Chapitre 8

Groupes - Anneaux - Corps

Simon Dauguet
simon.dauguet@gmail.com

14 novembre 2024

Le but de ce chapitre est d'étudier la notion d'opérations. Il s'agit de comprendre ce qu'est réellement une opération sur un ensemble, puis d'identifier les propriétés que peuvent vérifier une opération et ce que cela induit comme structure sur l'ensemble sur lequel elles sont définies.

On va donc déconstruire tout ce qui a été fait depuis la petite enfance pour essayer de comprendre comment les choses fonctionnent vraiment et ne plus fonctionner par habitude. Bien entendu, on verra des monde très proche de ce qu'on a l'habitude de manipuler mais où les choses seront très différentes. Et on verra des mondes en apparences très éloignés des milieux dans lesquels on a l'habitude d'évoluer et qui, pourtant, vont se comportement de façon très similaire. Tout va dépendre des opérations définies et de leurs propriétés.

> Groups, as men, will be known by their actions.
>
> Guillermo Moreno

Table des matières

1 Lois de compositions internes **2**

2 Structure de groupe **8**
2.1 Généralités 8
2.2 Sous-groupes 16
2.3 Homomorphismes de groupe 22

3 Structure d'anneau **26**
3.1 Généralités 26
3.2 Groupes des inversibles 31
3.3 Sous-anneau 34
3.4 Homomorphismes d'anneaux 35
3.5 Structure de corps 37

1 Lois de compositions internes

Définition 1.1 (Loi de composition interne) :
Soit E un ensemble. On appelle *loi de composition interne sur* E, toute application $E \times E \to E$.

Une opération est toujours une loi de composition interne. C'est une application qui prend deux éléments d'un ensemble et qui renvoie un autre élément du même ensemble. Tout se passe en interne de E.

Exemple 1.1 :

- L'addition est une loi de composition interne sur $\mathbb{N}$, sur $\mathbb{Z}$, sur $\mathbb{Q}$, sur $\mathbb{R}$, sur $\mathbb{C}$.
- Le produit est une loi de composition interner sur $\mathbb{N}$, sur $\mathbb{Z}$, sur $\mathbb{Q}$, sur $\mathbb{R}$, sur $\mathbb{C}$.
- Dans $[0, 1[$, la loi $x * y = x + y - \lfloor x + y \rfloor$ est une LCI.
- Dans $\mathbb{R}^*$, la loi $x \diamond y = \frac{(x+y+1)^2+(x-y-1)^2}{xy}$ est une LCI.
- L'application
$$\square : \begin{array}{ccc} \mathbb{R}_+ \times \mathbb{R}_+ & \to & \mathbb{R}_+ \\ (x, y) & \mapsto & e^{x+y} - 1 \end{array}$$
est une loi de composition interne.
- La relation $x \Delta y = x^2 - y^2$ n'est pas une loi de composition interne sur $\mathbb{N}$, mais c'en est une sur $\mathbb{Z}$ (et $\mathbb{Q}$ et $\mathbb{R}$).
- La loi $a \star b = b$ définie sur $\mathbb{N}$ est une loi de composition interne.
- La composition est une LCI sur $\mathcal{F}(E, E)$ où E est un ensemble non vide quelconque.

Remarque :
Je noterais souvent les loi de composition interne sous l'abréviations LCI.

Une LCI n'est donc qu'une opération au sens le plus brut. Elle n'a, a priori, aucune propriété particulière, rien de remarquable. Ce n'est qu'une méthode, une façon de "mélanger" deux éléments entre eux. Par exemple, il n'y a aucune raison, a priori, qu'elle soit commutative (comme le dernier exemple).

Toutes les LCI ne sont pas intéressantes. Ce sont les propriétés vérifiées par une LCI qui vont permettre de donner à l'ensemble sur lequel elles sont définies une structure algébrique, une sorte de rigidité sur l'ensemble.

Définition 1.2 (Commutativité, Associativité [✓]) :
Soit E un ensemble muni d'une LCI notée $\star$. Alors :

- Si $\forall a, b \in E$, $a \star b = b \star a$, alors on dit que la LCI $\star$ est *commutative*.
- Si $\forall a, b, c \in E$, $(a \star b) \star c = a \star (b \star c)$, on dira que la LCI $\star$ est *associative*.

Remarque :
Les notions d'associativités et de commutativité sont indépendantes l'une de l'autre. Une LCI peut être associative et commutative, ou seulement associative, ou seulement commutative, ou ni l'un ni l'autre.

Exemple 1.2 :
Déterminer parmi les exemples de LCI précédents, lesquelles sont associatives ou commutatives.

Définition 1.3 (Élément neutre, Inversibilité [✓]) :
Soit E un ensemble, $\star$ une LCI sur E.

- Si $\exists e \in E$ tel que $\forall x \in E$, $x \star e = e \star x = x$, on dit que $\star$ admet *un élément neutre* et c'est e.
- Si $\star$ admet un élément neutre noté e et si $x \in E$ tel que $\exists y \in E$ tel que $x \star y = e$, alors on dit que x est inversible à droite pour $\star$ et son inverse à droite est y.
- Si $\star$ admet un élément neutre noté e et si $x \in E$ tel que $\exists z \in E$ tel que $z \star x = e$, alors on dit que x est inversible à gauche pour $\star$ et son inverse à gauche est z.
- Si $\star$ admet un élément neutre noté e et si $x \in E$ tel que $\exists u \in E$ tel que $u \star x = x \star u = e$, alors on dit que x est inversible et son inverse est u. On dit parfois que x a un inverse bilatéral.

Remarque :
On pourrait définir la notion d'élément neutre à droite et d'élément neutre à gauche. La théorie des groupes a beaucoup de raffinements. Mais l'étude complète de la théorie des groupes n'est pas au programme. Le but ici est de donner un aperçu de la théorie des groupes, suffisamment développée pour pouvoir étudier les cas simples les plus courant. Pour plus de détails, voir les années ultérieures.

Remarque :
Nous verrons au fur et à mesure de l'année des exemples de groupes avec une LCI pour laquelle, certains sont inversibles à droite, d'autre à gauche, d'autres pas du tout.

Ces notions d'inversibilité, et de semi inversibilité, sont indépendantes des propriétés algébriques de la LCI. On peut très bien avoir une LCI non commutative mais un élément neutre quand même. On peut également avoir un élément inversible à droite et à gauche, mais qui ne soit pas inversible.

Exemple 1.3 :
Toujours en reprenant les exemple de LCI donné au dessus :

- $*$ a un élément neutre qui est 0. Et tout élément a un inverse bilatère qui est $1-x$ si $x \neq 0$ et 0 si $x = 0$.
- $\diamond$ n'a pas d'élément neutre. Et donc aucun élément n'est inversible.
- $\square$ n'a pas d'élément neutre non plus.
- Δ n'a pas d'élément neutre.
- $\star$ n'a pas d'élément neutre.

Remarque :
Si E un ensemble muni d'une LCI $\star$ commutative et qui a un élément neutre noté e. Si $x \in E$, alors :

$$x \text{ est inversible à droite } \iff x \text{ est inversible à gauche } \iff x \text{ est inversible}$$

C'est évident par commutativité : si $y \in E$ est un inverse à gauche, alors $e = y \star y = y \star x$ par commutativité et donc x est inversible à droite. Et l'inverse à droite est le même que l'inverse à gauche, donc x est inversible. Et bien sûr, si x est inversible, il est en particulier inversible à gauche.

Proposition 1.1 (Unicité de l'élément neutre [✓]) :
Soit E un ensemble muni d'une LCI notée $\star$.
Si $\star$ admet un élément neutre, alors il est unique.

Démonstration :
Soit $e, e' \in E$ deux éléments neutres pour $\star$. Alors $e \star e' = e$ car e' est un élément neutre, mais on a aussi $e \star e' = e'$ car e est un élément neutre. D'où l'unicité. $\square$

Proposition 1.2 (Unicité de l'inverse (bilatère) [✓]) :
Soit E un ensemble et $\star$ une LCI associative sur E admettant un élément neutre e. Soit $x \in E$.
Si x est inversible (bilatère), alors son inverse (biltère) est unique.

Démonstration :
Soit $y, z \in E$ deux inverses de x dans E. Alors

$$\begin{aligned} y &= e \star y && \text{élément neutre} \\ &= (z \star x) \star y && \text{def } z \\ &= z \star (x \star y) && \text{associativité} \\ &= z \star e && \text{def } y \\ &= z && \text{élément neutre} \end{aligned}$$

D'où l'unicité. □

Évidemment, si un élément est inversible, son inverse bilatéral est unique également. Il suffit d'applique le cas gauche ou la cas droite.

!!! ATTENTION !!!

⚠ Attention ! Tout est très important ici. S'il n'y a pas le même élément neutre à gauche et à droite, il n'y a pas unicité de l'inverse. Si la loi n'est pas associative non plus. S'il y a le même élément neutre, mais pas forcément le même inverse à gauche et à droite, alors il n'y a pas unicité de l'inverse à gauche et à droite. Etc. Évidemment, il y a un contre-exemple pour chacun des cas possible.

Contre-exemple :
Par exemple, si on définit la loi $\star$ sur $\mathbb{N}$ par $a \star 0 = 0 \star a = a$ et $a \star b = 0$ si $a \neq 0$ et $b \neq 0$. Par définition, 0 est élément neutre pour cette loi. Mais elle n'est pas associative. Et par définition tout $b \in \mathbb{N}^*$ est l'inverse de tous les $a \in \mathbb{N}^*$. Donc un élément a une infinité d'inverse.

!!! ATTENTION !!!

⚠ Tous les éléments d'un ensemble muni d'une LCI avec un élément neutre ne sont pas forcément inversible ! Ce ne serait pas intéressant, sinon. Certains le sont, d'autres ne le sont pas.

Proposition 1.3 (Inversibilité d'un produit) :
Soit E un ensemble muni d'une LCI $\star$ associative et d'un élément neutre e pour cette loi. Soit $x, y \in E$.

Si $x \in E$ et $y \in E$ sont inversibles à gauche (resp. à droite) d'inverses respectifs x' et y', alors $x \star y$ est inversible à gauche (resp. à droite) et son inverse est $y' \star x'$.

