Relations d'équivalence

Baptiste Calmès

16 janvier 2022

Table des matières

1 Définition

1.1 Définition. Une *relation* sur un ensemble E est un sous-ensemble de $E \times E$. Si R est une relation, on écrit alors souvent $x \sim_R y$ au lieu de $(x, y) \in R$.

C'est une manière de formaliser qu'il y a une relation entre certains éléments de E. On dit que x est en relation avec y si $x \sim_R y$ (i.e. si $(x, y) \in R$).

1.2 Définition. Une relation R sur un ensemble E est appelée une *relation d'équivalence* si elle satisfait aux propriétés suivantes :

1. (réflexivité) $\forall x$, $x \sim_R x$;
2. (symétrie) $\forall x, y \in E$, $x \sim_R y$ implique yRx ;
3. (transitivité) $\forall x, y, z \in E$, $x \sim_R y$ et $y \sim_R z$ implique $x \sim_R z$.

Si R est une relation d'équivalence, on écrit alors souvent $x \sim_R y$ au lieu de $x \sim_R y$, voire même $x \sim y$ si la relation est claire par le contexte.

1.3 Exemple. Voici quelques exemples de relations d'équivalence (le vérifier).

1. E est l'ensemble des droites du plan et la relation est le parallèlisme.
2. E est l'ensemble des triangles du plan et la relation est le fait d'être semblables.
3. E est l'ensemble des fonctions continues par morceaux $\mathbb{R} \to \mathbb{R}$ et la relation est l'égalité des valeurs sauf en un nombre fini de points.

1.4 Exemple. Voici également quelques exemples de relations qui ne sont pas d'équivalence.

1. $E = \mathbb{R}$ et la relation est le fait d'être inférieur ou égal.
2. $E = \mathbb{R}$ et la relation est le fait d'être à distance au plus 1.

1.5 Exemple. La *relation triviale* est celle où $R = \{(x, x),\ \forall x \in E\}$, autrement dit $x \sim_R y$ ssi $x = y$, et la relation la plus grossière est celle où $R = E \times E$, autrement dit $x \sim_R y$ pour tous x, y. Ce sont bien entendu des relations d'équivalence.

L'exemple qui suit est *très important*. L'idée est qu'on veut considérer deux éléments d'un groupe G comme équivalents si l'on peut passer de l'un à l'autre par multiplication *à droite* par un élément d'un sous-groupe H (donné).

1.6 Exemple. Soit G un groupe, et H un sous-groupe de G. Posons $x \sim_R y$ si $x^{-1}y \in H$. Montrer que c'est équivalent à demander qu'il existe $h \in H$ tel que $xh = y$. On dit que x est *congru* à y *modulo* H à droite. Cela définit une relation d'équivalence sur G.

1.7 Remarque. Si $H = \{1\}$ ou si $H = G$, on retrouve respectivement les relations triviale et grossière précédentes.

1.8 Exercice. Bien entendu, la notion existe aussi en remplaçant la droite par la gauche. La définir.

1.9 Remarque. Quand le groupe est abélien, ces deux relations, définies par multiplication à droite ou à gauche, sont les mêmes.

1.10 Exercice. Si $G = \mathbb{Z}$, et que $H = n\mathbb{Z}$ pour un $n \neq 0$, montrer qu'avec la relation précédente, on a $x \sim y$ si et seulement si n divise $x - y$. En fait, c'est vrai même avec $n = 0$, mais à quoi ressemble la relation d'équivalence dans ce cas ?

La relation précédente sur $\mathbb{Z}$ est particulièrement importante pour l'arithmétique, on utilise donc une terminologie spécifique.

1.11 Définition. Quand $x \sim_R y$, on dit que x est *congru* à y *modulo* n et on note

$$x \equiv y \mod n \qquad \text{ou encore} \qquad x \equiv y\ [n]$$

2 Classes d'équivalence

2.1 Définition. Étant donné une relation d'équivalence R sur E, et $x \in E$, on appelle *classe* de x le sous-ensemble de E constitué des éléments y tels que $x \sim_R y$. On le note $\overline{x}^R$. On a donc

$$\overline{x}^R = \{y \in E,\ x \sim_R y\}.$$

Lorsque la relation est claire, on note juste $\overline{x}$.

