) Stabilité par produit : $\forall x, y \in H, x * y \in H$ ;

(iv) Stabilité par passage à l'inverse : $\forall x \in H$, on a $x^{-1} \in H$.

**Remarque 2.2.2** (peu utile, mais traditionnelle)**.**
En vertu des points (iii) et (iv), le point (ii) peut être remplacé par $H \neq \varnothing$.

**Exemple 2.2.3.**
Sont des sous-groupes :

- $\{e\}$ et $G$ dans $(G, *)$.
- $\mathbb{U}$ dans $(\mathbb{C}^*, \times)$.
- $n\mathbb{Z}$ dans $(\mathbb{Z}, +)$.
- $H = \{f \in S_{\mathbb{R}} \mid f(0) = 0\}$ dans $(S_{\mathbb{R}}, \circ)$.

**Proposition 2.2.4.**
Un ensemble $H$ est un sous groupe de $G$ si et seulement si $H$ est un sous-ensemble non vide de $G$ et pour tout $(x, y) \in H^2$, on a $x^{-1} * y \in H$.

**Démonstration.**
Montrons l'implication et sa réciproque :

— Supposons que $H$ est un sous-groupe de $G$. Alors $H$ contient $e$ et n'est donc pas vide. De plus, soit $(x, y) \in H$. $H$ étant stable par passage à l'inverse, on a alors $x^{-1} \in H$ et par stabilité par produit, on a donc $x^{-1} * y \in H$.

— Réciproquement, supposons que $H$ est non vide et que pour tout $(x, y) \in H^2$, on a $x^{-1} * y \in H$. Montrons que $H$ possède les trois propriétés énumérées dans sa définition :

(i) $H$ étant non vide, il possède au moins un élément $x_0$. On a alors $e = x_0^{-1} x_0 \in H$.

(iii) Soit $x \in H$. On a alors $(x, e) \in H^2$, donc $x^{-1} * e \in H$.

(ii) Soit $(x, y) \in H$. D'après ce qui précède, on a alors $x^{-1} \in H$, donc $(x^{-1}, y) \in H^2$, donc $x * y = \left(x^{-1}\right)^{-1} * y \in H$.

□

**Remarque 2.2.5.**
On obtient une proposition vraie également en remplaçant ci-dessus la condition $x^{-1}y \in H$ par $xy^{-1} \in H$.

**Théorème 2.2.6.**
Un sous-groupe muni de la loi induite du groupe est lui-même un groupe.

**Démonstration.**
Soit $(G, *)$ un groupe de neutre $e$ et $H$ un sous-groupe de $G$.

1. Montrons qu'on peut restreindre $* : G \times G \to G$ au départ à $H \times H$ et à l'arrivée à $H$. On appellera alors loi induite par $*$ sur $H$ cette restriction de $*$. On a $H \times H \subset G \times G$, donc la restriction au départ est légitime, pour effectuer la restriction à l'arrivée, il suffit de montrer que pour tout $(x, y) \in H^2$, on a $x * y \in H$, c'est-à-dire que $H$ est stable par $*$. Or $H$ est un sous-groupe de $G$ donc c'est évident.
2. $H$ muni de la loi induite par $*$ est un magma associatif. En effet $(G, *)$ est un magma associatif, on a donc
$$\forall (x, y, z) \in G^3 \quad (x * y) * z = x * (y * z)$$
Or $H \subset G$ donc
$$\forall (x, y, z) \in H^3 \quad (x * y) * z = x * (y * z)$$
Donc la restriction de $*$ à $H$ est associative, d'où le résultat.
3. $e$ est neutre pour la loi induite par $*$ sur $H$. En effet, $e$ est le neutre de $*$, donc
$$\forall x \in G \quad e * x = x * e = x$$
D'où le résultat.
4. Tout élément de $H$ admet un inverse pour la loi induite par $*$. En effet tout élément $x$ de $H$ admet un inverse $x^{-1}$ dans $G$ pour la loi $*$ et par stabilité de l'inverse sur le sous-groupe $H$, on a $x^{-1} \in H$. Donc tout élément de $H$ admet un inverse dans $H$ pour la loi induite par $*$.
5. On déduit des points précédents que $H$ muni de la loi induite par $*$ est un groupe.

□

**Remarque 2.2.7.**
Il est plus facile de montrer qu'un ensemble est un sous-groupe que de montrer que c'est un groupe (pas besoin de redémontrer l'associativité, etc.). Par exemple $(\mathbb{U}, \times)$ est un groupe, vu comme sous-groupe de $(\mathbb{C}^*, \times)$.
À chaque fois que l'on essaiera de montrer qu'un ensemble est muni d'une structure de groupe, on tentera de le voir comme un sous-groupe d'un groupe bien connu.

**Remarque 2.2.8.**
La réciproque de ce théorème est également vraie (bien que moins utilisée) : si $H$ est un sous-ensemble de $G$ tel que, muni de la loi induite par celle de $G$, $H$ soit un groupe, alors $H$ est un sous-groupe de $G$.