Démonstration :
Il suffit de faire la vérification :

$$\begin{array}{lll} (x\star y)\star(y'\star x') = x\star(y\star y')\star x' & (y'\star x')\star(x\star y) = y'\star(x'\star x)\star y & \text{asso} \\ = x\star e\star x' & = y'\star e\star y & \text{def } y' \\ = x\star x' & = y'\star y & \text{asso et def } e \\ = e & = e & \text{def } x' \end{array}$$

□

Proposition 1.4 (L'inversion est une involution) :
Soit E un ensemble muni d'une LCI $\star$ associative munie d'un élément neutre e. Soit $x \in E$ inversible à gauche (resp. à droite) et y son inverse à gauche (resp. à droite).

Alors y est inversible à droite (resp. à gauche) et son inverse à droite (resp. à gauche) est x.

Démonstration :
C'est évident. Il suffit de réécrire la définition et se focaliser sur y. □

Proposition 1.5 (Égalité des inverses à droite et à gauche s'ils existent [✓]) :
Soit G un ensemble muni d'une LCI $\star$ associative qui admet un élément neutre (bilatère) noté e. Soit $x \in G$.

Si x est inversible à gauche et à droite, alors x est inversible (bilatère).

Démonstration :
Soit g l'inverse à gauche de x et d l'inverse à droite (qui sont unique puisque $\star$ est associative). Alors

$$g = g \star e = g \star (x \star d) = (g \star x) \star d = e \star d = d$$

par associativité. Et donc x admet le même inverse à gauche et à droite et donc x est inversible □

Définition 1.4 (Distributivité [✓]) :
Soit E un ensemble muni de deux LCI notées $\star$ et $\diamond$. On dit que $\diamond$ *est distributive sur* $\star$ si :

$$\forall a, b, c \in E,\ (a \star b) \diamond c = (a \diamond c) \star (b \diamond c) \qquad \text{et} \qquad a \diamond (b \star c) = (a \diamond b) \star (a \diamond c).$$

!!! ATTENTION !!!

⚠ Les lois ne sont pas forcément commutatives ! On le rappelle ! Donc bien prendre garde à la position relative des différents éléments !

Remarque :
Comme il y a deux côtés et qu'il n'y a pas de raison que les deux côtés se traitent de la même manière, on peut définir aussi des notions de distributivité à droite et de distributivité à gauche. Mais nous ne devrions pas être (trop) confronté à ce genre de situation.

Il faut garder à l'esprit en permanence, toutefois, qu'il n'y a pas de raison de supposer que ce qui est normal pour la gauche, le soit pour la droite. Il peut se passer des choses à droite qui n'ont pas cours à gauche.

Définition 1.5 (Partie stable sous l'action de la LCI) :
Soit E un ensemble muni d'une LCI $\star$. Soit $A \subset E$.
On dit que A est *stable par* $\star$ si

$$\forall a, b \in A,\ a \star b \in A.$$

Remarque :
Évidemment, pour une LCI, l'ensemble total est stable par la LCI. C'est la définition même d'une LCI. La notion d'ensemble stable par une LCI n'est vraiment intéressante que pour un sous-ensemble stricte de l'ensemble global.

Exemple 1.4 :
Pour la loi $\square$ du début de chapitre, $[1, +\infty[$ est un sous-ensemble stable par $\square$.
Pour les lois Δ et $\star$, l'ensemble des entiers pairs est un ensemble stables pour ces deux lois là.

2 Structure de groupe

2.1 Généralités

Définition 2.1 (Structure de groupe [✓]) :
Soit G un ensemble muni d'une LCI $\star$. Si :

(i) $\star$ a un élément neutre

(ii) $\star$ est associative

(iii) $\star$ est symétrisable (*i.e.* tout élément de G admet un inverse bilatère pour $\star$)

On dit alors que $(G, \star)$ est *un groupe*.

Exemple 2.1 :
Soit E un ensemble. Alors $(\mathcal{F}(E, E), \circ)$ n'est pas un groupe mais si on note Bij$(E) = \{f : E \to E$ bijective$\}$ alors $(\text{Bij}(E), \circ)$ est un groupe.

!!! ATTENTION !!!

L'inversibilité à gauche ou à droite seulement ne suffit pas pour avoir une structure de groupe. Tous les éléments doivent être inversible à gauche ET à droite et avoir le même inverse.

Contre-exemple :

Soit E un ensemble non vide. Soit $f \in \mathcal{F}(E,E)$. Montrer que f est surjective $\iff \exists g \in \mathcal{F}(E,E)$ telle que $f \circ g = \mathrm{Id}_E$. Montrer que f est injective $\iff \exists g \in \mathcal{F}(E,E)$ telle que $g \circ f = \mathrm{Id}_E$.

Remarque :
Comme la LCI d'un groupe est associative, on a des conséquences immédiates qui proviennent de l'étude des LCI :

- Les inverses à gauche et à droite sont toujours égaux
- Les inverses sont uniques
- L'élément neutre est unique

Proposition 2.1 (Groupe des bijections d'un ensemble) :
Soit E un ensemble. Si on note $\mathcal{S}(E)$ l'ensemble des bijections de E dans E (qu'on appelle aussi permutations), alors $(\mathcal{S}(E), \circ)$ est un groupe.

Démonstration :
C'est assez évident de puis le chapitre sur les ensembles et applications. Par définition d'une bijection, elle sont inversibles pour $\circ$. Donc $\circ$ est symétrique. De plus, on a élément neutre connue pour $\circ$ qui est Id_E. Et enfin, $\circ$ est associative (toujours le chapitre sur les ensembles et applications). □

Remarque :
En fait, on sait déjà tout ça. Ça a déjà été prouvé dans le chapitre sur les ensembles et applications, mais sans le dire clairement. On a montré chacune des propriétés de la définition d'un groupe. On a juste pas donné le vocabulaire.

Définition 2.2 (Groupe abélien [✓]) :
Soit $(G, \star)$ un groupe. Si la loi $\star$ est commutative, on dit que le groupe est commutatif ou qu'il est *abélien*.

Remarque :
Pour montrer qu'un ensemble est un groupe, il vaut mieux commencer par montrer que la LCI est commutative, de sorte qu'une bonne partie des choses à montrer ensuite est automatiquement vérifiée, s'il avers que la LCI est effectivement commutative. En d'autre terme, pour montrer qu'un ensemble est un groupe, on pourra commencer par :

- Montrer que la LCI est commutative
- Montrer qu'il y a un élément neutre à gauche (qui le sera automatiquement à droite par commutativité)
- Montrer que tout élément est inversible à gauche (et qui le sera aussi à droite par commutativité)
- Montrer que la loi est associative.

Exemple 2.2 :
$\mathbb{U} = \{z \in \mathbb{C},\ |z| = 1\}$ est un groupe abélien pour la multiplication complexe.

Notation (Notation additive ou multiplicative d'un groupe) :
Comme l'essentiel des groupes que nous étudierons seront des groupes de nombres (des ensembles de nombres) et que nous avons deux opérations "naturelles" sur les nombres qui sont l'addition et la multiplication, il peut être intéressant de réutiliser ces notations pour rester dans un cadre familier (et facile de notation).

La LCI sera donc souvent notée additivement $+$ ou multiplicativement $\times$.

Une convention largement répandue mais pas canonique veut que si la LCI est commutative, on la note $+$ et si elle ne l'est pas, on la note $\times$. En effet, nous verrons plus tard des produits non commutatifs (dans les matrices par exemple). Dans tous les exemples "naturels" l'addition est commutative, mais le produit n'est pas naturellement commutatif. C'est ce que réutilise cette convention.

Proposition 2.2 (Groupes de références) :
Il y a les exemples usuels de groupes de nombres additifs (pour la "vraie" addition) : $(\mathbb{Z}, +)$, $(\mathbb{Q}, +)$, $(\mathbb{R}, +)$ et $(\mathbb{C}, +)$.

Et des exemples usuels de groupes de nombres multiplicatifs (pour le "vrai" produit) : $(\mathbb{Q}^*, \times)$, $(\mathbb{R}^*, \times)$, $(\mathbb{R}_+^*, \times)$, $(\mathbb{C}^*, \times)$, $(\mathbb{U}, \times)$, $(\mathbb{U}_n, \times)$.

!!! ATTENTION !!!

⚠ Bien prendre gardes aux définition des notations ! Ce n'est pas parce qu'on note une LCI additivement, même sur un ensemble de nombres, que c'est forcément une addition. Le symbole "$+$" n'est qu'un symbole. Il ne veut rien dire en lui même. Ce n'est que la représentation d'une LCI. C'est la LCI que l'on manipule à travers le symbole et pas le symbole. Il faut donc bien garder les idées claires sur la LCI qui est représentée par ce symbole. Ce n'est pas forcément l'addition au sens usuel.

Notation :
En réutilisant les notations des opérations usuelles sur les nombres, on introduit les notations :

- Si $(G,+)$ est un groupe d'élément neutre e, on notera

$$\forall n \in \mathbb{N},\ \forall x \in G,\ nx \overset{\text{nota}}{:=} \begin{cases} \underbrace{x+x+x+\cdots+x}_{n \text{ fois}} & \text{si } n \geq 1 \\ e & \text{si } n = 0 \end{cases}$$

  De plus, l'inverse sera noté $-x$.

- Si $(G,\times)$ est un groupe d'élément neutre e, on notera

$$\forall n \in \mathbb{N},\ \forall x \in G,\ x^n \overset{\text{nota}}{:=} \begin{cases} \underbrace{x\times x\times\cdots\times x}_{n \text{ fois}} & \text{si } n \geq 1 \\ e & \text{si } n = 0 \end{cases}$$

  De plus, l'inverse sera noté x^{-1}.

Remarque :
Pour plus de commodité, j'adopterais ces conventions. Je noterais en général un groupe multiplicativement. Sauf dans le cas abélien où je le noterai additivement. Pour des besoins pédagogique, des fois, je réutiliserais une notation nouvelle pour la loi.

!!! ATTENTION !!!

⚠ En utilisant les notations additives, on a pas forcément $3 \in G$ (et en général ce ne sera pas le cas). Faire donc très attention à la façon dont on lit les notations. La notation $3x$ avec $x \in G$ n'est pas un produit. Ou plutôt, ce n'est pas un "vrai" produit. On s'autorise à écrire des choses qui n'ont pas de sens à proprement parlé, mais qui permettent de raccourcir les expressions. C'est plus agréable.

