Les structures algébriques

MPSI-1 Prytanée National Militaire

Pascal Delahaye - D'après le cours d'Alain Soyeur

16 décembre 2010

Dans ce cours, nous présentons les structures d'ensembles habituellement utilisées en mathématiques.

⚠ Il va vous falloir être très prudent : dans ce chapitre, les choses ne semblent pas toujours être ce qu'elles sont. La loi " + " ne sera pas forcément l'addition et la loi " × " ne sera pas toujours la multiplication des nombres. Ces lois ne vérifieront donc pas nécessairement les propriétés usuelles de l'addition et de la multiplication (commutativité, associativité ...).

1 Loi de composition interne

DÉFINITION 1 : **Loi de composition interne**
Soit E un ensemble. On appelle *loi de composition interne* une application de $E \times E$ dans E :

$$\begin{array}{rccc} \phi & : & E \times E & \longrightarrow & E \\ & & (a,\, b) & \mapsto & \phi(a,\, b) \end{array}$$

Pour simplifier les notations, on pourra par exemple noter : $\phi(a,\, b) = a \star b$
L'ensemble E muni de la lci $\star$ est noté $(E,\star)$: on dit alors que c'est un *magma*.

Remarque 1.

1. Soient a et b deux éléments de E.
   Il n'y a aucune raison pour que $\phi(a,\, b) = \phi(b,\, a)$, c'est à dire que $a \star b = b \star a$.
2. On peut itérer une lci : si $(a,\, b,\, c) \in E^3$. On notera : $\begin{cases} \phi\big(\phi(a,\, b),\, c\big) = (a \star b) \star c \\ \phi\big(a,\, \phi(b,\, c)\big) = a \star (b \star c) \end{cases}$
   Il n'y a a priori aucune raison pour $(a \star b) \star c = a \star (b \star c)$.

⚠⚠⚠. La lci sera souvent notée "+", "×" ou ".".
Mais attention : ces notations n'auront souvent rien à voir avec l'addition et la multiplication dans $\mathbb{R}$.
On réservera en général la notation "+" lorsque la lci sera commutative.

`Exemple 1.`

1.	Sur $\mathbb{N}$,		la multiplication et l'addition des entiers	sont des lci.
2.	Sur $E = \mathcal{F}(G,G)$	(où G est un ensemble),	la composition des applications	est une lci.
3.	Sur $\mathcal{P}(G)$	(où G est un ensemble),	l'union et l'intersection	sont des lci.
4.	Sur $\mathbb{R}^{\mathbb{N}}$,		la multiplication et l'addition	sont des lci.

Définition 2 : **Propriétés possibles d'une lci**
Soit $\star$ une lci sur un ensemble E.

On dit que $\star$ est : $\begin{cases} \textit{commutative} & \text{ssi} \quad \forall (a,\, b) \in E^2, & a \star b = b \star a \\ \textit{associative} & \text{ssi} \quad \forall (a,\, b,\, c) \in E^3, & a \star (b \star c) = (a \star b) \star c \end{cases}$

Définition 3 : **Elément Neutre**
Un élément $e \in E$ est dit *neutre* ssi $\boxed{\forall x \in E, \quad e \star x = x \star e = x}$

1. Si la loi est noté "+" alors l'élément neutre de E sera noté 0_E (ou 0 s'il n'y a pas d'ambiguité).
2. Si la loi est noté "$\times$" alors l'élément neutre de E sera noté 1_E (ou 1 s'il n'y a pas d'ambiguité).

Pour mq $\star$ est commutative :	Pour mq $\star$ est associative :	Pour mq $e \in E$ est neutre :
1. Soit $(x,\, y) \in E^2$	1. Soit $(x,\, y,\, z) \in E^3$	1. Soit $x \in E$
2. Mq : $x \star y = y \star x \ldots$	2. Mq : $x \star (y \star z) = (x \star y) \star z \ldots$	2. Mq : $e \star x = x$ et $x \star e = x \ldots$
3. Donc $\star$ est commutative	3. Donc $\star$ est associative	3. Donc e est neutre.

Remarque 2.
1. Pour deviner la forme de l'élément neutre, on pourra procéder à une analyse.
2. Si la loi est commutative, il suffit de prouver que $\forall x \in G,\ x \star e = x$ pour prouver que e est élément neutre.

`Exemple 2.`

1.	$(\mathbb{N},\, +)$:	$+$ est une lci commutative et associative,	0 est l'unique élément neutre
2.	$(\mathbb{N},\, \times)$:	$\times$ est une lci commutative et associative,	1 est l'unique élément neutre
3.	$(\mathcal{F}(\mathbb{R},\mathbb{R}),\, \circ)$:	$\circ$ est une lci associative mais pas commutative,	l'application $\mathrm{id}_{\mathbb{R}}$ est un élément neutre
4.	$(\mathcal{P}(G),\, \cup)$:	$\cup$ est une lci commutative, associative,	la partie $\emptyset$ est neutre pour cette loi.

Exercice : 1
$(*)$ Sur $\mathbb{Z}$, étudier les propriétés de la loi $\star$ définie par $''p \star q = p + q + pq''$.

Définition 4 : Si une lci est *associative*, on peut définir les notations suivantes :

1) Lorsque la loi est notée additivement, on définit $\displaystyle\sum_{i=1}^{n} x_i = x_1 + \cdots + x_n$

2) Lorsque la loi est notée multiplicativement, on définit $\displaystyle\prod_{i=1}^{n} x_i = x_1 \times \cdots \times x_n$

Théorème 1 : **Unicité de l'élément neutre**
Si $(E,\, \star)$ possède un élément neutre, il est unique.

Preuve 1 : On considère e et e' deux éléments neutres et on montre facilement qu'ils sont identiques.