2.2 Remarque. Bien entendu, on a $\overline{x}^R = \overline{y}^R$ si et seulement si $x \sim_R y$.

2.3 Exemple. Reprenons l'exemple 1.6. Si $g \in G$, alors

$$\overline{g} = gH = \{gh, h \in H\}.$$

Pour cette raison, on écrira souvent $gH = g'H$ (resp. $Hg = Hg'$) pour dire que g et g' sont congrus modulo H à droite (resp. à gauche).

Remarquons également que $\overline{1_G} = H$, aussi bien pour la relation à gauche que pour la relation à droite.

En fait, se donner une relation d'équivalence sur E est la même chose que se donner une partition de E, i.e. qu'écrire E comme une union de sous-ensembles disjoints. Ces sous-ensembles sont justement les classes d'équivalences. Plus précisément :

2.4 Définition. Soit $\mathcal{U} \subset \mathcal{P}(E)$ un ensemble de parties d'un ensemble E. On dit que $\mathcal{U}$ est une *partition* de E si

1. $C \neq \emptyset$ pour tout $C \in \mathcal{U}$;
2. $\bigcup_{C \in \mathcal{U}} C = E$;
3. $C \cap C' = \emptyset$ pour tous $C, C' \in \mathcal{U}$ avec $C \neq C'$.

Pour tout élément $x \in E$, on a alors un unique $C \in \mathcal{U}$ tel que $x \in C$, qu'on note alors C_x.
On associe à une telle partition $\mathcal{U}$ la relation $R_{\mathcal{U}}$ sur E définie par

$$x \sim_{R_{\mathcal{U}}} y \quad \text{si} \quad C_x = C_y.$$

À l'inverse, si R est une relation d'équivalence sur E, on peut considérer

$$\mathcal{U}_R = \{\overline{x}^R, \quad x \in E\} \subset \mathcal{P}(E).$$

2.5 Proposition. *Étant donné un ensemble E*

1. *Pour tout partition $\mathcal{U}$ de E, la relation $R_{\mathcal{U}}$ est une relation d'équivalence, dont les classes d'équivalence sont les $C \in \mathcal{U}$.*
2. *Pour toute relation d'équivalence R sur E, le sous-ensemble des parties $\mathcal{U}_R$ est une partition de E.*
3. *$\mathcal{U} \mapsto R_{\mathcal{U}}$ et $R \mapsto \mathcal{U}_R$ sont des bijections inverses l'une de l'autre entre les partitions de E et les relations d'équivalence sur E.*

Autrement dit, se donner une relation d'équivalence sur E est "la même chose" que se donner une partition de E. Même si cette seconde description peut sembler plus simple, dans les exemples pratiques, on a souvent la donnée de quand $x \sim_y$.

3 Ensemble quotient

3.1 Définition (ensemble quotient)**.** L'ensemble des classes d'équivalences d'un ensemble E par une relation d'équivalence R s'appelle l'*ensemble quotient* de E par R et se note E/R ou bien $E/\sim$.

3.2 Notation. Dans l'exemple 1.6 d'une relation d'équivalence sur G définie à l'aide d'un sous-groupe H, on note G/H l'ensemble quotient pour la relation modulo H à droite, et symétriquement $H\backslash G$ l'ensemble quotient pour la relation modulo H à gauche.

La notation suivante est fondamentale.

3.3 Notation. Le quotient de $\mathbb{Z}$ par son sous-groupe $n\mathbb{Z}$ est donc noté $\mathbb{Z}/n\mathbb{Z}$.

3.4 Lemme. *Soit m un élément de $\mathbb{Z}$ et soit r le reste de la division euclidienne de m par n (avec $n \neq 0$). Alors $m \equiv r \mod n$, autrement dit $\overline{m} = \overline{r}$ dans $\mathbb{Z}/n\mathbb{Z}$.*

3.5 Proposition. *Soit $n \in \mathbb{N}^*$. On a*

$$\mathbb{Z}/n\mathbb{Z} = \{\overline{0}, \overline{1}, \ldots, \overline{n-1}\}$$

et toutes ces classes sont différentes. En particulier $\#(\mathbb{Z}/n\mathbb{Z}) = n$.

