Chapitre 1

Structures algébriques usuelles

En mathématiques, nous avons l'habitude de travailler avec diverses ensembles de nombres tels que l'ensemble des entiers naturels $\mathbb{N}$, l'ensemble des entiers relatifs $\mathbb{Z}$, l'ensemble des rationnels $\mathbb{Q}$, l'ensemble des nombres réels $\mathbb{R}$ ou encore l'ensemble des nombres complexes $\mathbb{C}$. On peut munir ces ensembles de plusieurs opérations : addition, multiplication etc. Dans ce chapitre, nous allons formaliser ces concepts en introduisant des structures algébriques générales telles que les groupes, les anneaux ou les corps que l'on munira d'opérations appelées lois.

1.1 Lois de composition interne

On commence ce chapitre par une définition générale qui servira aux différentes structures.

1.1.1 Loi de composition interne et parties stables

Définition 1.1. *Soit E un sous-ensemble non vide. On appelle loi de composition interne sur E (notée l.c.i.), toute application de $E \times E = E^2$ dans E.*

Notation. Usuellement, on note une l.c.i. parmi la liste de symboles suivants : $+$, $\times$, $*$, $\top$, $\perp$, o.

Remarque. Par exemple, lorsque $*$ est une l.c.i. sur E, on associe à un couple (x, y) de E^2 son image $x * y$ pour la l.c.i. $*$:

$$\begin{cases} E \times E \longrightarrow E \\ (x, y) \longmapsto x * y \end{cases}$$

Exemples 1.2.

1. L'addition $+$ et la multiplication $\times$ sont des l.c.i. sur $\mathbb{N}$.

2. L'addition $+$, la multiplication $\times$ et la soustraction $-$ sont des l.c.i. sur $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ et $\mathbb{C}$.
3. La division est une l.c.i. sur $\mathbb{Q}^*$, $\mathbb{R}^*$ et $\mathbb{C}^*$.
4. La composition o est une l.c.i. sur l'ensemble des applications de E dans E noté $\mathcal{A}(E, E)$.
5. L'addition et le produit matriciels sont des l.c.i. sur l'ensemble des matrices des matrices carrées réelles d'ordre n noté $\mathcal{M}_n(\mathbb{R})$.

Contre-exemples 1.3.

1. La soustraction $-$ n'est pas une l.c.i. sur $\mathbb{N}$ car par exemple, $1 - 2 = -1 \notin \mathbb{N}$.
2. La division n'est pas une l.c.i. sur $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ et $\mathbb{C}$ puisque $2 : 0$ n'existe pas.
3. La multiplication $\times$ n'est pas une l.c.i. sur l'ensemble des nombres imaginaires purs $i\mathbb{R}$ car $i \times i = -1 \notin i\mathbb{R}$.
4. L'addition n'est pas une l.c.i. sur l'ensemble $\mathbb{U}$ des nombres complexes de module 1 car par exemple, 1 et i sont des nombres complexes de module 1 mais leur somme $1+i$ qui est de module $\sqrt{2}$ n'appartient pas à $\mathbb{U}$.

Définition 1.4. *Soit E un ensemble non vide muni d'une l.c.i. $*$. Une partie F de E est dite stable par la l.c.i. $*$ si $\forall (x, y) \in F^2$, $x * y \in F$. On appelle l.c.i. induite par $*$ dans F la restriction de $*$ à $F \times F$.*

Exemples 1.5.

1. Les parties $\mathbb{R}^-$ et $\mathbb{R}^+$ de $\mathbb{R}$ sont stables par l'addition $+$.
2. La partie $\mathbb{R}^+$ de $\mathbb{R}$ est stable par la multiplication $\times$.
3. La partie $\mathbb{R}^-$ de $\mathbb{R}$ n'est pas stable par la multiplication $\times$ car $-1 \times (-2) = 2$ et $2 \notin \mathbb{R}^-$.

1.1.2 Propriétés d'une l.c.i.

Définition 1.6. *Soit E un ensemble non vide muni d'une l.c.i. $*$. On dit que la loi est associative si $\forall (x, y, z) \in E^3$, $(x * y) * z = x * (y * z)$.*

Remarque. Cela permet d'écrire et de définir sans ambiguïté $x * y * z$.