Définition 5 : **Monoïde**
Un ensemble $(E,\star)$ muni d'une lci associative et admettant un élément neutre est appelé un monoïde.

`Exemple 3.` $(\mathbb{N},+)$ est un monoïde d'élément neutre 0.

`Exemple 4.` On considère un ensemble fini A appelé *alphabet*, et on définit un *mot* sur A comme étant une suite finie de *lettres* de A. On notera $m = a_1 \ldots a_n$ un tel mot. On définit également le mot vide ε. Sur l'ensemble $A^\star$ des mots de A, on définit une lci appelée la *concaténation* de deux mots de la façon suivante : si $m_1 = a_1 \ldots a_n$ et si $m_2 = b_1 \ldots b_p$, on note $m_1.m_2 = a_1 \ldots a_n b_1 \ldots b_p$. Alors l'ensemble des mots muni de la concaténation, $(A^\star,.)$ admet pour élément neutre le mot vide ε. La lci étant associative, cet ensemble muni de cette lci est un monoïde très utilisé en informatique théorique et en théorie des langages.

`Exemple 5.` Les ensembles suivants admettent-ils un élément neutre?

1. $(P(E), \cap)$ 2. $(P(E), \cup)$ 3. $(\mathbb{N}, +)$ 4. $(\mathbb{N}, \times)$ 5. $(\mathbb{R}, o)$ 6. $(\mathbb{R}, \times)$ 7. $(\mathbb{R}, +)$

DÉFINITION 6 : **Symétrique**
On suppose que $(E, \star)$ possède un élément neutre e. Soit un élément $x \in E$.

On dit qu'un élément $y \in E$ est un *symétrique* de l'élément x ssi : $x \star y = y \star x = e$
Dans ce cas, on dit aussi que x est *symétrisable*.

Remarque 3. Impossible de s'intéresser aux symétriques des éléments de $(E, \star)$ si l'on n'a pas prouvé auparavant l'existence d'un élément neutre.

`Exemple 6.`

1. Dans $(\mathbb{Z}, +)$ tous les éléments admettent un symétrique, en revanche, dans $(\mathbb{N}, +)$ seul 0 admet un symétrique.
2. Dans $(\mathbb{Q}, \times)$, $(\mathbb{R}, \times)$ et $(\mathbb{C}, \times)$ tous les éléments non nuls admettent un symétrique.
3. Dans $(\mathbb{Z}, \times)$ seuls 1 et -1 admettent un symétrique.

`Exemple 7.` Déterminer les éléments des ensembles suivants admettant un symétrique.

1. $(P(E), \cap)$ 2. $(P(E), \cup)$ 3. $(\mathbb{N}, +)$ 4. $(\mathbb{N}, \times)$ 5. $(\mathbb{R}, o)$ 6. $(\mathbb{R}, \times)$ 7. $(\mathbb{R}, +)$

Exercice : 2
$(*)$ Chercher les éléments de $(\mathbb{Z}, \star)$ admettant un symétrique. (où $''p \star q = p + q + pq''$)

Remarque 4. Dans un ensemble E munis d'une lci $\star$, on dit que $a \in E$ est :

1. *régulier à droite* lorsque $\forall (x, y) \in E \times E$, $x \star a = y \star a \Rightarrow x = y$.
2. *régulier à gauche* lorsque $\forall (x, y) \in E \times E$, $a \star x = a \star y \Rightarrow x = y$.
3. *régulier* s'il est régulier à droite et régulier à gauche.

Dans un monoïde, tout élément admettant un symétrique est régulier !

THÉORÈME 2 : **Unicité du symétrique**
Dans un monoïde $(E, \star)$, si un élément $x \in E$ possède un symétrique, ce symétrique est unique.

Preuve 2 : Très facile ! On suppose qu'il y en a deux ...

Remarque 5.

1. Si la loi est notée "+" alors le symétrique de x (alors appelé l'*opposé)* est noté $-x$
2. Si la loi est notée "." ou "$\times$" ou "$\star$" alors le symétrique de x (alors appelé l'*inverse)* est noté x^{-1}

Pour déterminer si un élément x admet un symétrique :

1. On commence par une analyse pour déterminer la forme de ce symétrique y
2. Pour prouver alors que $y \in E$ est le symétrique de $x \in E$:
   (a) Montrons que : $x \star y = e$ ...
   (b) Montrons que : $y \star x = e$ ...
   (c) Donc $y = x^{-1}$.

Remarque 6.

1. Si la loi est commutative, on peut se contenter de démontrer que $x \star y = e$
2. Lorsqu'on sait que $x \in (E, \star)$ admet un symétrique alors $x \star y = e$ suffit à prouver que y est le symétrique de a.
3. Si un élément $x \in E$ possède un symétrique $y \in E$, alors l'élément y possède également un symétrique qui est l'élément x.
   En d'autres termes, nous avons : $(x^{-1})^{-1} = x$ ou $-(-x) = x$

Remarque 7. L'élément neutre est toujours son propre symétrique : $e^{-1} = e$.

Exercice : 3
Dans un monoïde $(E, \star)$, on suppose que pour un élément x, il existe $y, y' \in E$ tels que $\begin{cases} y \star x = e \\ x \star y' = e \end{cases}$.
Prouver que x est inversible.

2 Structure de groupe

2.1 Définition d'un groupe

DÉFINITION 7 : **Groupe**
Soient un ensemble G et $\star$ une loi sur G. On dit que $(G, \star)$ est un *groupe* si :

1. la loi $\star$ est une lci
2. la loi $\star$ est associative
3. G possède un élément neutre pour cette loi
4. Tout élément x de G admet un symétrique dans G

Si de plus la loi $\star$ est commutative, on dit que le groupe est *abélien* (ou *commutatif*).