3.6 Remarque. Si $n = 0$, alors $\mathbb{Z}/0\mathbb{Z}$ est en bijection avec $\mathbb{Z}$.

4 Théorème de Lagrange

4.1 Lemme. *Si E est un ensemble fini muni d'une relation d'équivalence R, on a*

$$\#E = \sum_{C \in E/R} \#C \tag{4.1}$$

et en particulier, si toutes les classes d'équivalences ont le même nombre d'élément N, on a

$$\#E = \#(E/R) \cdot N. \tag{4.2}$$

4.2 Théorème (Lagrange)**.** *Soit G un groupe fini et H un sous-groupe de G. Alors le cardinal de H divise celui de G, et plus précisément*

$$\#G = \#(G/H) \cdot \#H$$

5 Application quotient

Soit E un ensemble muni d'une relation d'équivalence R.

5.1 Définition. L'application canonique

$$\begin{array}{rccc} \pi_R : & E & \to & E/R \\ & x & \mapsto & \overline{x} \end{array}$$

est appelée *projection sur le quotient*.

5.2 Remarque. Soient $x, y \in E$, on a $\overline{x} = \overline{y}$ si et seulement si $\pi_R(x) = \pi_R(y)$, par définition.

Considérons maintenant une application quelconque $f : E \to F$. On peut lui associer une relation d'équivalence sur E de la manière suivante.

5.3 Définition. On pose $x \sim_f y$ si $f(x) = f(y)$. Cela définit une relation d'équivalence R_f sur E.

On a ainsi $\overline{x} = f^{-1}(f(x))$.

5.4 Proposition (décomposition canonique d'une application)**.** *Dans la situation précédente, notons $\pi_f = \pi_{R_f}$. Alors :*

1. *L'application f se factorise de manière unique en une application $\bar{f} : E/R_f \to F$ telle que $f = \bar{f} \circ \pi_f$.*
2. *L'application π_{R_f} est surjective et l'application $\bar{f}$ est injective.*
3. *L'application $\bar{f}$ arrive en fait dans $\mathrm{im}(f)$ et induit une bijection $E/R_f \to \mathrm{im}(f)$.*
4. *Toute factorisation $f = i \circ g$ avec $g : E \to G$ et $i : G \to F$ injective se factorise canoniquement par la précédente en le sens qu'il existe une unique application $h : E/R_f \to G$ telle que $p = h \circ \pi_f$ et $i \circ h = \bar{f}$.*

Posons-nous maintenant une question un peu différente. Étant donné une application $f : E \to F$ et une relation R sur E, a priori sans rapport avec f, en quel sens f peut-elle être compatible à la relation d'équivalence ?

5.5 Proposition. *Les conditions suivantes sont équivalentes.*

1. *Pour tous $x, y \in E$, on a $x \sim_R y$ implique $f(x) = f(y)$;*
2. *Pour tous $x, y \in E$, on a $x \sim_R y$ implique $x \sim_{R_f} y$;*
3. *On a l'inclusion $R \subset R_f$ (comme sous-ensembles de $E \times E$).*

5.6 Proposition. *Si $f : E \to F$ satisfait aux conditions équivalentes de la proposition 5.5, si et seulement si elle se factorise en une application $\bar{f} : E/R \to F$ telle que $f = \bar{f} \circ \pi_f$. Une telle application $\bar{f}$ est alors unique.*

5.7 Définition. Si les conditions de la proposition 5.5 sont vérifiées, on dit que l'application f *passe aux classes d'équivalences* de R, ou encore que f *passe au quotient* par R.

6 Passage d'une loi au quotient

Lorsqu'un ensemble E est muni d'une loi (par exemple E est un groupe) ainsi que d'une relation d'équivalence R, on veut savoir si l'on peut définir de manière naturelle une loi sur le quotient E/R. Nous ne traiterons ici que du cas des lois à deux entrées, internes et externes car ce sont les plus courantes, mais le principe est le même pour d'autres lois.

L'idée est simple : on veut que le résultat de la loi appliquée à (x, y) ne change pas de classe d'équivalence tant que x (resp. y) ne change pas de classe d'équivalence.