Exemples 1.7.

1. L'addition et la multiplication sont associatives sur $E = \mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ ou $\mathbb{C}$. En effet, pour tout $x, y, z \in E$, on a $(x + y) + z = x + (y + z)$ et $(x \times y) \times z = x \times (y \times z)$.
2. La loi de composition o est associative sur $\mathcal{A}(E, E)$. On a toujours $(fog)oh = fo(goh)$.

3. L'addition et le produit matriciels sont associatifs sur $\mathcal{M}_n(\mathbb{R})$. En effet, pour tout $A \in \mathcal{M}_n(\mathbb{R})$, $(A+B)+C = A+(B+C)$ et $(A \times B) \times C = A \times (B \times C)$.

Contre-exemple 1.8. La soustraction n'est pas associative sur $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ et $\mathbb{C}$ car par exemple $(2-1)-3 \neq 2-(1-3)$.

Définition 1.9. *Soit E un ensemble non vide muni d'une l.c.i. $*$. La loi est dite commutative si pour tout $(x,y) \in E^2$, $x * y = y * x$.*

Exemples 1.10.

1. L'addition et la multiplication sont commutatives sur $E = \mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ et $\mathbb{C}$. En effet, pour tout x, y dans E, on a $x+y = y+x$ et $x \times y = y \times x$.
2. L'addition est commutative sur $\mathcal{M}_n(\mathbb{R})$. En effet, pour tout $A, B \in \mathcal{M}_n(\mathbb{R})$, $A + B = B + A$.

Contre-exemples 1.11.

1. La soustraction n'est pas commutative sur $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ et $\mathbb{C}$. Par exemple, $2 - 1 \neq 1 - 2$.
2. Le produit matriciel n'est pas commutatif sur $\mathcal{M}_n(\mathbb{R})$ dès que $n \geq 2$. Dans $\mathcal{M}_2(\mathbb{R})$, prenons par exemple, $A = \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}$ et $B = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$. On a $AB = A$ alors que $BA = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} = 0_2$.
3. La composition n'est pas commutative sur $\mathcal{A}(E,E)$. En effet, considérons par exemple les fonctions de $\mathbb{R}$ dans $\mathbb{R}$, f et g définies par $f(x) = e^x$ et $g(x) = x + 2$. On a, pour tout réel x, $(fog)(x) = e^{x+2}$ tandis que $(gof)(x) = e^x + 2$. Les fonctions f et g ne sont pas égales (vu que par exemple, elles n'ont pas la même valeur en 0).

Remarque. Même si la l.c.i. $*$ n'est pas commutative, il peut exister deux éléments a et b dans E tels que $a * b = b * a$. On dit que a et b commutent.

Définition 1.12. *Soit E un ensemble non vide muni d'une l.c.i. $*$. Soit $e \in E$. L'élément e est dit élément neutre pour $*$ si pour tout $x \in E$, $x * e = e * x = x$.*

Exemples 1.13.

1. $(\mathbb{C}, +)$ a pour élément neutre 0 car $x+0 = 0+x = x$, pour tout $x \in \mathbb{C}$.
2. $(\mathbb{C}, \times)$ a pour élément neutre 1 car on a toujours $x \times 1 = 1 \times x = x$.
3. $(\mathcal{M}_n(\mathbb{R}), +)$ a pour élément neutre la matrice nulle 0_n car pour tout A dans $\mathcal{M}_n(\mathbb{R})$, $A + 0_n = 0_n + A = A$.
4. $(\mathcal{M}_n(\mathbb{R}), \times)$ a pour élément neutre la matrice identité I_n car pour tout A dans $\mathcal{M}_n(\mathbb{R})$, $A \times I_n = I_n \times A = A$.

5. $(\mathcal{A}(E,E),o)$ a pour élément neutre l'application Id_E :

$$\mathrm{Id}_E\colon \begin{cases} E \longrightarrow E \\ x \longmapsto x \end{cases}$$

En effet, pour tout fonction f de E dans E, on a $f o \mathrm{Id}_E = \mathrm{Id}_E o f = f$.