Remarque 8.

1. Un groupe est donc un monoïde dont tous les éléments sont symétrisables.
2. Soit E un ensemble non vide. Le groupe $(\mathcal{B}(E, E), \circ)$ montre qu'un groupe n'est pas forcément abélien.

`Exemple 8.` IMPORTANT : Les groupes de référence (E est ici un ensemble quelconque non vide) :
$(\mathbb{Z},+)$, $(\mathbb{Q},+)$, $(\mathbb{Q}^*,\times)$, $(\mathbb{R},+)$, $(\mathbb{R}^*,\times)$, $(\mathbb{C},+)$, $(\mathbb{C}^*,\times)$, $(\mathcal{B}(E,E),\circ)$, $(\mathcal{F}(E,\mathbb{R}),+)$, $(\mathbb{R}^{\mathbb{N}}, +)$.

Exercice : 4
(**) Soit E un ensemble non vide et Δ désigne la différence symétrique de deux ensembles : $A\Delta B = (A \cup B)\backslash(A \cap B)$. Démontrer que $(\mathcal{P}(E), \Delta)$ est un groupe commutatif.

THÉORÈME 3 : **Règles de calcul dans un groupe**
Soit $(G,\star)$ un groupe.

1. L'élément neutre est unique
2. Tout élément possède un *unique* symétrique
3. $\forall x \in G$, on a : $\left(x^{-1}\right)^{-1} = x$ (notation multiplicative) ou $-(-x) = x$ (notation additive)
4. On peut *simplifier* : $\forall (a, x, y) \in G^3 : \begin{cases} a \star x = a \star y & \Rightarrow x = y \\ x \star a = y \star a & \Rightarrow x = y \end{cases}$.
5. Soit $(a, b) \in G^2$. L'équation $a \star x = b$ possède une unique solution : $x = a^{-1} \star b$
6. $\forall (x, y) \in G^2$, $(x \star y)^{-1} = y^{-1} \star x^{-1}$ ou $-(x + y) = (-y) + (-x)$

Preuve 3 : La plupart des propriétés précédentes ont été démontrées.

⚠⚠⚠. La loi $\star$ n'étant pas nécessairement commutative, on ne peut simplifier par a l'égalité : $a \star x = y \star a$.

Remarque 9. Notations et propriétés :

Avec la notation Multiplicative	Avec la notation Additive
Notations	**Notations**
$\forall n \in \mathbb{N}^*$, $a^n = a.a.\ldots.a$ et $a^0 = e_G$	$\forall n \in \mathbb{N}^*$, $na = a + a + \cdots + a$ et $0a = e_G$
$\forall n \in \mathbb{N}^*$, $a^{-n} = (a^n)^{-1}$	$\forall n \in \mathbb{N}^*$, $(-n)a = -(na)$
Propriétés	**Propriétés**
$(a.b)^{-1} = b^{-1}.a^{-1}$	$-(a + b) = (-b) + (-a)$
$\forall n \in \mathbb{Z}^*$, $a^n = (a^{-n})^{-1} = (a^{-1})^{-n}$	$\forall n \in \mathbb{Z}^*$, $na = -(-na) = (-n).(-a)$
$\forall (n, m) \in \mathbb{Z}^{*2}$, avec $n + m \neq 0$, $a^{n+m} = (a^n).(a^m)$	$\forall (n, m) \in \mathbb{Z}^{*2}$, avec $n + m \neq 0$, $(n + m)a = na + ma$
$\forall (n, m) \in \mathbb{Z}^{*2}$, $(a^n)^m = a^{n.m}$	$\forall (n, m) \in \mathbb{Z}^{*2}$, $m(na) = (mn)a$

⚠⚠⚠. Les propriétés $\begin{cases} (a.b)^n = a^n.b^n \\ n(a + b) = na + nb \end{cases}$ ne sont valables que si la loi est commutative !

Exercice : 5
(**) Déterminer la structure des groupes à 3 éléments.

2.2 Sous-groupes

DÉFINITION 8 : Soit $(G, \star)$ un groupe.
Les sous-groupes de G sont les sous-ensembles H de G tels que $(H, \star)$ sont des groupes.

`Exemple 9.`
1. Si $(G, \star)$ est un groupe, alors $(\{e_G\}, \star)$ et $(G, \star)$ sont 2 sous-groupes de $(G, \star)$.
2. $\left(C^0(\mathbb{R}, \mathbb{R}),\ +\right)$ est un sous groupe de $\left(\mathcal{F}(\mathbb{R}, \mathbb{R}),\ +\right)$

PROPOSITION 4 : **Caractérisation des Sous-groupes**
Soit $(G, \star)$ un groupe. $(H, \star)$ est un *sous-groupe* de G ssi :
1. H est une partie de G
2. Elément Neutre : $e_G \in H$
3. Stabilités :
   (a) H est *stable* par la lci : $\forall (x, y) \in H^2,\ x \star y \in H$.
   (b) H est stable par *symétrisation* : $\forall x \in H,\ x^{-1} \in H$. (ou $-x \in H$ avec la notation additive)

Preuve 4 : Pas de difficulté, sauf peut-être pour prouver que $e_G \in H$.
H étant un sous-groupe, alors il admet un élément neutre noté e_H. Prouvons que $e_H = e_G$.
On a : $\begin{cases} e_H \star e_H = e_H \\ e_H \star e_G = e_H \end{cases}$ donc $e_H \star e_H = e_H \star e_G$ et en composant par e_H^{-1} on obtient $e_H = e_G$.

Remarque 10.
1. L'avantage de cette caractérisation est qu'elle nous dispense de vérifier l'associativité de la loi $\star$.
2. Si e_g n'appartient pas à H alors H ne peut pas être un sous-groupe de G.
   Ainsi $(2\mathbb{Z} + 1, +)$ *n'est pas un sous-groupe de* $(\mathbb{Z}, +)$.