Soient E et F deux ensembles, respectivement munis de relations binaires R et S. On définit une relation notée $R \times S$ sur $E \times F$ en considérant le sous-ensemble de $E \times E \times F \times F$ qui est exactement $R \times S$ si on permute les deux facteurs centraux $E \times E \times F \times F \simeq E \times F \times E \times F$. Autrement dit :

$$(x_1, y_1) \sim_{R\times S} (x_2, y_2) \iff x_1 \sim_R x_2 \quad \text{et} \quad y_1 \sim_S y_2.$$

6.1 Lemme. *Si R et S sont des relations d'équivalence, alors $R \times S$ aussi. On l'appelle la relation d'équivalence produit de R et de S.*

Les lois qui nous intéressent sont soit internes, donc des applications $E \times E \to E$, soit externes, donc des applications $K \times E \to E$ où K est un autre ensemble. Pour englober les deux cas, considèrons donc le cas d'une loi $E \times F \to G$, notée $\star$, où

— E est muni d'une relation d'équivalence R ;

— F est muni d'une relation d'équivalence S ;

— G est muni d'une relation d'équivalence T.

6.2 Définition. On dit que la loi passe au quotient si la composée $E \times F \to G \to G/T$ passe au quotient par $R \times S$ au sens de la définition 5.7 ; autrement dit, si

$$x_1 \sim_R x_2 \quad \text{et} \quad y_1 \sim_S y_2 \Longrightarrow (x_1 \star y_1) \sim_T (x_2 \star y_2)$$

6.3 Théorème. *Si la loi passe au quotient, il existe une unique loi $E/R \times F/S \to G/T$, notée provisoirement $\bar{\star}$,telle que pour tous $x \in E$ et $y \in F$, on ait :*

$$\overline{x}^R \bar{\star} \overline{y}^S = \overline{x \star y}^T .$$

6.4 Remarque. Si une loi satisfait à certaines égalités (comme l'associativité, la commutativité, etc.), alors la loi induite sur E/R satisfait automatiquement aux mêmes égalités.

6.1 Cas des groupes

Soit G un groupe. Nous allons montrer que les relations d'équivalence R sur G telles que la loi de G passe au quotient G/R sont les relations induites par un sous-groupe comme dans l'exemple 1.6 où le sous-groupe est de plus *normal*.

Regardons d'abord de plus près le cas discuté dans l'exemple 1.6. Rappelons la terminologie suivante de théorie des groupes.

6.5 Définition. Soit H un sous-groupe d'un groupe G. On dit que H est *normal* si pour tout $g \in G$ et pour tout $h \in H$, on a $ghg^{-1} \in H$. Autrement dit, le sous-groupe H est stable par conjugaison par tout élément de G.

6.6 Remarque. Si G est un groupe abélien, tout sous-groupe de G est normal, puisque $ghg^{-1} = gg^{-1}h = h$.

6.7 Proposition. *Soit H un sous-groupe de G. La loi de G passe au quotient pour la relation d'équivalence ${}_H\sim$ si et seulement si H est un sous-groupe normal. Si c'est le cas, la relation modulo H à droite coïncide avec la relation modulo H à gauche.*

6.8 Lemme. *Si H est un sous-groupe normal de G, alors $\overline{1_G}$ est l'élément neutre de G/H et $\overline{g^{-1}}$ est l'inverse de $\overline{g}$. De plus, la projection $\pi : G \to G/H$ est un morphisme de groupes.*

Cela montre que non seulement G/H est bien muni d'une loi (associative par la remarque 6.4), mais qu'en plus elle admet bien un élément neutre et des inverses, donc c'est bien une loi de groupe.

6.9 Définition. Dans la situation précédente, c'est-à-dire si H est un sous-groupe normal de G, on dit que G/H est le *groupe quotient* de G par le sous-groupe H.

6.10 Proposition. *Soit R une relation d'équivalence sur un groupe G. Supposons que la loi de groupe sur G passe au quotient G/R, alors la classe du neutre $\overline{1}^R$ est un sous-groupe normal de G et R est la relation d'équivalence induite par ce sous-groupe normal.*

Voici l'exemple qui sera le plus important pour la suite de ce cours.