Remarque :
À l'aide d'une petite récurrence facile, il est facile d'avoir :

$$\forall n, p \in \mathbb{N},\ \forall g \in G,\ (n+p)g = ng \star pg \qquad \text{ou} \qquad g^{n+p} = g^n \star g^p$$

selon la convention de notation additive ou multiplicative adoptée.

Proposition 2.3 (Commutativité des puissances [✓]) :
Soit $(G, \star)$ un groupe et $g \in G$. Alors, si on utilise des notations multiplicative, $\forall n, p \in \mathbb{N}$, g^n et g^p commutent et

$$g^{n+p} = g^n \star g^p = g^p \star g^n$$

En utilisant les notations additives, on a

$$\forall n, p \in \mathbb{N},\ (n+p)g = ng \star pg = pg \star ng$$

Démonstration :
Ça provient de l'associativité :

$$\forall n, p \in \mathbb{N},\ g^{n+p} = \underbrace{g \star g \star \cdots \star g}_{n+p} = (\underbrace{g \star \cdots \star g}_{n}) \star (\underbrace{g \star \cdots \star g}_{p}) = g^n \star g^p$$

et en mettant les parenthèses à un autre endroit en utilisant l'associativité, on a le résultat. □

!!! ATTENTION !!!

⚠ En général

$$\underbrace{(x \star y) \star (x \star y) \star \cdots \star (x \star y)}_{n} = (x \star y)^n \neq x^n \star y^n = (\underbrace{x \star x \star \cdots \star x}_{n}) \star (\underbrace{y \star y \star \cdots \star y}_{n})$$

Contre-exemple :
Si on reprend la loi $\square$ de début de chapitre définie sur $\mathbb{R}_+$ par $x\square y = e^{x+y} - 1$. C'est une LCI sur $\mathbb{R}_+$ et

$$(x\square y)^2 = (x\square y)\square(x\square y) = (e^{x+y} - 1)\square(e^{x+y} - 1) = e^{2e^{x+y}-2} - 1$$

alors que

$$x^2\square y^2 = (e^{2x} - 1)\square(e^{2y} - 1) = e^{e^{2x}+e^{2y}-2} - 1$$

Il n'est pas alors difficile de se convaincre que ce n'est pas la même chose, en général. D'ailleurs : à quelles conditions sur $x, y \in \mathbb{R}_+$ a-t-on l'égalité ?

!!! ATTENTION !!!

Attention à bien comprendre les notations ! L'écriture "nx" ne correspond pas forcément à la définition dont vous avez l'habitude. Tout dépend des opérations (donc des LCI) sous-entendues. En particulier, il faut revenir à la définition de la multiplication par des entiers qui correspond à l'addition répétée. Ce n'est pas une multiplication !

De même, la notation "x^n" ne correspond pas forcément à une puissance. Nous avons déjà vu les différentes façons de lire cette écriture dans le chapitre sur les fonctions usuelles. Il faut ici revenir à la définition de base, c'est à dire, c'est la multiplication d'un élément par lui même répétée autant de fois que nécessaire.

!!! ATTENTION !!!

Attention en particulier à la notation $\frac{x}{y}$ qui n'a pas de sens ! Si la loi n'est pas commutative, on rappelle que $x \star y^{-1} \neq y^{-1} \star x$. Et dans ce cas, à quoi correspond $\frac{x}{y}$? La trop grande symétrie de la notation ne permet pas de pouvoir savoir dans quel sens on effectue l'opération.

On rappelle qu'en réalité, il n'y a que deux opérations dans les réels : l'addition et la multiplication. Il n'y a pas de soustraction, ni de division. C'est additionner ou multiplier par l'inverse par ces opérations. Et c'est la commutativité de la multiplication qui autorise à utiliser une nouvelle notation qui supprime l'ordre dans lequel on fait l'opération. Mais techniquement, la notation $\frac{x}{y}$ est illisible.

Proposition 2.4 (Inversibles dans un groupe [✓]) :
Soit G un groupe noté multiplicativement. Alors :

1. L'inverse est unique
2. $\forall g \in G$, $(g^{-1})^{-1} = g$ [*Involution*]
3. $\forall g, h \in G$, $(gh)^{-1} = h^{-1}g^{-1}$.
4. $\forall x \in G$, $\forall n \in \mathbb{N}$, $(x^n)^{-1} = (x^{-1})^n$. On notera $x^{-n} \overset{\text{nota}}{:=} (x^n)^{-1}$.

Démonstration :
C'est évident. Tout à été fait plus haut. Il suffit de reprendre des résultats précédents et les noter multiplicativement. Pour le dernier point, il faut saupoudrer d'une petite récurrence facile (donc à faire). □

Exemple 2.3 :
Si E est un ensemble non vide, on sait déjà que si $f, g \in \mathcal{F}(E, E)$ sont bijectives, alors $f \circ g$ est bijective et $(f \circ g)^{-1} = g^{-1} \circ f^{-1}$.

Définition-Propriété 2.3 (Ordre d'un élément) :
Soit $(G, \star)$ un groupe d'élément neutre e. Soit $g \in G$.

On appelle *ordre de* g, s'il existe, le plus petit entier $n \in \mathbb{N}^*$, noté $\omega(g)$, tel que g composé avec lui même n fois soit égal à l'élément neutre, *i.e.*

$$\omega(g) = \min\{n \in \mathbb{N}^*,\ \underbrace{g \star g \star \cdots \star g}_{n} = e\}.$$

Démonstration :
Soit $g \in G$ tel que $\exists n_0 \in \mathbb{N}$ tel que $g^{n_0} = e$. On peut alors considérer $N = \{n \in \mathbb{N}^*,\ g^n = e\}$. Alors $N \neq \emptyset$ car $n_0 \in N$.

Donc N est un sous-ensemble non vide de $\mathbb{N}$. Donc N admet un minimum car $\mathbb{N}$ est un ensemble bien ordonné. Et donc l'ordre de g existe. □

Remarque :
Le fait de prendre des entiers non nuls est crucial : par convention, $\forall g \in G$, $g^0 = e$. En autorisant 0, on aurait alors tous le temps 0 comme ordre pour tous le monde, ce qui ne serait pas tellement intéressant (non seulement il faut que ce ne soit pas tous le temps le cas pour qu'il puisse avoir un intérêt, pour ne pas dire toujours la même chose sur tous les éléments ; mais aussi parce que ça ne donnerait qu'une information triviale, ce qui n'aurait pas beaucoup d'intérêt).

Exemple 2.4 :
On considère l'ensemble $\mathbb{Z}/6\mathbb{Z} = \{\overline{0}, \overline{1}, \overline{2}, \overline{3}, \overline{4}, \overline{5}\}$ que l'on munit d'une LCI notée additivement définie par :

$+$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$
$\overline{0}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$
$\overline{1}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$	$\overline{0}$
$\overline{2}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$	$\overline{0}$	$\overline{1}$
$\overline{3}$	$\overline{3}$	$\overline{4}$	$\overline{5}$	$\overline{0}$	$\overline{1}$	$\overline{2}$
$\overline{4}$	$\overline{4}$	$\overline{5}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$
$\overline{5}$	$\overline{5}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$

Montrer que $\mathbb{Z}/6\mathbb{Z}$ est un groupe abélien muni de cette opération et déterminer l'ordre de chacun de ses éléments.

Théorème (HP) 2.5 (*Lagrange*)

Soit G un groupe fini.
Alors $\forall g \in G$, $\omega(g) | \operatorname{Card}(G)$.

Remarque :
On peut même faire une autre version : tout sous-groupe d'un groupe fini a un cardinal qui divise le cardinal du groupe.

Autrement dit, les éléments ne peuvent pas faire n'importe quoi (ni les sous-groupes). Par exemple, dans un groupe fini à 6 éléments, on ne peut trouver que des éléments d'ordre 1, 2, 3 ou 6. Mais il ne peut pas y avoir d'éléments d'ordre 5 par exemple.

De même, il n'y a pas de sous-groupe de cardinal 4.

Proposition 2.6 (Produit cartésien de groupes) :
Soit $(G, *)$ et $(H, \star)$ deux groupes.
Alors $G \times H$ est muni de la LCI naturelle (coordonnée par coordonnée) est un groupe.
Autrement dit $(G \times H, \ \cdot \ )$ est un groupe où

$$\forall (x, y), (x', y') \in G \times H, \ (x, y) \cdot (x', y') = (x * x', y \star y').$$

Démonstration :
Il suffit de le vérifier. □

Remarque :
Par une récurrence immédiate, le produit cartésien d'une nombre fini de groupes est encore un groupes, pour la LCI naturelle.

2.2 Sous-groupes

Définition 2.4 (Sous-groupe [✓]) :
Soit $(G, \star)$ un groupe d'élément neutre e et $H \subset G$.
On dit que H est un sous-groupe de G pour la loi $\star$ si :

(i) H est stable pour la LCI

(ii) $(H, \star)$ est une groupe.

Remarque :
Si $(G, \star)$ est un groupe d'élément neutre e, $\{e\}$ est toujours un sous-groupe de $(G, \star)$. De même, G lui même est toujours un sous-groupe de $(G, \star)$. Ce sont les sous-groupes triviaux de $(G, \star)$.

Proposition 2.7 (Caractérisation des sous-groupes [✓]) :
Soit $(G, \times)$ un groupe d'élément neutre e et $H \subset G$. Alors

$$H \text{ sous-groupe de } (G, \times) \iff \begin{cases} e \in H \\ \forall x, y \in H, \ xy \in H \\ \forall x \in H, \ x^{-1} \in H \end{cases}$$

Remarque :

On peut reformuler cette caractérisation de plusieurs façons :

$$H \text{ sous-groupe } (G,\times) \iff \begin{cases} H \neq \emptyset \\ \forall x,y \in H,\ xy^{-1} \in H \end{cases}$$

Et on peut aussi mélanger les propriétés sur la on vacuité avec les deux relatives à la stabilité.