**Exemple 2.2.9.**
Si $n \in \mathbb{N}^*$, $\mathbb{U}_n$ est un sous-groupe de $(\mathbb{U}, \times)$, donc $(\mathbb{U}_n, \times)$ est un groupe.

## 2.3 Morphismes de groupes.

**Définition 2.3.1.**
Soient $(G,*)$ et $(G',\top)$ deux groupes et $\varphi : G \to G'$.

1. On dit que $\varphi$ est un *morphisme du groupe* $(G,*)$ *dans le groupe* $(G',\top)$ ou, par abus de langage, un *morphisme du groupe* $G$ *dans le groupe* $G'$, si pour tous $x,y \in G$, $\varphi(x*y) = \varphi(x)\top\varphi(y)$.
2. Tout morphisme d'un groupe dans lui-même est appelé *endomorphisme*.
3. Tout morphisme de $G$ dans $G'$ qui est une bijection est appelé *isomorphisme de $G$ sur $G'$*. Dans ce cas on dit que $G$ et $G'$ sont *isomorphes*. Un morphisme qui est à la fois un isomorphisme et un endomorphisme est appelé *automorphisme*.

**Remarque 2.3.2.**
• « Morphisme » signifie « forme » en grec.

**Exemple 2.3.3.**
• $\begin{array}{ccc} (\mathbb{Z},+) & \to & (\mathbb{Z},+) \\ x & \mapsto & 2x \end{array}$, est un morphisme, mais pas un isomorphisme.
• $\begin{array}{ccc} (\mathbb{C}^*,\times) & \to & (\mathbb{R}^*,\times) \\ z & \mapsto & |z| \end{array}$, est un morphisme, mais pas un isomorphisme.
• $\begin{array}{ccc} (\mathbb{R},+) & \to & (\mathbb{C}^*,\times) \\ x & \mapsto & \mathrm{e}^{ix} \end{array}$, est un morphisme, mais pas un isomorphisme.
• $\begin{array}{ccc} (\mathbb{R},+) & \to & (\mathbb{R}_+^*,\times) \\ x & \mapsto & \mathrm{e}^{x} \end{array}$ est un isomorphisme de réciproque ln, qui est aussi un isomorphisme.

**Exemple 2.3.4.**
On a déjà manipulé les morphismes suivants, lors des chapitres précédents.
• Si $n \in \mathbb{N}^*$, $\begin{array}{ccc} (\mathbb{C}^*,\times) & \to & (\mathbb{C}^*,\times) \\ z & \mapsto & z^n \end{array}$.
• Si $n \in \mathbb{N}^*$ et $a_1,\dots,a_n \in \mathbb{K}^n$, l'application $\begin{array}{ccc} (\mathbb{K}^n,+) & \to & (\mathbb{K},+) \\ (x_1,\dots,x_n) & \mapsto & a_1x_1+\dots a_nx_n \end{array}$.
• Si $I$ est un intervalle de $\mathbb{R}$, si $a : I \to \mathbb{K}$ est continue, l'application $\begin{array}{ccc} (\mathscr{D}(I,\mathbb{K}),+) & \to & (\mathscr{C}(I,\mathbb{K}),+) \\ f & \mapsto & f'+af \end{array}$.
• Si $a,b \in \mathbb{Z}$, l'application $\begin{array}{ccc} (\mathbb{Z}^2,+) & \to & (\mathbb{Z},+) \\ (x,y) & \mapsto & ax+by \end{array}$.
• Si $a \in \mathbb{K}$, l'application $\begin{array}{ccc} (\mathbb{K}^{\mathbb{N}},+) & \to & (\mathbb{K}^{\mathbb{N}},+) \\ u & \mapsto & (u_{n+1}-au_n)_{n\in\mathbb{N}} \end{array}$.

Dans toute la suite, $(G,*)$ et $(G',\top)$ sont deux groupes de neutres $e$ et $e'$, on adopte une notation muliplicative, et $\varphi : G \to G'$ est un morphisme.

**Théorème 2.3.5.**
Soit $\varphi$ un morphisme de $G$ sur $G'$, on a, $e$ et $e'$ désignant les neutres de $G$ et $G'$ :

1. $\varphi(e) = e'$ ;
2. $\forall x \in G \quad \varphi(x^{-1}) = (\varphi(x))^{-1}$.

**Démonstration.** 1. On a $\varphi(e)\top\varphi(e) = \varphi(e*e) = \varphi(e) = \varphi(e)\top e'$, donc en simplifiant par $\varphi(e)$, on en déduit $\varphi(e) = e'$.
2. Soit $x \in G$. Alors $\varphi(x^{-1})\varphi(x) = \varphi(x^{-1}x) = \varphi(e) = e'$.

□

**Corollaire 2.3.6.**
Sous les mêmes hypothèses, on a

$$\forall x \in G \quad \forall k \in \mathbb{Z} \quad \varphi(x^k) = \varphi(x)^k.$$

**Démonstration.**
Soit $x \in G$. D'après le théorème ci-dessus, on a

$$\varphi(x^0) = \varphi(e) = e' = \varphi(x)^0$$

On peut alors démontrer par récurrence que pour tout $n \in \mathbb{N}$, on a $\varphi(x^n) = \varphi(x)^n$ (l'hérédité résulte directement de la définition de morphisme).