6.11 Exemple. L'addition de $\mathbb{Z}$ passe au quotient de la relation d'équivalence de congruence modulo n de la notation 3.3.

Elle fait donc de $\mathbb{Z}/n\mathbb{Z}$ un groupe abélien, dont l'élément neutre est $\overline{0}$.

Nous reviendrons sur cet exemple de nombreuses fois, et en particulier décrirons tous les sous-groupes et quotients de $\mathbb{Z}$.

Dans le cas des groupes, la proposition 5.4 se décline ainsi :

6.12 Théorème (décomposition canonique d'un morphisme de groupes)**.** *Soit $f : G \to F$ un morphisme de groupes. Alors*

— $H = \ker(f)$ *est un sous-groupe normal de* G *;*
— *la relation* R_f *est égale à la relation d'équivalence modulo* H *;*
— f *se factorise uniquement en* $f = \bar{f} \circ \pi_f$ *;*
— $\bar{f}$ *est un morphisme de groupes ;*
— $\bar{f}$ *induit un isomorphisme* $G/H \simeq \mathrm{im}(f)$.

6.2 Cas des anneaux

Le cas des anneaux concerne deux lois à la fois, l'addition (commutative) et la multiplication de l'anneau. Nous allons montrer que si un anneau A est muni d'une relation d'équivalence R, alors les deux lois passent au quotient A/R si et seulement la relation d'équivalence est celle induite par un *idéal* de A. Commençons donc par examiner ce que cela veut dire.

Soit A un anneau, et soit R une relation d'équivalence sur A. En particulier A muni de son addition (notée $+$) est un groupe abélien. Par la proposition 6.10, pour que cette loi passe au quotient A/R, il faut que la relation d'équivalence soit celle induite par un sous-groupe (notons-le I) de A pour cette loi.

6.13 Proposition. *Pour que la loi multiplicative passe au quotient* A/I*, il faut et il suffit que* I *soit un idéal (bilatère) de* A*, c'est-à-dire qu'en plus d'être un sous-groupe additif, il vérifie que pour tout* $a \in A$ *et tout* $i \in I$*, on ait* $ia \in I$ *(idéal à gauche) et* $ai \in I$ *(idéal à droite).*

6.14 Définition (idéal)**.** On dit qu'un sous-groupe additif I de A est un *idéal bilatère* de A s'il satisfait aux conditions de la proposition 6.13.

Voici à nouveau l'exemple le plus important de ce cours.

6.15 Exemple. Pour tout $n \in \mathbb{Z}$, le sous-groupe $n\mathbb{Z}$ de $\mathbb{Z}$ est un idéal (bilatère) de $\mathbb{Z}$. En particulier, le groupe abélien $\mathbb{Z}/n\mathbb{Z}$ de l'exemple 6.11 est naturellement muni d'une multiplication telle que la projection $\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ soit un morphisme d'anneau.

Dans le cas des anneaux, la proposition 5.4 se décline ainsi :

6.16 Théorème (décomposition canonique d'un morphisme d'anneaux)**.** *Soit* $f : A \to B$ *un morphisme d'anneaux. Alors*
— $I = \ker(f)$ *est un idéal bilatère de* A*;*
— *la relation* R_f *est égale à la relation d'équivalence modulo* I *;*
— f *se factorise uniquement en* $f = \bar{f} \circ \pi_f$ *;*
— $\bar{f}$ *est un morphisme d'anneaux ;*
— $\bar{f}$ *induit un isomorphisme* $A/I \simeq \mathrm{im}(f)$.

A Groupes

On rappelle les définitions suivantes :

A.1 Définition (groupe)**.** Un *groupe* est un ensemble G muni d'une loi $G \times G \to G$, notée ici $(g, h) \mapsto g \cdot h$, qui satisfait à :
— $\forall g, h, k \in G$, $(g \cdot h) \cdot k$ (associativité)
— $\exists e \in G$ tel que $\forall g \in G$, on a $e \cdot g = g$ et $g \cdot e = g$ (existence d'un élément neutre)
Cet élément est alors unique (exercice).
— $\forall g \in G$, $\exists h \in G$ tel que $g \cdot h = h \cdot g = e$ (existence d'un inverse pour tout élément).
L'inverse d'un élément g est unique (exercice).