Démonstration :
$\boxed{\Rightarrow}$ Soit $x \in H$. Alors $x^{-1} \in H$ car $(H,\times)$ est un groupe. Donc $e = xx^{-1} \in H$. Et bien sûr, $xy \in H$ pour tout $x,y \in H$ puisque H est un groupe.

$\boxed{\Leftarrow}$ Il suffit de vérifier la définition. La stabilité pas la LCI est donnée directement. Donc $\times$ est une LCI sur H. L'associativité de $\times$ sur H provient de la stabilité et de l'associativité de $\times$ dans G. L'élément neutre de H sera e (l'élément neutre de G) par stabilité de H par la LCI de G. Et enfin, la stabilité de H par inversion assure que tous les éléments de H sont inversible (puisqu'ils sont dans G) et que leur inverse est dans H. Donc $(H,\times)$ est un groupe. □

Exemple 2.5 (Centre d'un groupe [✓]) :
Soit $(G,\star)$ un groupe. On note

$$Z(G) = \{x \in G,\ \forall y \in G,\ x \star y = y \star x\}$$

$Z(G)$ s'appelle le centre de G. Montrer que $Z(G)$ est un sous-groupe de G.

Exemple 2.6 :
Soit $n \in \mathbb{N}^*$. Montrer que $\mathbb{U}_n$ est un sous-groupe de $(\mathbb{U},\times)$.

Remarque :
G et $\{e\}$ sont automatiquement des sous-groupe de G. Ce sont les sous-groupes triviaux de G.

Proposition 2.8 (Intersections de sous-groupes [✓]) :
Soit $(G,\star)$ un groupe d'élément neutre e et H_1, H_2 deux sous-groupes de G.
Alors $H_1 \cap H_2$ est un sous-groupe de G.

Plus généralement, toute intersection quelconque de sous-groupe est un sous-groupe.

Démonstration :
Soit I un ensemble et $\forall i \in I$, H_i un sous-groupe de G. Alors $\bigcap_{i\in I} H_i \subset G$.

On sait que $\forall i \in I$, $e \in H_i$. Donc, par définition, $e \in \bigcap_{i\in I} H_i$.

De plus, si $x, y \in \bigcap_{i\in I} H_i$, alors, par définition, $\forall i \in I$, $x, y \in H_i$. Par stabilité d'un sous-groupe par la LCI, on a donc $\forall i \in I$, $x \star y \in H_i$. Et donc $x \star y \in \bigcap_{i\in I} H_i$. Donc $\bigcap_{i\in I} H_i$ est stable par la LCI.

Soit $x \in \bigcap_{i\in I} H_i$. Alors $\forall i \in I$, $x \in H_i$. Et donc, par stabilité par inversion, si on note z l'inverse de x dans G, alors $\forall i \in I$, $z \in H_i$. Et donc $\bigcap_{i\in I} H_i$ est stable par inversion.

Donc par caractérisation des sous-groupes, $\bigcap_{i\in I} H_i$ est un sous-groupe de G. □

Exemple 2.7 :
Soit $(G, \times)$ un groupe et H_1, H_2 deux sous-groupes de G. Montrer que

$$H_1 \cup H_2 \text{ sous-groupe } G \iff H_1 \subset H_2 \text{ ou } H_2 \subset H_1$$

Définition 2.5 (Composée de deux sous-groupes, d'un élément par un sous-groupe [✓]) :
Soit $(G, \star)$ un groupe et H, K deux sous-groupes de G et $g \in G$.

On note alors par $H \star K$ l'ensemble de tous les composés fait à partir d'un élément de H et d'un élément de K, *i.e.* :

$$H \star K = \{h \star k,\ (h, k) \in H \times K\}$$

On note aussi $g \star H$ l'ensemble composé de tous les éléments de H composé par g à gauche, *i.e.* :

$$g \star H = \{g \star h,\ h \in H\}.$$

Par extension, on peut définir $H \star g$ et $g \star H \star k$.

Proposition 2.9 (Caractérisation des sous-groupes de $(\mathbb{Z}, +)$ [✓]) :
Soit $H \subset \mathbb{Z}$.

H est un sous-groupe de $(\mathbb{Z}, +)$ si, et seulement si, $\exists n \in \mathbb{N}$ tel que $H = n\mathbb{Z}$, où $n\mathbb{Z} = \{np,\ p \in \mathbb{Z}\}$ est l'ensemble des multiples de n.

Démonstration :
D'abord,il est facile de vérifier que les $n\mathbb{Z}$ sont bien des sous-groupes de $(\mathbb{Z}, +)$.

Réciproquement, soit H est un sous-groupe de $(\mathbb{Z},+)$. Si $H=\{0\}$, alors $H=0\mathbb{Z}$. Supposons désormais $H\neq\{0\}$. On note alors $H_+=H\cap\mathbb{N}^*$. C'est un sous-ensemble de $\mathbb{N}$. Il admet donc un minimum. On note $n=\min H_+$. Alors, par stabilité de H par la LCI, il est facile de montrer que $n\mathbb{Z}\subset H$. Soit maintenant $x\in H$. Alors, par division euclidienne, $\exists!(q,r)\in\mathbb{Z}\times\{0,\dots,n-1\}$ tel que $x=nq+r$. Mais $nq\in H$ car $n\in H$ et H stable par addition. Donc $r=x-nq\in H$ car H sous-groupe de $(\mathbb{Z},+)$. Si $r\neq 0$, alors $r\in H_+$ et $r<n=\min H_+$. Donc ☠. Donc $r=0$. Et donc $x=nq\in n\mathbb{Z}$. D'où $H=n\mathbb{Z}$. □

Exemple 2.8 :
Déterminer $2\mathbb{Z}\cap 3\mathbb{Z}$ et $6\mathbb{Z}\cap 9\mathbb{Z}$.

Proposition 2.10 (Caractérisation des sous-groupes de $(\mathbb{R},+)$ [✓]) :
Soit H un sous-groupe de $(\mathbb{R},+)$. Alors :

(i) Soit $\exists a\geq 0$ tel que $H=a\mathbb{Z}$

(i) Soit H est dense dans $\mathbb{R}$.

Démonstration :
Si $H=\{0\}$, évidemment, $H=0\mathbb{Z}$. Supposons désormais $H\neq\{0\}$. Donc $\exists x\neq 0$, $x\in H$. Alors $-x\in H$. Donc $H\cap\mathbb{R}_+^*\neq\emptyset$. Donc, par propriété de la borne inf de $\mathbb{R}$, $a=\inf H\cap\mathbb{R}_+^*$ existe.

Supposons $a>0$. Par caractérisation séquentielle de la borne inf, $\exists(x_n)_{n\in\mathbb{N}}\in H^{\mathbb{N}}$ telle que

$$x_n \xrightarrow[n\to+\infty]{} a.$$

Par définition de la limite, $\exists n_0\in\mathbb{N}$, telle que $\forall n\geq n_0$, $a\leq x_n\leq\frac{3}{2}a$. Soit $n,m\geq n_0$. Alors $-a/2\leq x_n-x_m\leq a/2$. Si $x_n-x_m\leq 0$, on peut utiliser $x_m-x_n\in[-a/2,a/2]$. Et donc, sans perte de généralités, on peut suppose $0\leq x_n-x_m\leq a/2$. De plus, $x_n,x_m\in H$ et H sous-groupes de $(\mathbb{R},+)$, donc $x_n-x_m\in H$. Or $a/2<a=\inf H\cap\mathbb{R}_+^*$. Donc, si $x_n-x_m\neq 0$, on a ☠. Donc $x_n=x_m$. Et donc la suite $(x_n)_{n\in\mathbb{N}}$ est stationnaire.

Or $(x_n)_{n\in\mathbb{N}}$ converge vers a. Donc, par unicité de la limite, $\exists n_0\in\mathbb{N}$, $\forall n\geq n_0$, $x_n=a$. Or $(x_n)\in H^{\mathbb{N}}$. Donc $a\in H$.

On a alors immédiatement, $a\mathbb{Z}\subset H$.

Inversement, si $x\in H$, on pose $n=\lfloor x/a\rfloor$. Alors $na\leq x<(n+1)a$. Et donc $0\leq x-na<a$ et $x-na\in H$. Puis, par définition de la borne inf, on en déduit $x=na$. Donc $H\subset a\mathbb{Z}$.

Supposons maintenant que $a=0$. Soit $\alpha,\beta\in\mathbb{R}$ avec $\alpha<\beta$. Alors, $\exists x_0\in H$ tel que $0<x_0<\beta-\alpha$ par caractérisation de la borne inf. En particulier, $\alpha<x_0+\alpha<\beta$.

Notons $A = \{k \in \mathbb{N}^*,\ kx_0 > \alpha\}$. Alors A est non vide (car $kx_0 \xrightarrow[k\to+\infty]{} +\infty$) et minorée par 1. Donc $\gamma = \min A$ existe. Et donc, par définition du minimum, $\gamma - 1 \notin A$. Donc $\gamma x_0 > \alpha$ et $(\gamma - 1)x_0 \leq a$. Et donc $\alpha < \gamma x_0 \leq \gamma x_0 + \alpha < \beta$. Donc $\gamma x_0 \in]a, b[$.

De plus, H étant un sous-groupe de $(\mathbb{R}, +)$ et $x_0 \in H$, donc $\gamma x_0 \in H$ car $\gamma \in \mathbb{N}^*$. Et donc H est dense dans $\mathbb{R}$. □

Exemple 2.9 :
Montrer que $H = \{\ln(r),\ r \in \mathbb{Q}_+^*\}$ est dense dans $\mathbb{R}$.

Définition-Propriété 2.6 (Sous-groupe engendré par une partie) :
Soit $(G, \star)$ un groupe. Soit $A \subset G$.

Alors $\exists!\, \mathrm{Gr}(A) \subset G$ sous-groupe de G tel que

$$\begin{cases} A \subset \mathrm{Gr}(A) \\ \forall H \subset G \text{ sous-groupe},\ A \subset H \implies \mathrm{Gr}(A) \subset H \end{cases}$$

De plus,

$$\mathrm{Gr}(A) = \bigcap_{\substack{H \text{ ss-grp } G \\ A \subset H}} H$$

$\mathrm{Gr}(A)$ est appelé le *sous-groupe engendré par* A. Donc $\mathrm{Gr}(A)$ est le plus petit sous-groupe de G, au sens de l'inclusion, contenant A.