D'après le théorème ci-dessus, pour tout $n \in \mathbb{N}$, $\varphi(x^{-n}) = \varphi(x^n)^{-1}$, d'où $\varphi(x^{-n}) = \varphi(x)^{-n}$.

On en déduit le résultat. □

**Exemple 2.3.7.** 1. $\begin{array}{ccc}\mathbb{C}^* & \to & \mathbb{R}^* \\ z & \mapsto & |z|\end{array}$ est un morphisme de $(\mathbb{C}^*, \times)$ dans $(\mathbb{R}^*, \times)$, donc pour tout $z \in \mathbb{C}^*$, on a

$$\left|\frac{1}{z}\right| = \frac{1}{|z|}$$

2. exp est un morphisme de $(\mathbb{C}, +)$ dans $(\mathbb{C}^*, \times)$, donc pour tout $z \in \mathbb{C}$, $e^{-z} = \frac{1}{e^z}$
3. ln est un morphisme de $(\mathbb{R}_+^*, \times)$ dans $(\mathbb{R}, +)$, donc pour tout $x \in \mathbb{R}_+^*$, on a $\ln(1/x) = -\ln x$.

**Remarque 2.3.8.**
On peut adapter le théorème 2.3.5 dans le cas où on sait seulement que $(G, *)$ est un groupe, $G'$ est un ensemble muni d'une loi de composition interne $\top$ et où $\varphi$ est une application $G \to G'$ vérifiant $\forall (x, y) \in G^2\ \varphi(x * y) = \varphi(x) \top \varphi(y)$. Dans ce cas, on ne peut pas déduire que $(G', \top)$ est un groupe mais seulement que $(\varphi(G), \top)$ est un groupe. Voir aussi le théorème disant que «l'image d'un sous-groupe par un morphisme est un sous-groupe».

**Théorème 2.3.9.** (i) La composée de deux morphismes de groupes est un morphisme de groupe. Plus précisément, soit $(G_1, *_1)$, $(G_2, *_2)$ et $(G_3, *_3)$ trois groupes, $\varphi$ un morphisme de $G_1$ dans $G_2$ et $\psi$ un morphisme de $G_2$ dans $G_3$. Alors $\psi \circ \varphi$ est un morphisme de $G_1$ dans $G_3$.

(ii) La fonction réciproque d'un isomorphisme (en tant qu'application bijective) est un isomorphisme. Plus précisément, soit $(G_1, *_1)$ et $(G_2, *_2)$ deux groupes et $\varphi$ un isomorphisme de $G_1$ sur $G_2$. Alors $\varphi^{-1}$ est un isomorphisme de $G_2$ sur $G_1$.

**Démonstration.**
Les démonstrations pour montrer qu'une application est un morphisme ont TOUJOURS la même structure.

1. $\psi \circ \varphi$ est clairement une application de $G_1$ dans $G_3$. Soit $(x, y) \in G_1^2$, montrons qu'on a $\psi \circ \varphi(x *_1 y) = (\psi \circ \varphi)(x) *_3 (\psi \circ \varphi)(y)$.
   $\varphi$ est un morphisme de groupes donc on a $\varphi(x *_1 y) = \varphi(x) *_2 \varphi(y)$. Or $\psi$ est un morphisme de groupes donc on a $\psi(\varphi(x) *_2 \varphi(y)) = (\psi(\varphi(x)) *_3 \psi(\varphi(y))$.
   D'où $(\psi \circ \varphi)(x *_1 y) = (\psi \circ \varphi)(x) *_3 (\psi \circ \varphi)(y)$.
2. $\varphi^{-1}$ est évidemment une bijection de $G_2$ sur $G_1$. Il suffit donc de montrer que $\varphi^{-1}$ est un morphisme de $G_2$ dans $G_1$.
   Soit $(x, y)^2 \in G_2$. Montrons $\varphi^{-1}(x *_2 y) = \varphi^{-1}(x) *_1 \varphi^{-1}(y)$.
   On a d'une part $\varphi(\varphi^{-1}(x *_2 y)) = x *_2 y$ et d'autre part, comme $\varphi$ est un morphisme, $\varphi(\varphi^{-1}(x) *_1 \varphi^{-1}(y)) = \varphi(\varphi^{-1}(x)) *_2 \varphi(\varphi^{-1})(y)$, d'où $\varphi(\varphi^{-1}(x *_2 y)) = \varphi(\varphi^{-1}(x) *_1 \varphi^{-1}(y))$.
   Or $\varphi$ est injective donc $\varphi^{-1}(x *_2 y) = \varphi^{-1}(x) *_1 \varphi^{-1}(y)$.
   Donc $\varphi^{-1}$ est un morphisme, donc un isomorphisme.