Ainsi, pour montrer que H est un sous-groupe du groupe $(G,\star)$, on procède en **4 étapes** :
1. On vérifie que : $H \subset G$
2. On vérifie que : $e_G \in H$
3. Stabilité par $\star$: Soit $(x, y) \in H^2$, on vérifie que $x \star y \in H$
4. Stabilité par symétrisation : Soit $x \in H$, on vérifie que $x^{-1} \in H$

`Exemple 10.` Prouver que $(\mathbb{U}, \times)$ est un sous-groupe de $(\mathbb{C}^*, \times)$ où $\mathbb{U} = \{z \in \mathbb{C} \mid |z| = 1\}$.

Exercice : 6
$(**)$ Montrer que les sous-groupes de $(\mathbb{Z}, +)$ sont les $(n\mathbb{Z}, +)$ où $n \in \mathbb{Z}$.

Exercice : 7
$(*)$ Soit un ensemble E non-vide et un élément $a \in E$. On note $G = \{f \in \mathcal{B}(E, E), \text{ tq } f(a) = a\}$
C'est l'ensemble des bijections de G laissant invariant l'élément a.
Montrer que $(G, \circ)$ est un groupe.

Exercice : 8
$(*)$ Soit $(G, .)$ un groupe. On note $C = \{x \in G \mid \forall g \in G,\ g.x = x.g\}$
C'est l'ensemble des éléments de G qui commutent avec tous les éléments de G.
Montrer que $(C, .)$ est un sous-groupe de G (appelé *centre* du groupe G).

2.3 Génération de nouveaux groupes

THÉORÈME 5 : **Groupe produit**
On considère deux groupes $(G,.)$ et $(H,\star)$ et sur l'ensemble $G \times H$, on définit la loi Λ par :

$$\text{Pour tout } ((x, y), (x', y')) \in (G \times H)^2, \quad \text{on définit} \quad (x, y)\Lambda(x', y') = (x.x', y \star y')$$

Alors $(G \times H, \Lambda)$ est un groupe appelé *groupe produit.*

Preuve 5 : On montre que $(G \times H,\Lambda)$ vérifie bien les 4 points qui définissent la structure de groupe.

`Exemple 11.` Démontrer que : Λ est commutative $\iff$. et $\star$ sont commutatives

`Exemple 12.` $(\mathbb{R}^2,+)$ est un groupe où "+" est définie par: $\forall\big((a,\,b),(a',\,b')\big) \in (\mathbb{R}^2)^2$, $(a,\,b)+(a',\,b')=(a+a',\,b+b')$

THÉORÈME 6 : **L'intersection de sous-groupes est un sous-groupe**
Si H_1 et H_2 sont deux sous-groupes d'un groupe G, alors $H_1 \cap H_2$ est un sous-groupe de G

Preuve 6 : Facile!

Remarque 11. Ce théorème se généralise à une famille de sous-groupes de G.

`Exemple 13.` Déterminer $(2\mathbb{Z} \cap 3\mathbb{Z},\,+)$.

⚠⚠⚠. $H_1 \cup H_2$ n'est pas un sous-groupe de G en général. Trouver un contre-exemple!!

Exercice : 9
(**) Soient H_1 et H_2 deux sous-groupes d'un groupe $(G,.)$.
Montrer que: $H_1 \cup H_2$ est un sous-groupe de $G \iff H_1 \subset H_2$ ou $H_2 \subset H_1$

Exercice : 10
(*) Soient F_1 et F_2 deux sous-groupes de G, un groupe commutatif.
1. Démontrer que $F_1+F_2=\{x_1+x_2 \mid (x_1,\,x_2) \in F_1 \times F_2\}$ est un sous-groupe de G.
2. Plus généralement, prouver que la somme de n ($n \geq 2$) sous-groupes de G est un sous-groupe de G.

2.4 Morphisme de groupes

DÉFINITION 9 : **Morphisme de groupes**
Soient deux groupes $(G_1,\,\star)$ et $(G_2,\,\bullet)$.
Une application $f: G_1 \mapsto G_2$ est un *morphisme* de groupes si et seulement si:

$$\forall (x,\,y) \in G_1^2,\quad \boxed{f(x \star y)=f(x) \bullet f(y)}$$

Remarque 12. Un morphisme d'un groupe G vers lui-même est appelé un *endomorphisme* de groupes.

Pour montrer que $f: G_1 \mapsto G_2$ est un morphisme de groupes:
1. On vérifie que $(G_1,\,\star)$ et $(G_2,\,\bullet)$ sont bien des groupes.
2. On vérifie que pour tout $(x,\,y) \in G_1^2$, on a bien $f(x \star y)=f(x) \bullet f(y)$.

`Exemple 14.` Soit $(G,\,.)$ un groupe et $a \in G$. Prouver que $f : \begin{array}{ccc}(\mathbb{Z},+) & \longrightarrow & (G,.) \\ n & \mapsto & a^n\end{array}$ est un morphisme de groupes.

`Exemple 15.` Soit $\mathcal{T}$ l'ensemble des translations du plan $\mathcal{P}$. On note t_a est la translation de vecteur $\vec{v}_a$ d'affixe $a \in \mathbb{C}$.

Prouver que $f : \begin{array}{ccc}(\mathbb{C},+) & \longrightarrow & (\mathcal{T},\,o) \\ a & \mapsto & t_a\end{array}$ est un morphisme de groupes.

PROPOSITION 7 : **Composition**
La composée de deux morphismes de groupes est un morphisme de groupes.

Preuve 7 : Il suffit de bien poser le problème et la démonstration ne présente aucune difficulté.