Lorsque le groupe G vérifie de plus

— $\forall g, h \in G$, on a $g \cdot h = h \cdot g$ (commutativité),

on dit qu'il est *commutatif* ou encore *abélien*.

A.2 Remarque. Un groupe n'est jamais vide car il doit contenir au moins un élément, le neutre.

A.3 Remarque. L'ensemble à un seul élément $\{1\}$ (donc cet élément est noté 1 ici, mais il pourrait bien être noté autrement) admet une unique loi, et elle fait de lui un groupe. On l'appelle le groupe *trivial*.

A.4 Notation. Il est courant de ne pas noter la loi du tout lorsqu'il n'y a pas d'ambiguïté, et donc d'écrire gh au lieu de $g \cdot h$. On note également le neutre 1, et g^{-1} l'unique inverse d'un élément g. On parle alors de groupe noté *multiplicativement*. C'est la notation que nous utiliserons en général.

A.5 Notation. Au contraire, lorsque le groupe est abélien, on utilise souvent (mais pas tout le temps)

— le signe $+$ pour la loi,

— 0 pour noter le neutre,

— $-g$ pour noter l'inverse d'un élément g, et on l'appelle également *opposé*.

On parle alors de groupe noté *additivement*.

A.6 Exemple. Les permutations de l'ensemble $\{1, \dots, n\}$ (i.e. les bijections de cet ensemble dans lui-même) muni de la composition forme un groupe, noté $\mathcal{S}_n$.

L'élément neutre est la permutation identité.

L'inverse d'un élement, qui est donc une bijection, est la bijection réciproque. Pour $n \geq 3$, le groupe $\mathcal{S}_n$ n'est pas abélien.

A.7 Exemple. L'ensemble $\mathbb{Z}$ muni de l'addition des entiers comme loi est un groupe abélien (noté additivement !). Son élément neutre est 0 et l'inverse (ou encore opposé) de $n \in \mathbb{Z}$ est $-n$.

A.8 Exemple. De même que $\mathbb{Z}$, les ensembles $\mathbb{Q}$, $\mathbb{R}$ et $\mathbb{C}$ munis de l'addition forment des groupes abéliens, qu'on note additivement.

A.9 Exemple. L'ensemble $\mathbb{Q}^* = \mathbb{Q} \setminus \{0\}$ muni de la multiplication est un groupe (ce ne serait pas le cas avec $\mathbb{Q}$ tout entier).

Il est abélien, mais on ne le note pas additivement, pour ne pas confondre la loi avec l'addition qui existe sur $\mathbb{Q}$.

Il en est de même de $\mathbb{R}^*$ et $\mathbb{C}^*$.

A.10 Exemple. Soit $n \in \mathbb{N}$ avec $n \geq 1$. L'ensmble des matrices *inversibles* carrées de taille n muni de la multiplication est un groupe, noté multiplicativement.

Son élément neutre est l'identité, l'inverse d'une matrice est la matrice inverse (!). Ce groupe n'est pas abélien.

A.11 Définition (sous-groupe)**.** Un *sous-groupe* H d'un groupe G est un sous-ensemble $H \subset G$ qui vérifie

— $1 \in H$ (le neutre de G est dans H) ;

— $\forall g, h \in H$, on a $gh \in H$ (H est stable par la loi) ;

— $\forall h \in H$, on a $h^{-1} \in H$ (H est stable par passage à l'inverse) ;

A.12 Remarque. Le second point de la définition de sous-groupe permet de restreindre la loi de G en une loi sur H, et cela fait alors de H un groupe.

A.13 Exemple (sous-groupe trivial)**.** Le sous-ensemble $H = \{1\} \subset G$ qui ne contient que le neutre dans un groupe G est un sous-groupe, appelé *sous-groupe trivial*.

A.14 Exemple. À l'autre extrême, le sous-ensemble $H = G$ d'un groupe G est également un sous-groupe.

A.15 Exemple. Le sous-ensemble $\mathcal{A}_n \subset \mathcal{S}_n$ formé des permutations de signature 1 forme un sous-groupe de $\mathcal{S}_n$.