□

**Remarque 2.3.10.**
L'ensemble des automorphismes d'un groupe $G$ est donc un sous-groupe de $(S_G, \circ)$.

**Exemple 2.3.11.**
On a vu que exp et ln sont des isomorphismes réciproques.

**Théorème 2.3.12.** (i) L'image d'un sous-groupe par un morphisme de groupes est un sous-groupe (du groupe d'arrivée).

(ii) Le tiré en arrière d'un sous-groupe par un morphisme est un sous-groupe (du groupe de départ).

**Démonstration.**
Les démonstrations pour montrer qu'un ensemble est un sous-groupe ont TOUJOURS la même structure.

(i) Soient $(G, *)$ et $(G', \top)$ deux groupes de neutres respectifs $e$ et $e'$, et $\varphi : G \to G'$ un morphisme de groupes. Soit $H$ un sous-groupe de $G$. Montrons que $\varphi(H)$ est un sous-groupe de $G'$.

1. On a évidemment $\varphi(H) \subset G'$ et de plus $e \in H$ et $e' = \varphi(e) \in \varphi(H)$.
2. Soit $x, y \in \varphi(H)$. Alors $x$ possède un antécédent $x' \in H$ et $y$ un antécédent $y' \in H$ par $\varphi$. On a alors successivement

$$\begin{aligned} x \top y^{-1} &= \varphi(x') \top \varphi(y')^{-1} && \text{par définition de } x' \text{ et } y' \\ &= \varphi(x') \top \varphi(y'^{-1}) && \text{car } \varphi \text{ est un morphisme} \\ &= \varphi(x' * y'^{-1}) && \text{car } \varphi \text{ est un morphisme} \end{aligned}$$

Donc $x \top y^{-1} \in \varphi(H)$.

$\varphi(H)$ est donc un sous-groupe de $G'$.

(ii) Gardons les même notations que dans le premier point, et notons $H'$ un sous-groupe de $G'$.

1. On a évidemment $\varphi^{\leftarrow}(H') \subset G$ et de plus $e' \in H'$ et $e' = \varphi(e) \in H'$ donc $e \in \varphi^{\leftarrow}(H')$.
2. Soit $x, y \in \varphi^{\leftarrow}(H')$. Alors $\varphi(x), \varphi(y) \in H'$ et donc $\varphi(x * y^{-1}) = \varphi(x) \top (\varphi(y))^{-1} \in H'$ donc $x * y^{-1} \in \varphi^{\leftarrow}(H')$.

$\varphi^{\leftarrow}(H')$ est donc un sous-groupe de $G$.

□

**Remarque 2.3.13.**
On complète la remarque 2.2.7 comme suit : lorsque l'on veut montrer qu'un ensemble est muni d'une structure de groupe, on commence toujours par essayer de l'identifier comme image réciproque (ou directe) d'un sous-groupe d'un groupe bien connu par un morphisme.

**Définition 2.3.14.** (i) On appelle *noyau* de $\varphi$, noté $\operatorname{Ker}\varphi$, l'image réciproque de $\{ e' \}$ par $\varphi$, autrement dit l'ensemble des antécédents de $e'$ par $\varphi$ : $\operatorname{Ker}\varphi = \{ x \in G \mid \varphi(x) = e' \}$.

(ii) On appelle *image* de $\varphi$ notée $\operatorname{Im}\varphi$, l'image directe de $G$ par $\varphi$. Autrement dit $\operatorname{Im}\varphi = \{ \varphi(x) \mid x \in G \}$.

**Exemple 2.3.15.**
Déterminer les images et noyaux des exemples de 2.3.3.

**Théorème 2.3.16.**
Les noyaux et les images sont des sous-groupes respectivement de $G$ et $G'$.

**Démonstration.**
Ceci découle directement du théorème 2.3.12. Néanmoins, redémontrons-le dans le cas particulier du noyau :

Montrons que $\operatorname{Ker}\varphi$ est un sous-groupe de $G$ :

1. On a évidemment $\operatorname{Ker}\varphi \subset G$ et de plus $\varphi(e) = e'$ donc $\operatorname{Ker}\varphi$ est un sous-ensemble non vide de $G$.
2. Soit $x, y \in \operatorname{Ker}\varphi$. Alors on a successivement
$$\begin{aligned}\varphi(x * y^{-1}) &= \varphi(x) \top \varphi(y)^{-1} \\ &= e' \top e'^{-1} \\ &= e'\end{aligned}$$
Donc $x * y^{-1} \in \operatorname{Ker}\varphi$.

Donc $\operatorname{Ker}\varphi$ est un sous-groupe de $G$. □

**Exemple 2.3.17.**
Constatation avec les Im et Ker tirés des exemples de 2.3.3.

**Remarque 2.3.18.**
On complète la remarque 2.3.13 comme suit : lorsque l'on veut montrer qu'un ensemble est muni d'une structure de groupe, on commence toujours par essayer de l'identifier comme noyau ou image d'un morphisme.