PROPOSITION 8 : **Propriétés d'un morphisme de groupes**
Soit $\begin{cases} e_1 \text{ l'élément neutre d'un groupe } (G_1,\,.) \\ e_2 \text{ l'élément neutre d'un groupe } (G_2,\,\star)\end{cases}$, et $f : G_1 \mapsto G_2$ un morphisme de groupes. Alors:

1. $f(e_1)=e_2$.
2. $\forall x \in G_1,\, f(x^{-1})=[f(x)]^{-1}$.
3. $\begin{cases}\forall x \in G_1 \\ \forall n \in \mathbb{Z}\end{cases}$, $f(x^n)=f(x)^n$.

Preuve 8 : Il suffit de bien poser le problème et les démonstrations ne présentent aucune difficulté.

Remarque 13. Traduisez les deux dernières propriétés précédentes lorsque les lci sont notées sous forme additive.

THÉORÈME 9 : **Image directe et réciproque de sous-groupes par un morphisme**
Soit $f : G_1 \mapsto G_2$ un morphisme de groupes.
1. Si H_1 est un sous-groupe de G_1, alors $f(H_1)$ est un sous-groupe de G_2.
2. Si H_2 est un sous-groupe de G_2, alors $f^{-1}(H_2)$ est un sous-groupe de G_1.

Preuve 9 : Là encore, il suffit de bien poser le problème et les démonstrations ne présentent aucune difficulté.

DÉFINITION 10 : **Noyau, image d'un morphisme**
On considère un morphisme de groupes $f : G_1 \mapsto G_2$.
On note e_1 l'élément neutre du groupe G_1 et e_2 l'élément neutre du groupe G_2.
On définit :
1) le *noyau* du morphisme f par : $\boxed{\ker(f) = \{x \in G_1 \mid f(x) = e_2\} = f^{-1}(\{e_2\})}$
Il s'agit de l'ensemble des antécédents de e_2 par f

2) l'*image* du morphisme f par : $\boxed{\mathrm{Im}(f) = f(G_1) = \{f(x) \mid x \in G_1\}}$

Remarque 14. D'après le théorème précédent, $\ker f$ est un sous-groupe de G_1 et $\mathrm{Im}\, f$ est un sous-groupe de G_2.

`Exemple 16.` Déterminer le noyau et l'image du morphisme de groupes suivant :

$$f : \begin{array}{ccc}(\mathbb{Z},+) & \longrightarrow & (\mathbb{C}^*,\times) \\ p & \mapsto & \omega^p\end{array} \quad \text{où} \quad \omega = e^{\frac{2i\pi}{n}} \text{ et } n \in \mathbb{N}^* \text{ fixé.}$$

THÉORÈME 10 : **Caractérisation des morphismes injectifs, surjectifs**
Soit un morphisme de groupes $f : G_1 \mapsto G_2$.
On note e_1 l'élément neutre du groupe G_1 et e_2 l'élément neutre du groupe G_2.
On a les propriétés suivantes :
1. f injective $\iff \ker f = \{e_1\}$.
2. f surjective $\iff \mathrm{Im}\, f = G_2$.

Preuve 10 :
1. Pour l'injectivité, on utilise le critère usuel : f injective $\iff \big(f(x) = f(x') \Rightarrow x = x'\big)$.
2. La surjectivité est immédiate.

Pour montrer qu'un morphisme $f : (G_1,\star) \mapsto (G_2,\bullet)$ est injectif :
1. Soit $x \in G_1$ tel que $f(x) = e_2$. Prouvons que : $x = e_1 \ldots$
2. Donc $\ker f = \{e_1\}$, et puisque f est un morphisme de groupes, f est injectif.

DÉFINITION 11 : **Isomorphisme**
On dit qu'une application $f : G_1 \mapsto G_2$ est un *isomorphisme* de groupes si et seulement si
1. l'application f est un morphisme de groupes.
2. l'application f est bijective.

Remarque 15. Un isomorphisme d'un groupe G vers lui-même est appelé un *automorphisme*.

Exercice : 11
(∗)
1. Soit f un isomorphisme de groupes.
Démontrer que sa bijection réciproque $f^{-1} : G_2 \mapsto G_1$ est aussi un isomorphisme.

2. Soit $f : \begin{array}{ccc}(\mathbb{R},+) & \longrightarrow & (\mathbb{R}^{+*},\times) \\ x & \mapsto & e^x\end{array}$
Vérifier que l'application f est un isomorphisme de groupes. Quel est son isomorphisme réciproque?

Exercice : 12
(∗∗) Trouver tous les endomorphismes du groupe $(\mathbb{Z}, +)$. En déduire les automorphismes de $(\mathbb{Z}, +)$.

3 Structure d'anneau

DÉFINITION 12 : **anneau**
Soit A un ensemble muni de deux lci notées $+$ et $\times$. On dit que $(A,\ +,\ \times)$ est un *anneau* ssi :

1. $(A,\ +)$ est un groupe *commutatif*
2. la loi $\times$ est *associative*
3. la loi $\times$ est *distributive* par rapport à la loi $+$:

$$\forall (x,\ y,\ z) \in A^3,\quad x \times (y+z) = x \times y + x \times z$$
$$(x+y) \times z = x \times z + y \times z$$

4. Il existe un *élément neutre* pour $\times$, noté 1_A (ou 1 s'il n'y a pas d'ambiguïté)

Remarque 16. Si en plus la loi $\times$ est commutative, on dit que $(A,\ +,\ \times)$ est un anneau commutatif.

Remarque 17.