Contre-exemple 1.14. $(\mathbb{N}^*,+)$ n'a pas d'élément neutre car $0 \notin \mathbb{N}^*$.

Proposition 1.15. *Si E ensemble muni d'une l.c.i. $*$ admet un élément neutre alors il est unique.*

Démonstration. Supposons que e_1 et e_2 sont deux éléments neutres. Calculons $e_1 * e_2$ de deux manières différentes. D'une part, comme e_1 est un élément neutre, on a $e_1 * e_2 = e_2$. D'autre part, puisque e_2 est un élément neutre, on a $e_1 * e_2 = e_1$. Ainsi, $e_1 = e_2$ d'où l'unicité de l'élément neutre. □

Définition 1.16. *Soit $(E,*)$ un ensemble non vide muni d'une l.c.i. $*$ admettant un élément neutre e. Soit $x \in E$. On dit que x est symétrisable pour $*$ dans E s'il existe $x' \in E$ tel que $x*x' = x'*x = e$. x' est appelé symétrique de x.*

Proposition 1.17. *Soit E un ensemble non vide muni d'une l.c.i. $*$, associative et admettant un élément neutre e. Soit $x \in E$. Si x est symétrisable alors son symétrique est unique.*

Démonstration. Soit $x \in E$. Montrons que x admet un unique symétrique. On suppose qu'il existe deux éléments x'_1 et x'_2 de E tels que $x*x'_1 = x'_1*x = e$ et $x * x'_2 = x'_2 * x = e$. On calcule $x'_1 * x * x'_2$ de deux manières différentes grâce à l'associativité de la loi $*$. D'une part,

$$x'_1 * x * x'_2 = x'_1 * (x * x'_2) = x'_1 * e = x'_1.$$

D'autre part,

$$x'_1 * x * x'_2 = (x'_1 * x) * x'_2 = e * x'_2 = x'_2.$$

On en déduit que $x'_1 = x'_2$ d'où l'unicité du symétrique de x. □

Remarque. Si la loi est notée additivement, on parle de l'opposé de x et on le note $-x$. Si la loi est notée multiplicativement, on parle de l'inverse de x et on le note x^{-1}.

Exemples 1.18.

1. Dans $(\mathbb{C},+)$ (qui a pour élément neutre 0), tout élément z admet pour opposé $-z$ car $z + (-z) = 0$ et $(-z) + z = 0$.
2. Dans $(\mathbb{C},\times)$ (qui a pour élément neutre 1), tout élément z admet un inverse sauf l'élément 0. En effet, il n'existe aucun complexe y tel que $0 \times y = y \times 0 = 1$.

3. Dans $(\mathbb{Z}, \times)$ seuls 1 et -1 sont inversibles.
4. Dans $(\mathcal{M}_n(\mathbb{R}), +)$ tout élément admet un opposé.
5. Les applications symétrisables de $(\mathcal{A}(E, E), o)$ sont les bijections de E dans E.

Proposition 1.19. *Soit E un ensemble non vide muni d'une l.c.i. $*$ associative et admettant un élément neutre e.*

1. *L'élément neutre e est son propre inverse i.e. $e' = e$.*
2. *Si x est symétrisable alors x' est aussi symétrisable et $(x')' = x$.*
3. *Si x et y sont symétrisables alors $x*y$ est aussi symétrisable et $(x*y)' = y' * x'$.*

Démonstration. 1. Montrons que e est son propre inverse. Comme e est l'élément neutre, on a $e * e = e$ d'où $e' = e$.

2. Par définition de x', on a $x'*x = x*x' = e$ donc x' est bien symétrisable, de symétrique x.
3. Soient x et y deux éléments de E symétrisables. On pose $z = x * y$ et $t = y' * x'$. Puisque $*$ est associative, on a :

$$z * t = (x * y) * (y' * x') = x * (\underbrace{y * y'}_{=e}) * x' = (x * e) * x' = x * x' = e.$$

On montrerait de même que $t * z = e$. On a bien montré que z admet t comme symétrique, i.e. $z' = t$ ou encore $(x * y)' = y' * x'$.

□

Remarque. Attention, si la l.c.i. $*$ n'est pas commutative, il n'est pas vrai en général que $(x * y)' = x' * y'$!