**Exemple 2.3.19.**
$\mathbb{U}$ est le noyau du morphisme « module », de $(\mathbb{C}^*, \times)$ dans $(\mathbb{R}^*, \times)$.

La proposition suivante est primordiale.

**Proposition 2.3.20.**
Soit $\varphi : G \to G'$ un morphisme de groupes, soit $x, y \in G$. Alors $\varphi(x) = \varphi(y)$ si et seulement si $xy^{-1} \in \operatorname{Ker}\varphi$.

**Démonstration.**
$\varphi(x) = \varphi(y)$ si et seulement si $\varphi(x)\varphi(y)^{-1} = 1_{G'}$ si et seulement si $\varphi(xy^{-1}) = 1_{G'}$. □

**Remarque 2.3.21.**
Avec les mêmes notations, si on a $a \in \mathscr{G}$ et $y \in G'$ vérifiant $y = \varphi(a)$, l'ensemble des solutions sur $G$ de l'équation $y = \varphi(x)$ est $\{ ax \mid x \in \operatorname{Ker}(\varphi) \}$.

**Exemple 2.3.22.**
Reprendre les exemples exposés en 2.3.4.

On retrouve ainsi la structure des racines $n^{\text{es}}$ d'un nombre complexe, la structure des solutions d'un système linéaire, la structure des solutions d'une équation différentielle linéaire, les solutions d'une relation de Bézout et la structure des suites vérifiant une relation de récurrence arithmético-géométrique.

**Théorème 2.3.23.** (i) $\varphi$ injectif si et seulement si $\operatorname{Ker}\varphi = \{e\}$.

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

**Démonstration.** (ii) Rien de nouveau.

(i) On montre l'implication et sa réciproque :

— Supposons $\varphi$ injectif. Alors $e'$ a au plus un antécédent par $\varphi$. Or $\varphi(e) = e'$ donc il en a au moins un : $e$. Donc $\operatorname{Ker}\varphi = \{ e \}$.

— Réciproquement, supposons $\operatorname{Ker}\varphi = \{ e \}$ et montrons que $\varphi$ est injectif.
Soit $(x, y) \in G^2$ vérifiant $\varphi(x) = \varphi(y)$. Alors on a succesivement

$$\begin{aligned}\varphi(x * y^{-1}) &= \varphi(x) \top \varphi(y)^{-1} \quad \text{car } \varphi \text{ est un morphisme} \\ &= \varphi(x) \top \varphi(x)^{-1} \\ &= e'\end{aligned}$$

Donc $x * y^{-1} \in \operatorname{Ker}\varphi$, donc $x * y^{-1} = e$, donc $x = y$.

□

**Remarque 2.3.24.**
Pour montrer qu'un morphisme est injectif, on utilisera **TOUJOURS** le noyau et **JAMAIS** (ou presque) la méthode classique pour des fonctions quelconques : c'est beaucoup plus rapide !

**Exemple 2.3.25.**
Reprendre les exemples de exp et ln, ainsi que les morphismes vus en 2.3.4.

# 3 Anneaux

## 3.1 Structure d'anneau.

**Définition 3.1.1.**
On appelle *anneau* tout triplet $(A, +, \times)$ constitué d'un ensemble $A$ et de deux lois internes sur $A$, une loi $+$ appelée *addition* et une loi $\times$ appelée *multiplication*, vérifiant :

1. $(A, +)$ est un groupe abélien dont l'élément neutre est noté 0 (ou $0_A$ si ambiguïté) ;
2. $(A, \times)$ est un magma associatif possédant un neutre noté 1 (ou $1_A$ si ambiguïté) ;
3. La multiplication est distributive par rapport à l'addition.

Si la loi $\times$ est commutative, on dit que l'anneau $A$ est commutatif.

**Exemple 3.1.2.**
• $\mathbb{C}$, $\mathbb{R}$, $\mathbb{Q}$, $\mathbb{Z}$ et $\mathscr{F}(\mathbb{R}, \mathbb{R})$ avec $+$ et $\times$ sont des anneaux.
• $(\mathbb{R}^3, +, \wedge)$ et $(\mathscr{F}(\mathbb{R}, \mathbb{R}), +, \circ)$ n'en sont pas.
• $(\mathbb{Z}/n\mathbb{Z}, +, \times)$ en est un.
• $(\mathscr{M}_n(\mathbb{R}), +, \times)$ est un anneau.
• On note $\mathscr{L}(\mathbb{R}^2)$ l'ensemble des endomorphismes de $\mathbb{R}^2$. Alors $(\mathscr{L}(\mathbb{R}^2), +, \circ)$ est un anneau.
• Si $X$ est un ensemble, $(\mathbb{R}^X, +, \times)$ est un anneau.

**Remarque 3.1.3.**
Quand il n'y a pas d'ambiguïté, on dit juste que $A$ est un anneau sans préciser les lois. Pour la multiplication, on utilise les mêmes raccourcis de notation que dans $\mathbb{R}$ (omission du $\times$, etc).