Démonstration :
On considère $\mathcal{G}(A) = \{H \subset G,\ \text{t.q. } A \subset H,\ H \text{ sous-groupe } G\}$. Alors $\mathcal{G}(A)$ est non vide car $G \subset \mathcal{G}(A)$. Alors $\mathrm{Gr}(A) = \bigcap_{H \in \mathcal{G}(A)} H$ est un sous-groupe de G. Et par définition, $A \subset \mathrm{Gr}(A)$.

Soit H un sous-groupe de G contenant A. Alors par définition, $H \in \mathcal{G}(A)$. Donc $\mathrm{Gr}(A) \subset H$. Donc $\mathrm{Gr}(A)$ est bien minimum au sens de l'inclusion.

Soit H_A sous-groupe de G tel que $A \subset H_A$ et $\forall H \subset G$ sous-groupe, si $A \subset H$, alors $H_A \subset H$. Alors $\mathrm{Gr}(A)$ est un sous-groupe de G contenant A, donc par définition de H_A, on a $\mathrm{Gr}(A) \subset H_A$. Mais $\mathrm{Gr}(A)$ vérifie aussi cette propriété et H_A est un sous-groupe de G contenant A, donc $H_A \subset \mathrm{Gr}(A)$. D'où l'unicité. □

Remarque :
Évidemment, $A \subset \mathrm{Gr}(A)$.

On pourrait développer en détaillant ce qu'est le groupe engendré par une intersection, par une réunion etc.

Proposition 2.11 (Groupe engendré par un sous-groupe) :
Soit $(G, \star)$ un groupe. Soit $H \subset G$.
Alors

$$H \text{ sous-groupe de } G \iff \mathrm{Gr}(H) = H.$$

Démonstration :
C'est naturel et assez évident. Le sens indirecte est triviale. On sait déjà que $H \subset \mathrm{Gr}(H)$. De plus $H \in \mathcal{G}(H) = \{K \subset G,\ K \text{ sous-groupe } G,\ H \subset K\}$. Donc, par définition

$$\mathrm{Gr}(H) = \bigcap_{K \in \mathcal{G}(H)} K \subset H.$$

D'où l'égalité. □

Exemple 2.10 :
Dans $\mathbb{Z}$, $\mathrm{Gr}(1) = \mathbb{Z}$, $\mathrm{Gr}(2) = 2\mathbb{Z}$, $\mathrm{Gr}(2,3) = \mathbb{Z}$, $\mathrm{Gr}(2,4) = 2\mathbb{Z}$ et $\mathrm{Gr}(6,9) = 3\mathbb{Z}$.

Définition 2.7 (Groupe monogène) :
Soit $(G, *)$ un groupe.
On dit que G est monogène si il existe $g \in G$ tel que $\mathrm{Gr}(g) = G$, *i.e.* si G est engendré par un seul élément (bien choisi). L'élément g s'appelle alors *élément générateur de* G.

Remarque :
Dans un groupe monogène, tous les éléments peuvent donc être exprimé à partir d'un seul élément.

Exemple 2.11 :
$\mathbb{Z}$ est monogène car $\mathbb{Z} = \mathrm{Gr}(1)$. Et donc $2 = 1 + 1$, $3 = 1 + 1 + 1$ etc.

2.3 Homomorphismes de groupe

Un homomorphisme de groupe est en fait une "bonne application" entre groupes. C'est une application entre deux groupes qui sera compatible avec la structure de groupe.

Définition 2.8 (Homomorphisme de groupe) :
Soit $(G, *)$ et $(H, \star)$ deux groupes. Soit $f : G \to H$.
f est un *homomorphisme de groupe* si :

$$\forall g, g' \in G,\ f(g * g') = f(g) \star f(g')$$

On dit aussi que f est un morphisme de groupe.

Remarque :
Étymologiquement, *homomorphisme* vient du grec *morphos* et *homo*, qui peut se traduire littéralement par : même structure, au sens où elles se ressemblent. D'une façon générale, un homomorphisme est une application entre deux structure algébrique qui va conserver la structure en question. Nous verrons plusieurs structure algébrique et donc, plusieurs type d'homomorphisme.

Exemple 2.12 :
L'exponentielle est un morphisme de $(\mathbb{R}, +)$ dans $(\mathbb{R}_+^*, \times)$. L'exponentielle est également un morphisme de $(\mathbb{C}, +)$ dans $(\mathbb{C}^*, \times)$.

Proposition 2.12 (Image de l'élément neutre et d'un inverse par un morphisme de groupe) :
Soit $(G, *)$ et $(G', \star)$ deux groupes et $f : G \to G'$ un homomorphisme de groupe.
Alors :
(i) $f(e_G) = e_{G'}$
(ii) $\forall g \in G,\ f(g^{-1}) = f(g)^{-1}$.

Démonstration :
On $f(e_G) = f(e_g * e_G) = f(e_G) \star f(e_G)$. Et par structure de groupe $e_{G'} = f(e_G) \star f(e_G)^{-1} = f(e_G)$.
Puis $\forall g \in G$, $e_{G'} = f(e_G) = f(g * g^{-1}) = f(g) \star f(g^{-1})$. Et par unicité de l'inverse, $f(g^{-1}) = f(g)^{-1}$. □

Attention ! L'inversibilité ne se fait pas dans le même groupe, donc ne se fait pas par rapport à la même LCI et donc n'a pas le même sens !

Exemple 2.13 ([✓]) :
Le but de cet exercice est de montrer que les seuls morphismes de groupes de $(\mathbb{Q},+)$ dans lui-même sont les homothéties.

Soit $f : (\mathbb{Q},+) \to (\mathbb{Q},+)$ un morphisme de groupe.

1. Montrer que $\forall n \in \mathbb{N}$, $f(n) = nf(1)$.
2. En déduire que $\forall n \in \mathbb{Z}$, $f(n) = nf(1)$.
3. Montrer que $\forall p \in \mathbb{N}^*$, $f(1/p) = f(1)/p$.
4. En déduire que $\forall r \in \mathbb{Q}$, $f(r) = rf(1)$.
5. Conclure.
6. Déterminer les morphismes de $(\mathbb{Q},+) \to (\mathbb{Q}^*,\times)$ et $(\mathbb{Q},+) \to (\mathbb{Z},+)$.

Proposition 2.13 (Composée de morphismes de groupes) :
Soit $(G,*),(H,\star),(K,\ \cdot\ )$ trois groupes et $f : G \to H$ et $g : H \to K$ deux morphismes de groupes.

Alors $g \circ f : G \to K$ est un morphisme de groupe.

Démonstration :
Il suffit de l'écrire : si $x, x' \in G$, alors $(g \circ f)(x * x') = g(f(x) \star f(x')) = g(f(x)) \cdot g(f(x')) = (g \circ f)(x) \cdot (g \circ f)(x')$. □

Remarque :
On pourra recoller donc ici et utiliser tous ce que l'on sait sur les composées d'applications.

Proposition 2.14 (Image directe et réciproque d'un sous-groupe) :
Soit $(G,*)$ et $(H,\star)$ deux groupes et $f : G \to H$ un homomorphisme de groupe. Alors :

1. $\forall G' \subset G$, si G' est un sous-groupe de G, alors $f(G')$ est un sous-groupe de H.
2. $\forall H' \subset H$, si H' est un sous-groupe de H, alors $f^{-1}(H')$ est un sous-groupe de G.

Démonstration :
Il suffit de faire les vérification.

Dans le cas de H' sous-groupe de H, on a $f(e_G) = e_H$ donc $e_G \in f^{-1}(\{e_H\}) \subset f^{-1}(H')$. Et si $g, g' \in f^{-1}(H')$, alors $f(g * g') = f(g) \star f(g') \in H'$ car f est un morphisme de groupe et H' un sous-groupe de H'. Donc $g * g' \in f^{-1}(H')$ par définition de l'image réciproque. De plus, si $g \in f^{-1}(H')$, alors $f(g) \in H'$ et donc $f(g)^{-1} = f(g^{-1}) \in H'$ car H' sous-groupe. Et donc $g^{-1} \in f^{-1}(H')$. Donc $f^{-1}(H')$ sous-groupe de G. □

Exemple 2.14 :
L'application $f : \mathbb{C}^* \to \mathbb{C}^*$ définie par $f(z) = z^n$ est un homomorphisme de groupe de $(\mathbb{C}^*, \times)$ et $U_n = f^{-1}(\{1\})$. Donc $(U_n, \times)$ est un sous-groupe de $\mathbb{C}^*$.

Définition 2.9 (Image et noyau d'un morphisme) :
Soit $(G, *)$ et $(H, \star)$ deux groupes et $f : G \to H$ un homomorphisme de groupe.

On définit *le noyau de* f, noté $\ker(f)$ comme l'ensemble des antécédents de l'élément neutre de H par f, *i.e.*

$$\ker(f) = \{g \in G,\ f(g) = e_H\}.$$

On définit *l'image de* f, noté $\mathrm{Im}(f)$, comme l'ensemble des images de f, *i.e.*

$$\mathrm{Im}(f) = f(G) = \{f(g),\ g \in G\}.$$

Proposition 2.15 (Structure de $\mathrm{Im}(f)$ et $\ker(f)$) :
Soit $(G, *)$ et $(H, \star)$ deux groupes et $f : G \to H$ un morphisme de groupes.
Alors $\ker(f)$ et $\mathrm{Im}(g)$ sont des groupes (respectivement des sous-groupes de G et de H).

Démonstration :
C'est évident, puis que $\ker(f) = f^{-1}(\{e_H\})$ et $\mathrm{Im}(f) = f(G)$ et $\{e_H\}$ est un sous-groupe (trivial) de H. □

Exemple 2.15 :
Soit $(G, *)$ et $(G', \star)$ deux groupes et $f : G \to G'$ un morphisme de groupes.

1. Montrer que si H est un sous-groupe de G, alors $f^{-1}(f(H)) = H * \ker(f)$.

2. Montrer que si H' est un sous-groupe de G', alors $f(f^{-1}(H')) = H' \cap \mathrm{Im}(f)$.

Proposition 2.16 (Caractérisation de l'injectivité et surjectivité par noyau et image) :
Soit $(G, *)$ et $(H, \star)$ deux groupes et $f : G \to H$ un morphisme de groupe.