1. Dans un anneau $(A,\ +,\ \times)$, on note $-x$ le symétrique de x pour la loi $+$ et 0 l'élément neutre de la loi $+$.
2. Par convention, on conviendra que pour tout $x \in A$, $x^0 = 1_A$. (en particulier, on convient que $0_A^0 = 1_A$)
3. ⚠ Un élément $x \in A$ n'a pas forcément de symétrique pour la loi $\times$, il ne faudra donc pas utiliser abusivement la notation x^{-1}.

`Exemple 17.`

1. $(\mathbb{Z}, +,\ \times)$, $(\mathbb{Q},\ +, \times)$, $(\mathbb{R},\ +, \times)$, $(\mathbb{C},\ +, \times)$, $(\mathcal{P}(E), \Delta, \cap)$ et $(\mathcal{F}(\mathbb{R},\ \mathbb{R}),\ +, \times)$ sont des anneaux commutatifs.
2. $(\mathbb{R}^I,\ +, \times)$, $(\mathbb{C}^I,\ +, \times)$ sont des anneaux commutatifs (I étant un intervalle de $\mathbb{R}$)
3. $(\mathbb{R}^{\mathbb{N}},\ +, \times)$, $(\mathbb{C}^{\mathbb{N}},\ +, \times)$ sont des anneaux commutatifs.
4. $(\mathbb{R}[X],\ +, \times)$, $(\mathbb{C}[X],\ +, \times)$ sont des anneaux commutatifs.

THÉORÈME 11 : **Règles de calcul dans un anneau**
On considère un anneau $(A,\ +,\ \times)$. On a les règles de calcul suivantes :

1)	$\forall a \in A$	$a \times 0 = 0 \times a = 0$
2)	$\forall a \in A$	$(-1) \times a = -a$
3)	$\forall (a,\ b) \in A^2$	$(-a) \times b = -(a \times b) = a \times (-b)$
4)	$\forall (a,\ b) \in A^2$	$(-a) \times (-b) = a \times b$
5)	Si x est inversible, (-x) l'est aussi et :	$(-x)^{-1} = -x^{-1}$
6)	Si x et y sont inversibles, $x \times y$ l'est aussi et :	$(x \times y)^{-1} = y^{-1} \times x^{-1}$
7)	On a la propriété de distributivité suivante :	$a.\sum_{k=1}^{n} x_k = \sum_{k=1}^{n} a.x_k$

Preuve 11 : Petites démonstrations intéressantes qui demandent parfois un peu d'astuce.

`Exemple 18.` Que pouvez-vous dire d'un anneau dont l'élément neutre pour l'addition est le même que celui pour la multiplication ?

Remarque 18. Si $(A,\ +,\ \times)$ est un anneau, $(A,\ \times)$ n'est pas un groupe. (car 0_A n'admet pas d'inverse)

Exercice : 13
Groupe des unités d'un anneau
$(*)$ Soit un anneau $(A,\ +,\ \times)$.
On note A^* l'ensemble des éléments inversibles pour la loi $\times$: $A^* = \{a \in A \mid \exists a' \in A \text{ tq } a \times a' = a' \times a = 1_A\}$
Démontrer que l'ensemble $(A^*,\ \times)$ a une structure de groupe : c'est le *groupe des unités* de l'anneau A.

`Exemple 19.`

1. Dans l'anneau $(\mathbb{Z}, +, \times)$, le groupe des unités est $(\{1, -1\}, \times)$.
2. Dans l'anneau $\left(\mathcal{F}(I, \mathbb{R}), +, \times\right)$, le groupe des unités est constitué des fonctions qui ne s'annulent pas.

⚠⚠⚠. En général, dans un anneau : $\boxed{a \times b = 0 \not\Rightarrow a = 0 \text{ ou } b = 0}$
Lorsque $a \times b = 0$ avec $a \neq 0$ et $b \neq 0$, on dit que a et b sont des *diviseurs de zéro*.
Recherchez des divideurs de zéro dans les anneaux $(\mathcal{F}(\mathbb{R},\ \mathbb{R}),\ +, \times)$ et $(\mathcal{P}(E), \Delta, \cap)$ où E contient au moins 2 éléments.

Exercice : 14

(∗∗) Soit un anneau $(A,\ +,\ \times)$ vérifiant : $\forall x \in A,\quad x^2 = x$
Montrer que l'anneau A est commutatif.

Définition 13 : Anneau intègre
Soit un anneau $(A,\ +,\ \times)$. On dit que cet anneau est *intègre* si et seulement si :
1. $A \neq \{0\}$
2. la loi $\times$ est commutative
3. $\forall (x,\ y) \in A^2,\ x \times y = 0 \Rightarrow x = 0$ ou $y = 0$

Remarque 19. Un anneau intégre est un anneau qui n'admet pas de diviseurs de 0.

Proposition 12 : Simplification dans un anneau intègre
Dans un anneau *intègre*, on a : Si $(a,\ y,\ z) \in A^3$, avec $\begin{cases} ax = ay \\ a \neq 0 \end{cases}$ $\begin{cases} \text{ou} \quad xa = ya \\ \text{ou} \quad ax = ya \end{cases}$, alors $x = y$.

Preuve 12 : Pas de difficulté si l'on pense à utiliser la propriété distributivité de $\times$ sur $+$.

⚠⚠⚠. Cette propriété est généralement fausse dans un anneau quelconque. Donner des exemples !!

Remarque 20. En d'autres termes, dans un anneau intègre, tout élément non nul est régulier.

Définition 14 : Élément nilpotent
Soit un anneau $(A,\ +,\ \times)$.
On dit qu'un élément $a \in A$ $(a \neq 0_A)$ est *nilpotent* s'il existe un entier $n \in \mathbb{N}^*$ tel que $a^n = 0_A$.
Le plus petit entier n vérifiant $a^n = 0_A$ s'appelle l'*indice de nilpotence* de l'élément a.