 Tous les éléments de $A$ ne sont pas inversibles pour $\times$. Les éléments inversibles sont parfois appelés *éléments unités* de $A$ et leur ensemble est noté $U(A)$, $A^\times$, $A^*$, voire $E(A)$ (*Einheit*).

 Avec cette notation, $A^*$ n'est pas nécessairement $A \setminus \{ 0 \}$.

**Théorème 3.1.4** (Règles de calcul dans un anneau)**.**
Soit $A$ un anneau, $a, b \in A$ et $n \in \mathbb{Z}$.

1. $a \times 0 = 0 \times a = 0$.
2. $-(a \times b) = (-a) \times b = a \times (-b)$. Cas particuliers : $(-a)(-b) = ab$, $(-a)^2 = a^2$, $(-1)^2 = 1$.
3. $n(ab) = (na)b = a(nb)$.

**Démonstration.** 1. Il suffit de remarquer $a \times 0 + a \times 0 = a \times (0 + 0) = a \times 0$ et de simplifier par $a \times 0$ (ce qui est légitime car il est inversible pour la loi $+$).

2. On a successivement :

$$\begin{aligned} a\times b+(-a)\times b &= (a-a)\times b \quad \text{par distributivité}\\ &= 0\times b\\ &= 0 \qquad\qquad\qquad\qquad \text{d'après (1)}\end{aligned}$$

Donc $(-a)\times b$ est l'opposé de $a\times b$, donc $(-a)\times b = -(a\times b)$.

On montre de même $a\times(-b) = -(a\times b)$.

3. **Cas où $n\in\mathbb{N}$ :** On peut s'en convaincre par récurrence. Le cas $n=0$ se déduit du (1), l'hérédité se montre par application de la distributivité.

**Cas où $n<0$ :** alors $-n\in\mathbb{N}$, et on a

$$\begin{aligned} n(a\times b) =& (-n)(-(a\times b)) \text{ par définition de}\\ & \text{la multiplication par un entier}\\ =& (-n)((-a)b) \text{ d'après 2}\\ =& ((-n)(-a))b\\ & \text{d'après le cas précédent}\end{aligned}$$

L'autre égalité se démontre de la même façon.

□

**Remarque 3.1.5.**
On voit ainsi que si l'anneau $A$ possède au moins deux éléments, alors $1_A\neq 0_A$ et $0_A$ n'est pas inversible.

**Exercice 3.1.6.**
Étant donné un anneau $(A,+,\times)$, la notation $n\times a$ peut désigner d'une part le produit dans $A$ de $n$ par $a$ si $n$ et $a$ sont deux éléments de $A$, d'autre part si $a\in A$ et $n\in\mathbb{Z}$, la valeur $a+\ldots+a$ où $a$ est répété $n$ fois dans le cas où $n\geqslant 0$ et l'opposé de $a+\ldots+a$ où $a$ est répété $-n$ fois si $n<0$.

Dans le cas où $A$ et $\mathbb{Z}$ sont disjoints, cette ambiguïté n'est évidemment pas gênante si on sait auquel des deux ensembles $A$ et $n$ appartient.

Dans le cas contraire, cette ambiguïté n'est pas gênante non plus. Pourquoi ?

**Théorème 3.1.7.**
Soient $n\in\mathbb{N}$, $(A,+,\times)$ un anneau et $a,b\in A$ tels que $a$ et $b$ commutent (i.e. $a\times b = b\times a$). Alors :

(i) Formule du binôme de Newton :

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

(ii) $a^n-b^n = (a-b)\sum_{k=0}^{n-1}a^k b^{n-k-1}$.

**Démonstration.**
On remarque d'abord que si $a,b$ commutent, alors toutes les puissances de $a$ et de $b$ commutent (le faire par récurrence).

Recopier la démonstration concernant des complexes ou des matrices carrées, à nouveau en étant conscient de l'importance de l'hypothèse "$a$ et $b$ commutent". □

**Proposition 3.1.8** (Groupe des inversibles)**.**
Soit $(A,+,\times)$ un anneau. Alors $(A^*,\times)$ est un groupe, autrement dit l'ensemble des éléments inversibles de $A$, muni de (la loi induite par) la multiplication de $A$ est un groupe.

**Démonstration.**
— Remarquons tout d'abord que $\times$ induit une lci sur $A^*$. Soit $x$ et $y$ deux éléments de $A^*$. $x$ et $y$ sont donc deux éléments inversibles du magma $(A,\times)$ donc, d'après la proposition 1.2.10, $x\times y$ est inversible.
— $\times$ étant une loi associative sur $A$, elle l'est aussi sur $A^*$.
— $1_A$ est inversible car $1_A\times 1_A = 1_A$. Donc $1_A\in A^*$. De plus $1_A$ est élément neutre pour la multiplication sur $A$, donc est élément neutre pour la multiplication sur $A^*$.
— Pour tout $x\in A^*$, $x$ possède un inverse $y$ dans $A$. On remarque immédiatement que $y$ est lui-même inversible (d'inverse $x$), donc $y\in A^*$. Tout élément du magma $(A^*,\times)$ est donc inversible dans $A^*$.