(i) f injective $\iff \ker(f) = \{e_G\}$

(ii) f surjective $\iff \mathrm{Im}(f) = H$.

Démonstration :
Le second point est évident.

Supposons f injective. Soit $g \in \ker(f)$. Alors $f(g) = e_H = f(e_G)$. Et par injectivité, $g = e_G$. Or $e_G \in \ker(f)$. Donc $\ker(f) = \{e_G\}$.

Inversement, si $\ker(f) = \{e_G\}$. Soit $g, g' \in G$ tels que $f(g) = f(g')$. Alors, $f(g)^{-1} \star f(g') = e_H$ et donc $f(g^{-1}) \star f(g') = e_H$. Puis, $f(g^{-1} * g') = e_H$ par morphisme. Et donc, par définition du noyau, $g^{-1} * g' \in \ker(f) = \{e_G\}$. Donc $g^{-1} * g' = e_G$ et donc $g' = g$ (par unicité de l'inverse, par exemple, ou par le calcul simplement). □

Définition 2.10 (Isomorphisme de groupe, Automorphisme, Groupes isomorphes) :
Soit $(G, *)$ et $(H, \star)$ deux groupes et $f : G \to H$.

- Si f est un homomorphisme de groupe bijectif, alors on dit que f est un *isomorphisme de groupe*.
- Si $f : G \to G$ est un isomorphisme de groupes, on dit que f est un *automorphisme* du groupe G.
- Les groupes G et H sont dit *isomorphes* s'il existe un isomorphisme de groupe $f : G \to H$.

Remarque :
Étymologiquement, *isomorphisme* vient du grec *iso* et *morphos* et qui peut donc se traduire par "même forme", au sens où ce sont exactement les mêmes.

Proposition 2.17 (Réciproque d'un isomorphisme de groupe) :
Soit $(G, *)$ et $(H, \star)$ deux groupes et $f : G \to H$ un isomorphisme de groupe.

Alors f^{-1} est aussi un isomorphisme de groupe.

Démonstration :
Soit $g, g' \in G$ et $h, h' \in H$ tels que $f(g) = h$ et $f(g') = h'$. Alors $f^{-1}(h \star h') = f^{-1}(f(g) \star f(g')) = f^{-1}(f(g * g')) = g * g' = f^{-1}(h) * f^{-1}(h')$. Et donc f^{-1} est bien un homomorphisme de groupe. □

Les groupes sont particulièrement utiles pour les faire agir sur un ensemble. Voir la citation en début de chapitre.

Définition (HP) 2.11 (*Action de groupe*)

Soit E un ensemble et $(G, \star)$ un groupe.
On dit que G agit sur E si il existe $f : G \to \mathcal{S}(E)$ un homomorphisme du groupe $(G, \star)$ dans $(\mathcal{S}(E), \circ)$. Et dans ce cas, les éléments de G agissent sur les éléments de E par :

$$\forall (g, x) \in G \times E,\ g \cdot x = (f(g))(x).$$

Les actions de groupes est un intérêt, pour ne pas dire l'intérêt fondamental, des groupes.
On peut alors définir l'orbite d'un élément $x \in E$ sous l'action de G, qui consiste en tous les transformés de x sous l'action de G. Et inversement, on peut fixer un g et regarder en quoi il va transformer l'ensemble E.
Il faut également distinguer l'action de groupe à gauche ou à droite.
Il y a beaucoup de choses à faire sur les actions de groupes.

3 Structure d'anneau

3.1 Généralités

Définition 3.1 (Structure d'anneau [✓]) :
Soit A un ensemble muni de deux LCI notées respectivement $+$ et $\star$. On dit que $(A, +, \star)$ *est un anneau* si :

(i) $(A, +)$ est un groupe abélien dont l'élément neutre est noté 0_A (ou 0)
(ii) $\star$ a un élément neutre, noté 1_A (ou 1)
(iii) $\star$ est associative
(iv) $\star$ est distributive sur $+$

De plus, on dira que l'anneau $(A, +, \star)$ est commutatif si
(v) $\star$ est commutative

Remarque :
La présence d'un élément neutre pour la seconde LCI n'est pas obligatoire dans un anneau. Il est possible que vous trouviez dans la littérature la précision "anneau unitaire" ou (plus rarement) "anneau unifère". L'ajout de cet adjectif est pour préciser que l'on considère un anneau dans lequel, la seconde LCI a un élément neutre.

Notation :
En général, pour correspondre aux ensembles de nombres et aux notations usuelles des opérations de bases, on note un anneau $(A, +, \cdot)$ avec la seconde loi notée multiplicativement. On parle souvent de l'addition pour la loi de groupe et de la multiplication pour la seconde LCI. ATTENTION ! En toute généralités, ce sont des abus de langages ! Ce ne sont pas forcément des additions, ni des multiplications. C'est un choix de notation pour correspondre à la situation qu'on a l'habitude de côtoyer.

Exemple 3.1 :
$(\mathbb{Z}, +, \cdot)$, $(\mathbb{Q}, +, \cdot)$, $(\mathbb{R}, +, \cdot)$ et $(\mathbb{C}, +, \cdot)$ dont des exemples classiques d'anneau. Mais $(\mathbb{R}^{\mathbb{N}}, +, \times)$ avec la définitions usuelles des opérations entre suites est aussi un anneau.

Si E est un ensemble, $(\mathcal{F}(E, \mathbb{R}), +, \times)$ est un anneau. Plus généralement, si E est un ensemble et A un anneau, $(\mathcal{F}(E, A), +, \times)$ est un anneau.

Et $(\mathcal{F}(E, E), +, \circ)$ est aussi un anneau.

Remarque :
Un singleton est toujours anneau. Il suffit de définir deux LCI. Donc si a est un élément d'un ensemble quelconque, alors on peut définir $\star$ sur $\{a\}$ par $a \star a = a$ et on peut définir une autre LCI $\odot$ sur $\{a\}$ par $a \odot a = a$. Alors $\star$ admet un élément neutre qui est a, a a un inverse qui est lui-même, $\star$ est associative et elle est évidemment commutative. Donc $(\{a\}, \star)$ est un groupe abélien. De plus, $\odot$ est évidemment associative pour la même raison, elle a un élément neutre qui est a et elle est distributive sur $\star$. Donc $(\{a\}, \star, \odot)$ est un anneau.

Mais ce n'est pas très intéressant.

Proposition 3.1 (Règles de calculs dans un anneau [✓]) :
Soit $(A, +, \times)$ un anneau, $a, b \in A$ et $n \in \mathbb{Z}$. Alors :

(i) $a \times 0_A = 0_A \times a = 0_A$ [0 *est absorbant*]

(ii) $-(ab) = (-a)b = a(-b)$, en particulier, $-a = (-1_A) \times a = a \times (-1_A)$.

(iii) $n(ab) = (na)b = a(nb)$

(iv) $(-a)(-b) = ab$ et en particulier, $(-1_A)^2 = 1_A$.

(v) Si a et b commutent, alors $\forall p \in \mathbb{N}$, $(ab)^p = a^p b^p$.

Démonstration :

(i) Il y a une astuce :

$$\begin{aligned} a \times 0 &= a \times (0+0) && \text{élément neutre pour } + \\ &= a \times 0 + a \times 0 && \text{distributivité} \end{aligned}$$

En utilisant le symétrique de $a \times 0$ pour $+$, on a $0 = a \times 0$.

(ii) Il suffit de faire la vérification avec l'unicité du symétrique :

$$\begin{aligned} ab + (-a)b &= (a + (-a))b && \text{distributivité} \\ &= 0 \times b && \text{def symétrique} \\ &= 0 && \text{cf (i)} \end{aligned}$$

Donc $(-a)b$ est le symétrique de ab pour $+$, or c'est $-(ab)$ par définition de la notation, donc, par unicité, $-(ab) = (-a)b$. De même pour le dernier.

(iii) On va faire une récurrence. C'évident pour $n = 0$ et $n = 1$. Supposons que ce soit vraie pour un entier $n \in \mathbb{N}$. Alors

$$\begin{aligned} (n+1)(ab) &= \underbrace{(ab) + (ab) + \cdots + (ab)}_{n+1} && \text{def notation} \\ &= n(ab) + ab && \text{asso et nota} \\ &= (na)b + ab && \text{HR} \\ &= ((na) + a)b && \text{distri} \\ &= ((n+1)a)b && \text{asso} \end{aligned}$$

De même pour l'autre.

Pour le cas où $n \leq 0$, il suffit de multiplier par -1 et utiliser ce qui précède pour se ramener au cas $n \geq 0$ et conclure.

(iv) On utilise aussi le symétrique pour l'addition :

$$\begin{aligned} (-a)(-b) - ab &= (-a)(-b) + (-a)b && \text{cf (ii)} \\ &= (-a)((-b) + b) && \text{distributivité} \\ &= (-a) \times 0 && \text{def symétrique} \\ &= 0 && \text{cf (i)} \end{aligned}$$

Donc $(-a)(-b)$ est le symétrique de $-ab$ pour $+$. Par unicité du symétrique, on en déduit $(-a)(-b) = ab$.

(v) Il suffit de faire une récurrence sur p.

□

!!! ATTENTION !!!

⚠ Ne pas confondre les opérations et les notations de ses opérations. Par exemple, en écrivant $-a = (-1) \times a$, il n'y a rien de trivial là dedans. $-a$ est le symétrique de a pour la loi $+$, -1_A est le symétrique de 1_A (qui n'est pas le $1 \in \mathbb{R}$) pour la loi $+$. Il n'est pas dit que le produit du symétrique de 1_A pour $+$ par a donne le symétrique de a pour $+$, a priori.

On rappelle que A n'est pas forcément un ensemble de nombres. Donc il n'y a pas forcément d'entier dedans. Et donc na n'est pas une multiplication, au sens des LCI de A. C'est une notation condensée pour parler de plusieurs addition (de a) successives.

Proposition 3.2 (Distinction des deux éléments neutres) :
Soit $(A, +, \times)$ un anneau. Si $A \neq \{0_A\}$, alors $0_A \neq 1_A$.