A.16 Exemple. Soit $n \in \mathbb{N}$. Le sous-ensemble $n\mathbb{Z} \subset \mathbb{Z}$ formé des multiples de n est un sous-groupe de $\mathbb{Z}$.

B Anneaux, corps

B.1 Définition (anneau)**.** Un *anneau* est un ensemble A muni de deux lois $A \times A \to A$ telles que :

— La première fait de A un groupe *abélien*. On la note généralement additivement. En particulier son neutre est noté 0. On parle de *l'addition* de A.

— La deuxième est associative. On la note généralement multiplicativement (mais attention, elle ne fait pas de A un groupe). On parle de *la multiplication* de A.

— La multiplication admet un élément neutre, noté 1. On dit parfois pour insister que l'anneau est *unitaire*.

— $\forall a, b, c \in A$, on a $a(b + c) = (ab) + (ac)$ et $(b + c)a = (ba) + (ca)$ (distributivité de la multiplication sur l'addition).

On dit qu'un anneau est *commutatif* si sa multiplication l'est (l'addition l'est déjà dans tous les cas).

B.2 Exercice. Si A est un anneau, alors $0a = 0$ et $(-1)a = -a$.

B.3 Exemple. Munis de leur addition et multiplication classiques, les ensembles $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ et $\mathbb{C}$ sont des anneaux.

B.4 Exemple. Si A est un anneau commutatif, les polynômes $A[X]$, munis de leur addition et multiplication classiques forment un anneau commutatif.

B.5 Exemple. Si A est un anneau, et si $n \in \mathbb{N}$ et $n > 0$, alors $\mathrm{M}_n(A)$, les matrices carrées de taille n à coefficients dans A, forment un anneau pour l'addition et la multiplication des matrices.
Il n'est pas commutatif sauf si $n = 1$ et que A est lui-même commutatif.

Tout comme pour un sous-groupe, un sous-anneau est un sous-ensemble stable par les lois et qui contient les éléments structurels.

B.6 Définition (sous-anneau)**.** Un *sous-anneau* d'un anneau A est un sous-ensemble $B \subset A$ tel que :

— B est un sous-groupe de A pour l'addition ;

— B contient 1 et est stable par multiplication.

B.7 Remarque. Tout comme pour un sous-groupe, cette définition implique que les lois de A se restreignent à B et en font un anneau.

B.8 Définition (corps)**.** Un *corps* est un anneau dont tous les élément sauf 0 sont inversibles pour la multiplication.

B.9 Remarque. Certains auteurs rajoutent à la définition de corps la condition que l'anneau doit être commutatif, et quand il ne l'est pas nécessairement, parlent plutôt d'*anneau à division*. Nous ne considèrerons que des corps commutatifs.

B.10 Exemple. Parmi les exemples d'anneaux ci-dessus, $\mathbb{Q}$, $\mathbb{R}$ et $\mathbb{C}$ sont des corps (commutatifs) mais $\mathbb{Z}$ n'en est pas un.

B.11 Exemple. L'anneau $\mathrm{M}_n(A)$ n'est pas un corps, sauf si $n = 1$ et que l'anneau A est lui-même un corps.

B.12 Exercice. Si A est un anneau, l'ensemble $A^\times$ constitué des éléments de A inversibles pour la multiplication, muni justement de la multiplication, forme un groupe.

Il est commutatif si A l'est.

B.13 Définition. On appelle ce groupe $A^\times$ le *groupe multiplicatif* de A, ou encore le *groupe des éléments inversibles* de A.

B.14 Remarque. L'anneau A est un corps si et seulement si $A^\times$ coïncide avec $A \setminus \{0\}$.

B.15 Exemple. Le groupe $\mathbb{Z}^\times$ des éléments inversibles de $\mathbb{Z}$ est $\{1, -1\}$.

B.16 Exemple. Si A est un anneau commutatif, le groupe des éléments inversibles de l'anneau $A[X]$ est $A^\times$ (i.e. il ne contient rien de plus que les éléments inversibles de A).

B.17 Exemple. Si l'anneau est $\mathrm{M}_n(A)$, pour $n \geq 1$, alors $(\mathrm{M}_n(A))^\times$ est appelé le groupe linéaire de taille n et est noté $\mathrm{GL}_n(A)$.