$(A^*,\times)$ est donc un groupe, de neutre $1_A$. □

**Exemple 3.1.9.**
Quel est le groupe des inversibles des anneaux $(\mathbb{Z},+,\times)$, $(\mathbb{Q},+,\times)$, $(\mathbb{R},+,\times)$ et $(\mathbb{C},+,\times)$ ?

**Définition 3.1.10.** 1. On appelle *anneau nul* tout anneau $(\{0\},+,\times)$ (0 est alors le neutre pour les deux lois !).

2. Dans un anneau $A$, on appelle diviseur de 0 tout élément *$a$ non nul*, tel qu'il existe *$b$ non nul* vérifiant $a\times b = 0_A$ ou $b\times a = 0_A$.

3. On appelle *anneau intègre* tout anneau commutatif non nul *ne possédant aucun diviseur de* 0*, c'est-à-dire vérifiant*

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

**Remarque 3.1.11.**
Pour tout anneau $A$, on a $0_A = 1_A$ si et seulement si $A$ est un anneau nul. En effet, supposons $0_A = 1_A$, alors pour tout $x \in A$, on a $x = 1_A \times x = 0_A \times x = 0_A$, donc tout élément de $A$ est nul, donc $A$ est l'anneau nul. Réciproquement si $A$ est un anneau nul, tous les éléments de $A$ sont égaux (puisqu'il n'y en a qu'un !) donc $0_A = 1_A$.

**Remarque 3.1.12.**
Un élément inversible $a$ n'est jamais un diviseur de 0. En effet, pour tout $b$ vérifiant $ab = 0$, on a nécessairement $a^{-1}ab = 0$, donc $b = 0$.

**Exemple 3.1.13.**
• Les anneaux usuels $\mathbb{C}, \mathbb{R}, \mathbb{Q}, \mathbb{Z}$ sont intègres.
• $(\mathscr{F}(\mathbb{R},\mathbb{R}), +, \times)$ n'est pas intègre : ex : considérer $f, g : \mathbb{R} \to \mathbb{R}$, $f(x) = 0$ si $x \geqslant 0$ et $g(x) = 0$ si $x \leqslant 1$.
• $\mathbb{Z}/6\mathbb{Z}$ n'est pas intègre : $\bar{2} \times \bar{3} = \bar{0}$. De manière générale, $\mathbb{Z}/n\mathbb{Z}$ n'est pas intègre quand $n$ est composé.
• $(\mathscr{L}(\mathbb{R}^2), +, \circ)$ n'est pas intègre. Par exemple avec $f(x,y) = (x,0)$ et $g(x,y) = (0,y)$ nous avons $f \circ g = 0$.
• $\mathscr{M}_n(\mathbb{K})$ n'est pas intègre non plus, comme nous l'avons déjà vu en début d'année. En effet, $\mathscr{M}_n(\mathbb{K})$ n'est pas un anneau commutatif, et de plus cet anneau possède des diviseurs de zéro non nuls.

**Remarque 3.1.14.**
Attention donc aux simplifications de produits dans les anneaux : si l'anneau est intègre, tout fonctionne comme dans $\mathbb{R}$ : $ab = ac \Rightarrow a(b-c) = 0 \Rightarrow (a = 0 \text{ ou } b = c)$.

Sinon, on sait qu'on peut simplifier par des éléments inversibles mais on a du mal à en dire plus (quand un élément est non inversible, il se peut qu'il soit simplifiable ou non [3]).

3. Regarder l'ensemble des suites à valeurs entières muni de l'addition et de la multiplication terme à terme

## 3.2 Sous-anneaux

Un sous-anneau est à un anneau ce qu'un sous-groupe est à un groupe, à un détail près.

**Définition 3.2.1.**
Soit $(A, +, \times)$ un anneau, soit $B$ un ensemble. Alors, $B$ est un sous-anneau de $(A, +, \times)$ si
— $B \subset A$ ;
— $B$ est un sous-groupe de $(A, +)$ ;
— $B$ est stable par $\times$ : pour tout $x, y \in B$, $xy \in B$ ;
— $1_A \in B$.

**Remarque 3.2.2.**
Le caractère de sous-groupe d'un sous-anneau $B$ implique que $B \neq \varnothing$, la condition $1_A \in B$ est toutefois primordiale.

Par exemple, $2\mathbb{Z}$ vérifie les trois premiers points, mais n'est pas un sous-anneau de $(\mathbb{Z}, +, \times)$.

**Exemple 3.2.3.**
Si $(A, +, \times)$ est un anneau, alors $A$ est un sous-anneau de $(A, +, \times)$.

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

**Exercice 3.2.4** (anneau des entiers de Gauss)**.**
On note $\mathbb{Z}[i] = \{\, a + ib \mid \ a, b \in \mathbb{Z} \,\}$.

Montrer que $\mathbb{Z}[i]$ est un sous-anneau de $(\mathbb{C}, +, \times)$.