Démonstration :
Comme $A \neq \{0_A\}$, alors $\exists a \in A$ tel que $a \neq 0_A$. Supposons $0_A = 1_A$. Alors

$$\begin{aligned} a &= a \times 1_A && \text{élément neutre pour } \times \\ &= a \times 0_A && \text{hyp} \\ &= 0_A && \text{car } 0_A \text{ absorbant} \end{aligned}$$

Et donc ☠. □

Remarque :
Cette proposition n'est pas triviale. On avait parlé de deux éléments neutres qui étaient définies à partir de propriétés. A aucun moment on a imposé que les deux éléments neutres devaient être distincts. En fait, si A n'est pas trivial, c'est automatique. Mais ce n'est pas trivial a priori.

Proposition 3.3 (Binôme de Newton [✓]) :
Soit $(A, +, \times)$ un anneau et $a, b \in A$.
Si a et b ***commutent*** (*i.e.* si $ab = ba$), alors on a la formule du binôme de Newton :

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

Démonstration :
Voir la démo faite précédemment dans le chapitre sur le calcul algébrique. C'est le principe. Il faut simplement prendre plus de gants sur la nature des opérations qu'on utilise et leurs propriétés. □

Proposition 3.4 (Factorisation classique) :
Soit $(A, +, \times)$ un anneau et $a, b \in A$.
Si a et b commutent, alors

$$\forall n, p \in \mathbb{N},\ ab^n = b^n a \qquad \text{et} \qquad a^n b^p = b^p a^n$$

et donc aussi

$$\forall n \in \mathbb{N}^*,\ a^n - b^n = (a-b)\sum_{k=0}^{n-1} a^k b^{n-k-1}.$$

Démonstration :
On sait déjà $ab = ba$ et $ab^0 = b^0 a$. Si $\exists n \in \mathbb{N}$ tel que $ab^n = b^n a$, alors $ab^{n+1} = ab^n b = b^n ab = b^n ba = b^{n+1}a$ par associativité de $\times$ et commutativité de a et b. Et par principe de récurrence, on a ce qu'on veut.

Pour la deuxième, on refait une récurrence sur p. On sait déjà que $\forall n \in \mathbb{N}$, $ab^n = b^n a$ et $a^0 b^n = b^n a^0$. Si $\exists p \in \mathbb{N}$ tel que $\forall n \in \mathbb{N}$, $a^p b^n = b^n a^p$, alors $\forall n \in \mathbb{N}$, $a^{p+1}b^n = aa^p b^n = ab^n a^p = b^n aa^p = b^n a^{p+1}$. Et d'où le résultat par principe de récurrence.

Et enfin, pour la dernière, ce n'est qu'une vérification directe :

$$\begin{aligned}
\forall n \in \mathbb{N},\ (a-b)\sum_{k=0}^{n-1} a^k b^{n-k-1} &= a\sum_{k=0}^{n-1} a^k b^{n-k-1} - b\sum_{k=0}^{n-1} a^k b^{n-k-1} && \text{distributivité}\\
&= \sum_{k=0}^{n-1} a^{k+1} b^{n-k-1} - \sum_{k=0}^{n-1} ba^k b^{n-k-1} && \text{distributivité}\\
&= \sum_{k=1}^{n} a^k b^{n-k} - \sum_{k=0}^{n-1} a^k b^{n-k} && \text{commutativité}\\
&= \sum_{k=1}^{n} a^k b^{n-k} - \sum_{k=0}^{n-1} a^k b^{n-k} &&\\
&= a^n - b^n && \text{commutativité, associativité de } +
\end{aligned}$$

□

Définition 3.2 (Anneau intègre [✓]) :
Soit $(A, +, \times)$ un anneau. On dit que A est un *anneau intègre* si

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

Autrement dit, un anneau intègre est un anneau dans lequel il n'y a pas de diviseurs (non triviaux) de 0.

Là non plus, ce n'est pas trivial.

Remarque :
On peut utiliser la contraposée :

$$(A, +, \times) \text{ intègre} \iff \Big(\forall a, b \in A,\ a \neq 0_A,\ b \neq 0_A \implies ab \neq 0_A\Big).$$

!!! ATTENTION !!!

⚠ Dans un anneau non intègre $ab = ac$ n'entraîne pas $b = c$! ! On rappelle que tous les éléments ne sont pas inversibles pour la multiplication. En particulier, a ne l'est peut être pas. On ne peut donc pas "simplifier" par a (qui veut en réalité dire multiplier par l'inverse de a à gauche, mais il faut qu'il existe pour ça). Ici, on a, en utilisant le symétrique pour l'addition et la distributivité $a(b - c) = 0$. Mais si A n'est pas intègre, même si $a \neq 0$, on ne peut pas en déduire que $b = c$.

Exemple 3.2 :
On considère l'anneau $(\mathcal{F}(\mathbb{R}, \mathbb{R}), +, \times)$ pour les opérations usuelles entre fonctions. Soit $A \subsetneq \mathbb{R}$ non vide. Alors $\mathbb{1}_A \in \mathcal{F}(\mathbb{R}, \mathbb{R})$ et $\mathbb{1}_{\overline{A}} \in \mathcal{F}(\mathbb{R}, \mathbb{R})$. Et $\mathbb{1}_A \times \mathbb{1}_{\overline{A}} = 0_{\mathcal{F}(\mathbb{R},\mathbb{R})}$ mais $\mathbb{1}_A \neq 0$ et $\mathbb{1}_{\overline{A}} \neq 0$. Donc $(\mathcal{F}(\mathbb{R}, \mathbb{R}), +, \times)$ n'est pas intègre.

En particulier, on a $\mathbb{1}_{[-1,1]}\mathbb{1}_{[0,2]} = \mathbb{1}_{[0,1]} = \mathbb{1}_{[-1,1]}\mathbb{1}_{[0,3]}$ et pourtant, $\mathbb{1}_{[0,2]} \neq \mathbb{1}_{[0,3]}$.

3.2 Groupes des inversibles

Définition 3.3 (Inversibilité dans un anneau, Groupe des inversibles dans un anneau [✓]) :
Soit $(A, +, \times)$ un anneau et $x \in A$.

- Si $\exists y \in A$ tel que $xy = 1_A$, alors x est dit *inversible à droite* dans A et y s'appelle *inverse à droite de* x.
- Si $\exists y \in A$ tel que $yx = 1_A$, alors x est dit *inversible à gauche* dans A et y s'appelle *inverse à gauche de* x.
- Si $\exists y \in A$ tel que $xy = 1_A = yx$, alors x est dit *inversible (bilatère)* dans A et y s'appelle *inverse (bilatère) de* x.
- L'ensemble des éléments inversibles (donc des deux côtés avec le même inverse à gauche et à droite) pour la multiplication est noté $A^\times$.

Remarque :
Comme $(A, +)$ est un groupe, par définition d'un groupe, tous les éléments de A sont automatiquement inversible pour la première LCI. Il n'est pas inutile de le préciser. Si on précise que l'élément est inversible, c'est qu'il est utile de le préciser, que ça n'est pas automatique, que c'est une information supplémentaire. Elle relève donc d'une inversibilité qui n'est pas automatique, donc nécessairement pour la seule autre opération que nous sommes en train de considérer.

Donc toute précision d'inversibilté d'un élément dans un anneau fait automatiquement référence à la deuxième LCI, la seule pour qui ce n'est pas automatique.

Définition 3.4 (Groupes des inversibles [✓]) :
Soit $(A, +, \times)$ un anneau.

On note $A^\times$ l'ensemble des éléments de A inversibles pour la multiplication (donc pour la deuxième LCI), *i.e.*

$$A^\times = \{a \in A,\ \exists b \in A,\ ab = ba = 1_A\}.$$

Remarque :
Attention aux notations, dans les cas où les structures se superposent. Il ne faut pas confondre $A^\times = \{a \in A,\ \exists b \in A,\ ab = ba = 1\}$ et $A^* = \{a \in A,\ a \neq 0\}$. Les deux ensembles ne coïncident pas forcément. J'utiliserais autant que possible la distinction entre les deux ou éventuellement la notation $A \setminus \{0\}$ qui n'aura pas d'ambiguïté possible.

Exemple 3.3 :
Dans l'anneau $(\mathcal{F}(\mathbb{R}, \mathbb{R}), +, \times)$, déterminer le groupe des inversibles.

Proposition 3.5 (Groupes des inversibles [✓]) :
Soit $(A, +, \times)$ un anneau.
Alors $(A^\times, \times)$ est un groupe.

Démonstration :
On sait déjà que le produit de deux inversibles est un inversible. Donc $\times$ est une LCI sur $A^\times$. La loi est associative, il y a un élément neutre et tous les éléments son inversibles par définition. Donc $(A^\times, \times)$ est un groupe. □

Remarque :
Si A est commutatif, alors $(A^\times, \times)$ est un groupe abélien.

De plus, si A est commutatif, l'inversibilité à droite est équivalente à l'inversiblité à gauche qui est équivalente à l'inversibilité bilatérale.

Proposition 3.6 (Unicité de l'inverse bilatéral) :
Soit $(A, +, \times)$ un anneau.
Si $a \in A^\times$, alors son inverse (bilatère) est unique.

Démonstration :
C'est une démo classique qu'on a déjà fait : $b = b(ac) = (ba)c = c$. □

Remarque :
En revanche, les inverses à gauche ou à droite, eux, ne sont pas unique.

Contre-exemple :
On considère dans $\mathcal{F}(\mathbb{R},\mathbb{R})$ les fonctions :

$$f : \begin{array}{ccc} \mathbb{R} & \to & \mathbb{R} \\ x & \mapsto & \begin{cases} \tan(x) & x \not\equiv \frac{\pi}{2}\ [\pi], \\ 0 & x \equiv \frac{\pi}{2}\ [\pi] \end{cases} \end{array} \qquad \forall k \in \mathbb{Z},\ g_k : \begin{array}{ccc} \mathbb{R} & \to & \mathbb{R} \\ x & \mapsto & \arctan(x) + k\pi \end{array}$$

Alors $\forall k \in \mathbb{Z}$, $\forall x \in \mathbb{R}$, $f \circ g_k(x) = \tan(\arctan(x) + k\pi) = x$. Donc $\forall k \in \mathbb{Z}$, $f \circ g_k = \mathrm{Id}_{\mathbb{R}}$. Donc f est inversible à droite et à une infinité d'inverse à droite. Mais f n'est pas injective, donc non-inversible pour la composition car $f(\pi/2) = f(-\pi/2)$ par exemple.