Remarque 21. Il n'y a pas d'élément nilpotent dans un anneau intègre !

Remarque 22. La notion de nilpotence n'a de sens que dans un anneau puisque sa définition fait intervenir l'élément neutre de la loi "+" et la loi "×".

`Exemple 20.` Chercher un élément nilpotent dans l'anneau $(\mathbb{Z}/4.\mathbb{Z},\ +,\ \times)$.

Théorème 13 : Formule du binôme de Newton
Soit $(A,\ +,\ \times)$, un anneau.
Alors pour tout $n \in \mathbb{N}$ et pour tout couple $(a,\ b) \in A^2$ tels que $\boxed{a.b = b.a}$: $\boxed{(a+b)^n = \sum_{k=0}^{n} \binom{n}{k} a^k b^{n-k}}$

Preuve 13 : Vous pouvez tenter une démonstration par récurrence de cette formule ...

Remarque 23. Cette formule est toujours vraie si l'anneau est commutatif.

Théorème 14 : Formule de factorisation
Soit $(A,\ +,\ \times)$, un anneau.
Alors pour tout $n \in \mathbb{N}^*$ et pour tout couple $(a,\ b) \in A^2$ tels que $\boxed{a.b = b.a}$:

$$\boxed{a^n - b^n = (a-b)(a^{n-1} + a^{n-2}b + \cdots + ab^{n-2} + b^{n-1})} \quad = \quad (a-b)\sum_{k=0}^{n-1} a^{n-1-k}b^k$$

Preuve 14 : Il suffit de développer ...

Remarque 24. Cette formule est toujours vraie si l'anneau est commutatif.

Théorème 15 : Calcul d'une progression géométrique
Soit un anneau $(A, +, \times)$ et un élément $a \in A$. On considère un entier $n \in \mathbb{N},\ n \geq 1$.
On déduit de la formule de factorisation que :

$$\boxed{1 - a^n = (1-a)(1 + a + a^2 + \cdots + a^{n-1})}$$

Preuve 15 :
On applique la formule du théorème précédent lorsque $\left\{\begin{array}{l} a = 1_A \\ b = a \end{array}\right.$

Remarque 25. Les 3 formules précédentes sont bien entendu valables dans $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ et $\mathbb{C}$ munis de l'addition et la multiplication usuelles.

Remarque 26. Si l'élément a est *nilpotent* d'indice n ($a^n = 0$), alors l'élément $(1-a)$ est inversible pour la loi $\times$ et on sait calculer son inverse :

$$(1-a)^{-1} = 1 + a + a^2 + \cdots + a^{n-1}$$

DÉFINITION 15 : **Sous-anneau**
Soit A' un ensemble et $(A, +, \times)$ un anneau.
On dit que A' est un *sous-anneau* de l'anneau A si et seulement si $\left\{\begin{array}{l} A' \subset A \\ (A', +, \times) \text{ est un anneau} \end{array}\right.$.

THÉORÈME 16 : **Caractérisation des sous-anneaux**
Soit A' un ensemble et $(A, +, \times)$ un anneau.
$(A',\ +,\ \times)$ est un sous-anneau de l'anneau A si et seulement si :
1. $A' \subset A$
2. Eléments Neutres : 0_A et 1_A sont des éléments de A'
3. Stabilités :
   (a) A' est stable par les lois $+$ et $\times$
   (b) A' est stable par symétrisation pour $+$.

Preuve 16 : Pas de difficulté particulière.

Remarque 27. Pour montrer qu'un ensemble est un anneau, on préfèrera prouver que cet ensemble est un sous-anneau d'un autre anneau.

`Exemple 21.`

1. $(\mathbb{Z},\ +,\ \times)$ est un sous-anneau de $(\mathbb{Q},\ +,\ \times)$
2. $(\mathbb{Q},\ +,\ \times)$ est un sous-anneau de $(\mathbb{R},\ +,\ \times)$
3. $(\mathbb{R},\ +,\ \times)$ est un sous-anneau de $(\mathbb{C},\ +,\ \times)$
4. $(C_0(\mathbb{R}),\ +,\ \times)$ est un sous-anneau de $(\mathbb{R}^{\mathbb{R}}, +, \times)$

Remarque 28. On peut vérifier assez simplement que les sous-anneaux d'un anneau A sont les anneaux inclus dans A.

4 Structure de corps

DÉFINITION 16 : **Corps**
On considère un ensemble $\mathbb{K}$ muni de deux lois de composition interne, notées $+$ et $\times$.
On dit que $(\mathbb{K},\ +,\ \times)$ est un *corps* si et seulement si :
1. $(\mathbb{K},\ +,\ \times)$ est un anneau commutatif non réduit à $\{0_{\mathbb{K}}\}$.
2. Tout élément non-nul de $\mathbb{K}$ est inversible pour la loi $\times$.

`Exemple 22.`
1. $(\mathbb{Q},\ +,\ \times)$, $(\mathbb{R},\ +,\ \times)$, $(\mathbb{C},\ +,\ \times)$ sont des corps.
2. $(\mathbb{Z},\ +,\ \times)$ n'est pas un corps car 1 et -1 sont les seuls éléments inversibles.

Exercice : 15
$(*)$ Montrer que l'ensemble $(\mathbb{R}, \star, \Delta)$, muni des deux opérations suivantes, est un corps commutatif : $\left\{\begin{array}{l} x \star y = x + y - 1 \\ x \Delta y = x + y - xy \end{array}\right.$.
Aide : vous pourrez traiter cet exercice en vous aidant de Maple et en introduisant les fonctions $\left\{\begin{array}{l} f(x,\ y) = x \star y \\ g(x,\ y) = x \Delta y \end{array}\right.$

Remarque 29. Si $(\mathbb{K}, +, \times)$ est un corps, alors $(\mathbb{K}^*, \times)$ est un groupe, où $\mathbb{K}^* = \mathbb{K} \backslash \{0_{\mathbb{K}}\}$.