**Exercice 3.2.5.**
Quel est le plus petit sous-anneau d'un anneau $(A, +, \times)$ ?

**Proposition 3.2.6.**
Soit $(A, +, \times)$ un anneau, soit $B$ une partie de $A$.

Alors, $B$ est un sous-anneau de $(A, +, \times)$ si et seulement si, muni des lois $+$ et $\times$ induites sur $B$, $(B, +, \times)$ est un anneau.

**Démonstration.**
Élémentaire, procéder exactement comme pour les groupes. □

### 3.3 Morphismes d'anneaux

Les morphismes d'anneaux sont aux anneaux ce que les morphismes de groupes sont aux groupes, à un détail près.

**Définition 3.3.1.**
Soit $(A,+,\times)$, $(B,+,\times)$ deux anneaux. Un morphisme entre ces deux anneaux est une application

$$\varphi : A \to B$$

vérifiant les propriétés suivantes.
— $\forall x,y \in A,\ \varphi(x+y) = \varphi(x)+\varphi(y)$
— $\forall x,y \in A,\ \varphi(xy) = \varphi(x)\varphi(y)$
— $\varphi(1_A) = 1_B$
Si l'anneau de départ est égal à l'anneau d'arrivée, on parle bien entendu d'endomorphisme d'anneau.

Un morphisme d'anneaux bijectif est un isomorphisme d'anneau.

Enfin, un morphisme bijectif d'un anneau sur lui-même est un automorphisme d'anneau.

**Exemple 3.3.2.**
Dans l'anneau $(\mathbb{C},+,\times)$, on a les automorphismes Id et $z \mapsto \bar{z}$.

Sur l'anneau des fonctions réelles, si $a \in \mathbb{R}$, l'application d'évaluation $f \mapsto f(a)$ est un morphisme à valeurs dans l'anneau $\mathbb{R}$.

L'application nulle n'est pas un morphisme d'anneaux !

**Remarque 3.3.3.**
Un morphisme d'anneau est un morphisme de groupes. La notion de noyau ne change pas : pour un morphisme $\varphi$ entre deux anneaux $A$ et $B$,

$$\mathrm{Ker}(\varphi) = \{\, x \in A \mid \varphi(x) = 0_B \,\}.$$

Notamment, un morphisme d'anneaux est injectif si et seulement si son noyau est réduit à l'élément nul.

Remarquons que par définition $1_A \notin \mathrm{Ker}(\varphi)$ : ainsi, le noyau d'un morphisme d'anneaux n'est JAMAIS un sous-anneau de l'anneau de départ, en dehors de l'exemple dégénéré de l'anneau nul.

**Proposition 3.3.4** (transport par morphisme)**.**
Soit $(A,+,\times)$, $(B,+,\times)$ deux anneaux, soit $\varphi : A \to B$ un morphisme entre ces deux anneaux.

1. Si $C$ est un sous-anneau de $(A,+,\times)$, alors $\varphi(C)$ est un sous-anneau de $(B,+,\times)$.
2. Si $D$ est un sous-anneau de $(B,+,\times)$, alors $\varphi^{\leftarrow}(D)$ est un sous-anneau de $(A,+,\times)$.

**Démonstration.**
Élémentaire, procéder exactement comme pour les groupes. □

**Remarque 3.3.5.**
Si $\varphi$ est un morphisme entre deux anneaux $A$ et $B$, alors $\mathrm{Im}(\varphi) = \varphi(A)$ est un sous-anneau de $B$.

## 4 Structure de corps.

**Définition 4.0.1.**
On appelle *corps tout anneau commutatif non nul dans lequel tout élément non nul est inversible pour* $\times$.

**Exemple 4.0.2.**
• $\mathbb{C}$, $\mathbb{R}$ et $\mathbb{Q}$ sont des corps. $\mathbb{N}$ et $\mathbb{Z}$ n'en sont pas.
• $\mathbb{Z}/p\mathbb{Z}$ est un corps si et seulement si $p$ est premier.

**Proposition 4.0.3.** (i) Un corps est intègre.
(ii) Si $\mathbb{K}$ est un corps, on a $\mathbb{K}^* = \mathbb{K}\backslash\{0\}$ (qui est un groupe pour la loi induite par $\times$).

**Démonstration.** (i) Soit $(\mathbb{K},+,\times)$ un corps. Soit $(a,b) \in \mathbb{K}^2$ vérifiant $ab = 0$. Supposons que $a$ est non nul. Alors $a$ est inversible donc $a^{-1} \times ab = a^{-1} \times 0$, donc $b = 0$.
On a donc $a = 0$ ou $b = 0$.

(ii) Tout élément non nul est inversible pour $\times$ d'après la définition, d'où $\mathbb{K}^* = \mathbb{K} \setminus \{\, 0 \,\}$ et on sait d'après la proposition 3.1.8 que $(\mathbb{K}^*,\times)$ est un groupe. □

**Remarque 4.0.4.**
Un corps est un anneau qui est intègre, par contre

un anneau intègre n'est pas forcément un corps ! Trouvez un exemple ...