Proposition 3.7 ($\mathbb{Z}^\times$) :

$$\mathbb{Z}^\times = \{-1, 1\}$$

Démonstration :
Soit $n \in \mathbb{Z}^\times$. Alors $\exists m \in \mathbb{Z}$ tel que $nm = 1$. Donc, par définition, n est un diviseur de 1. Donc $n \in \{-1, 1\}$.
L'autre inclusion est évidente. □

3.3 Sous-anneau

Définition 3.5 (Sous-anneau) :
Soit $(A, +, \times)$ un anneau et $B \subset A$. On dit que B *est un sous-anneau de* A si :
(i) B est stable par addition, *i.e.* $\forall b, b' \in B$, $b + b' \in B$
(ii) B est stable par produit, *i.e.* $\forall b, b' \in B$, $bb' \in B$
(iii) $(B, +, \times)$ est un anneau

Autrement dit, si $B \subset A$, B est un sous-anneau de A si $1_A \in B$ et $(B, +|_{B^2}, \times|_{B^2})$ est un anneau.

Proposition 3.8 (Caractérisation des sous-anneau [✓]) :
Soit $(A, +, \times)$ un anneau, $B \subset A$.
Alors B est un sous-anneau de A, si et seulement si :
(i) $1_A \in B$
(ii) $\forall b, b' \in B$, $b - b' \in B$ (*i.e.* B est un sous-groupe de A)
(iii) $\forall b, b' \in B$, $bb' \in B$.

Démonstration :
Pour le sens directe, il faut démontrer seulement le premier point. Les deux autres étant évident par structure d'anneau de B. Mais si $x \in B$, alors $x^{-1} \in B$ puisque $(B, +, \times)$ est un anneau. Mais dans A, $xx^{-1} = 1_A$ et B est stable par produit. D'où le premier point.

Réciproquement, B est évidemment stable par produit et addition (c'est un sous-groupe additif et stable par produit). Il reste à vérifier la définition d'un anneau. Ce qui est assez facile. □

Proposition 3.9 (Sous-anneau de $\mathbb{Z}$ [✓]) :
Les sous-anneau de $\mathbb{Z}$ sont $\{0\}$ et $\mathbb{Z}$ lui-même.

Démonstration :
Soit A un sous-anneau de $(\mathbb{Z}, +, \times)$. Supposons $A \neq \{0\}$. En particulier, A est un sous-groupe de $(\mathbb{Z}, +)$. Donc $\exists n \in \mathbb{N}^*$ tel que $A = n\mathbb{Z}$. D'autre part, $1 \in A$. Donc $\exists m \in Z$ tel que $nm = 1$. Et donc $n = 1$. Donc $A = \mathbb{Z}$. □

3.4 Homomorphismes d'anneaux

Il y a beaucoup de choses que l'on peut dire sur les anneaux. Nous n'avons ici fait que survoler les anneaux. Ils seront étudié un peu plus en détails en MP en introduisant notamment la notion d'idéal.

Définition 3.6 (Homomorphisme d'anneau) :
Soit $(A, +, \times)$ et $(B, \oplus, \otimes)$ deux anneaux et $f : A \to B$.
f est un *homomorphisme d'anneaux* si f est compatible avec les LCI, *i.e.* si
(i) $\forall a, a' \in A$, $f(a + a') = f(a) \oplus f(a')$ (*i.e.* si $f : (A, +) \to (B, \oplus)$ est un homomorphisme de groupes)
(ii) $\forall a, a' \in A$, $f(a \times a') = f(a) \otimes f(a')$

(iii) $f(1_A) = 1_B$

Dans le cas où f est en plus bijective, on dit que f est isomorphisme d'anneaux.

Remarque :
Les homomorphismes d'anneaux sont des morphismes de groupes également (on rappelle qu'un anneau est un groupe muni d'une structure, d'une loi supplémentaire). Donc un morphisme d'anneau, le noyau est celui en tant que morphisme de groupe. Il n'existe pas d'ensemble spécifique aux morphismes d'anneaux et qui jouerait le rôle du noyau.

Remarque :
On peut encore définir le noyau de f, noté toujours $\ker(f)$, qui sera son noyau en tant que morphisme de groupe. La caractérisation de l'injectivité par le noyau s'applique alors encore.

Exemple 3.4 :
Soit $\varphi : \mathcal{F}(\mathbb{R}, \mathbb{R}) \to \mathbb{R}$ définie par $\varphi(f) = f(1)$. Montrer que φ est un morphisme d'anneau pour les lois usuelles.

Proposition 3.10 (Image d'un inversible) :
Soit $(A, +, \times)$ et $(B, \oplus, \otimes)$ deux anneaux et $f : A \to B$ un homomorphisme d'anneaux. Soit $a \in A$.
Si a est inversible (dans A), alors $f(a)$ est inversible (dans B) et $f(a)^{-1} = f(a^{-1})$.

Autrement dit, $f(A^\times) \subset B^\times$. Mais il n'y a pas égalité en générale. Autrement dit, ce n'est pas parce que $f(a) \in B^\times$ que a est inversible. Pour cela, il faudrait que f soit surjective.

Proposition 3.11 (Morphisme d'anneau restreint aux inversibles) :
Soit $(A, +, \times)$ et $(B, \oplus, \otimes)$ deux anneaux et $f : A \to B$ un morphisme d'anneaux.
Alors la restriction de f à $A^\times$ induit un morphisme de groupe de $A^\times$ dans $B^\times$.

Démonstration :
Si $a, a' \in A^\times$, alors, par définition d'un morphisme d'anneau, $f(a \times a') = f(a) \otimes f(a') \in B^\times$. Or $(A^\times, \times)$ et $(B^\times, \otimes)$ donc des groupes, donc la restriction de f à $A^\times$ induit bien un morphisme de groupes. □

Proposition 3.12 (Condition nécessaire d'isomorphisme d'anneaux) :
Soit $(A, +, \times)$ et $(B, \oplus, \otimes)$ deux anneaux et $f : A \to B$ un morphisme d'anneau.
Si f est un isomorphisme d'anneau, alors f est un isomorphisme de groupe de $(A, +)$ sur $(B, \oplus)$.

En particulier, $\ker(f) = \{0_A\}$.

!!! ATTENTION !!!

⚠

Ce n'est pas une équivalence. Il existe des morphisme d'anneaux qui sont des isomorphismes de groupes mais pas d'anneaux.

Les morphismes d'anneaux se comportent bien :

Proposition 3.13 (Compositions, images directes et réciproques de sous-anneau) :
Soit A, B deux anneaux et $f : A \to B$ un morphisme d'anneau. Alors

(i) La composée de deux morphismes d'anneaux et un morphisme d'anneaux.

(ii) Si f est isomorphisme d'anneau, alors f^{-1} est encore un isomorphisme d'anneau.

(iii) $\mathrm{Aut}(A)$, l'ensemble des automorphisme de A, forme un groupe pour la composition (dont l'élément neutre naturellement Id_A).

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

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

Démonstration :
C'est de la vérification très similaire à ce qui a pu être fait avec les morphismes de groupes. □

3.5 Structure de corps

Définition 3.7 (Corps [✓]) :
Un anneau $(A, +, \times)$ commutatif pour lequel $A^\times = A \setminus \{0_A\}$ est appelé *un corps*. Autrement dit, un corps est un anneau commutatif dans lequel tous les éléments non nuls sont inversibles.

Remarque (HP) :
La condition de la commutativité de l'anneau n'est pas obligatoire. En réalité, un corps n'est pas automatiquement commutatif. Par exemple, les octonions forment un corps non commutatifs.

Mais le programme impose de ne considérer que des corps commutatifs.

Remarque :
Dans un corps $\mathbb{K}$, on a $\mathbb{K}^\times = \mathbb{K}^* = \mathbb{K}\setminus\{0\}$. Le groupe des inversibles correspond à tous les éléments sauf l'élément neutre pour l'addition.

Proposition 3.14 (Un corps est intègre) :
Tout corps commutatif est intègre, *i.e.* tout corps n'a pas de diviseur de 0

Démonstration :
Si $ab = 0$ et si $a \neq 0$, alors a est inversible, car on est dans un corps. Et donc $0 = a^{-1}ab = b$ car 0 est absorbant. □

La réciproque est fausse !

Contre-exemple :
$(\mathbb{Z}, +, \times)$ est un anneau intègre qui n'est pas un corps.

Définition 3.8 (Sous-corps) :
Soit $(\mathbb{K}, +, \times)$ un corps et $\mathbb{L} \subset \mathbb{K}$. On dit que $\mathbb{L}$ est un sous-corps de $\mathbb{K}$ si :

(i) $\mathbb{L}$ est un sous-anneau de $\mathbb{K}$

(ii) $\mathbb{L}$ est un corps pour les opérations de $\mathbb{K}$.

Proposition 3.15 (Caractérisation des sous-corps) :
Soit $(\mathbb{K}, +, \times)$ un corps et $\mathbb{L} \subset \mathbb{K}$.
$\mathbb{L}$ est un sous-corps de $\mathbb{K}$ si, et seulement si, :

(i) $1_{\mathbb{K}} \in \mathbb{L}$

(ii) $\mathbb{L}$ est un sous-groupe de $(\mathbb{K}, +)$ (*i.e.* $\forall x, y \in \mathbb{L},\ x - y \in \mathbb{L}$)

(iii) $\mathbb{L}^* = \mathbb{L} \setminus \{0_{\mathbb{K}}\}$ est un sous-groupe de $(\mathbb{K}^*, \times)$ (*i.e.* $\forall x, y \in \mathbb{L}^*,\ xy^{-1} \in \mathbb{L}$).

Exemple 3.5 :
$\mathbb{Q}$ est un sous-corps de $\mathbb{R}$ qui lui même est un sous-corps de $\mathbb{C}$.

Remarque (HP) :
L'étude et la classification des corps fait, entre autre partie, de la théorie de Galois qui voulait unifier les mathématiques de son temps. Ce qu'il est parvenu à faire. À l'âge de 16 ans.