PROPOSITION 17 : **Un corps est un anneau intègre**
Dans un corps $(\mathbb{K},\ +,\ \times)$, si deux éléments $(x,\ y) \in \mathbb{K}^2$ vérifient $x \times y = 0_K$, alors $x = 0_K$ ou $y = 0_K$.
En particulier, on peut "simplifier par un élément non nul" :

$$\forall (a,\ x,\ y) \in \mathbb{K}^3 \quad \text{avec} \quad a \neq 0_K, \quad \text{on a} \quad a \times x = a \times y \Rightarrow x = y$$

Preuve 17 : Evident !

Remarque 30. Ainsi, il n'existe pas d'élément nilpotent dans un corps.

THÉORÈME 18 : **Calcul d'une somme géométrique dans un corps**
Soit un élément $k \in \mathbb{K}$ du corps $(\mathbb{K}, +, \times)$.
Alors la formule suivante permet de calculer une progression géométrique de raison k :

$$\sum_{i=0}^{n} k^i = 1 + k + k^2 + \cdots + k^n = \begin{cases} (1-k)^{-1}\left(1-k^{n+1}\right) & \text{si } k \neq 1 \\ (n+1).1_{\mathbb{K}} & \text{si } k = 1 \end{cases}$$

⚠ En général, cette formule n'a pas de sens dans un anneau quelconque.

Preuve 18 : Conséquence d'une formule vue précédemment.

Remarque 31. Les 3 formules vues précédemment dans le cas d'un anneau sont bien entendue valables ici.

DÉFINITION 17 : **Sous-corps**
Soit $\mathbb{K}'$ un ensemble et $(\mathbb{K}, +, \times)$ un corps.
On dit que $\mathbb{K}'$ est un *sous-corps* du corps $\mathbb{K}$ si et seulement si $\begin{cases} \mathbb{K}' \subset \mathbb{K} \\ (\mathbb{K}', +, \times) \text{ est un corps} \end{cases}$.

THÉORÈME 19 : **Caractérisation des sous-corps**
Soit $\mathbb{K}'$ un ensemble et $(\mathbb{K}, +, \times)$ un corps.
$(\mathbb{K}',\ +,\ \times)$ est un sous-corps du corps $\mathbb{K}$ si et seulement si :

1. $\mathbb{K}' \subset \mathbb{K}$
2. Eléments Neutres : $0_{\mathbb{K}}$ et $1_{\mathbb{K}}$ sont des éléments de $\mathbb{K}''$
3. Stabilités :
   (a) $\mathbb{K}'$ est stable par $+$ et $\times$
   (b) $\mathbb{K}'$ est stable par symétrisation pour les lois $+$ et $\times$.

Preuve 19 : Pas de difficulté.

Remarque 32. Pour montrer qu'un ensemble est un corps, on préfèrera prouver que cet ensemble est un sous-corps d'un autre corps.

4.1 Corps des fractions d'un anneau **Complément hors-programme**

Voici une méthode permettant de construire un corps à partir d'un anneau.
Elle permet en particulier de construire le corps $(\mathbb{Q}, +, \times)$ à partir de l'anneau $(\mathbb{Z}, +, \times)$.

1. On considère un anneau $(A, +, \times)$.

2. Sur l'ensemble $A \times A^\star$, on définit une relation par :

$$\boxed{\forall\big((a,\,b),\,(a',\,b')\big) \in A \times A^\star, \quad (a,\,b)\mathcal{R}(a',\,b') \iff a \times b' = a' \times b}$$

   On vérifie que la relation $\mathcal{R}$ est une relation d'équivalence sur l'ensemble $A \times A^\star$ (réflexive, symétrique et transitive).
   On note alors $\mathbb{K}$ l'ensemble des classes d'équivalences de cette relation. Un élément $k \in \mathbb{K}$ est donc la classe d'un couple $(a,\,b) \in A \times A^\star$, et on note cette classe

$$k = \frac{a}{b}$$

3. Sur l'ensemble K, on définit deux lois notées $+$ et $\times$ de la façon suivante :
   Soient $k = \mathrm{Cl}(a,\,b)$ et $k' = \mathrm{Cl}(a',\,b')$ deux classes d'équivalences de représentants $(a,\,b)$ et $(a',\,b')$.
   On note alors :

1)	$k + k' = \mathrm{Cl}(a \times b' + b \times a',\, b \times b')$:	$\dfrac{a}{b} + \dfrac{a'}{b'} = \dfrac{a \times b' + b \times a'}{b \times b'}$
2)	$k \times k' = \mathrm{Cl}(a \times a',\, b \times b')$:	$\dfrac{a}{b} \times \dfrac{a'}{b'} = \dfrac{a \times a'}{b \times b'}$

   et on vérifie que ces classes sont indépendantes des représentants $(a,\,b) \in k$ et $(a',\,b') \in k'$ choisis.

4. On montre alors que $(\mathbb{K}, +, \times)$ est un corps, appelé *corps des fractions* de l'anneau $(A, +, \times)$.

5. Comme l'application suivante est injective, elle permet de "plonger" l'anneau A dans le corps $\mathbb{K}$:

$$\begin{array}{rccc} \phi\ : & A & \longrightarrow & \mathbb{K} \\ & a & \mapsto & \mathrm{Cl}(a,\,1) \end{array}$$

   En d'autres termes, on identifiera la fraction $\dfrac{a}{1}$ à l'élément a de l'anneau A.

Remarque 33. Cette construction est aussi utilisée pour définir le corps des fractions rationnelles à partir de l'anneau des polynômes.