1.2 Structure de groupe

1.2.1 Définition d'un groupe et exemples

Définition 1.20. *Soit G un ensemble non vide et soit $*$ une loi de composition sur G. $(G, *)$ est un groupe si la loi $*$ satisfait les propriétés suivantes :*

1. *$*$ est une l.c.i. ;*
2. *$*$ est associative ;*
3. *$*$ admet un élément neutre e ;*
4. *Tout élément de G admet un symétrique dans G pour $*$.*

Définition 1.21. *Soit $(G, *)$ un groupe. G est dit commutatif ou abélien si $*$ est commutative.*

Exemples 1.22.

1. Les groupes $(\mathbb{Z}, +)$, $(\mathbb{Q}, +)$, $(\mathbb{R}, +)$ et $(\mathbb{C}, +)$ sont abéliens.
2. Les groupes $(\mathbb{Q}^*, \times)$, $(\mathbb{R}^*, \times)$, $(\mathbb{C}^*, \times)$ sont abéliens.
3. Le groupe $(\{-1, 1\}, \times)$ formé par les deux éléments -1 et 1 et muni de la multiplication est abélien.
4. Le groupe $(\mathbb{U}, \times)$ des nombres complexes de module 1 muni de la multiplication est abélien.
5. Le groupe $(\mathcal{S}(E), o)$ des bijections de E dans E muni de la composition des composition des applications linéaires est un groupe non abélien dès que $\text{card}(E) \geq 3$..
6. Le groupe $(\mathcal{M}_n(\mathbb{R}), +)$ des matrices carrées réelles de taille $n \in \mathbb{N}^*$ muni de l'addition est abélien.

Contre-exemples 1.23.

1. $(\mathbb{N}, +)$ n'est pas un groupe : à part 0, les éléments n'ont pas d'opposé.
2. $(\mathbb{Z}^*, \times)$ n'est pas un groupe : à part -1 et 1, les éléments n'ont pas d'opposé.
3. $(\mathbb{R}, \times)$ et $(\mathbb{C}, \times)$ ne sont pas des groupes car 0 n'a pas d'inverse.
4. $(\mathcal{M}_n(\mathbb{R}), \times)$ n'est pas un groupe car par exemple la matrice nulle 0_n n'admet pas d'inverse.

1.2.2 Table de loi

Lorsqu'un ensemble fini E est muni d'une l.c.i. $*$, il est possible de présenter les résultats obtenus pour la l.c.i. dans un tableau appelé table de Cayley.

Définition 1.24. *Soit $E = \{x_1, \ldots, x_n\}$ un ensemble fini à n éléments muni d'une l.c.i. $*$. On appelle table de Cayley de l'ensemble $(E, *)$, le tableau carré à n lignes et n colonnes obtenu en inscrivant à l'intersection de la i-ème ligne (représentant l'élément x_i) et de la j-ème colonne (représentant l'élément x_j) l'élément $x_i * x_j$.*

$*$	x_1	x_2	$\ldots$	x_j	$\ldots$	x_n
x_1						
x_2						
$\vdots$						
x_i				$x_i * x_j$		
$\vdots$						
x_n						

Analyse de la table de Cayley :

1. Si la table est symétrique par rapport à la diagonale descendante alors la loi $*$ est commutative.
2. Si l'élément neutre apparait une fois et une seule dans chaque ligne (resp. colonne) alors chaque élément possède un unique symétrique.

Remarque. Attention, la propriété d'associativité d'une loi $*$ ne se lit pas directement dans la table de Cayley. Il faut faire tous les calculs séparément.

Remarque. La table de Cayley d'un groupe fini a une particularité : c'est toujours un tableau carré dans lequel dans chaque ligne et chaque colonne apparait une et une seule fois chaque élément du groupe. Attention, la réciproque est fausse car il est possible que la règle d'associativité ne soit pas vérifiée.

Exemple 1.25. On considère la table de Cayley suivante. Définit-elle un groupe ? Si oui, est-il abélien ?

$*$	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

L'étude de la première ligne et de la première colonne montre que e est l'élément neutre. De plus, $a^2 = b^2 = c^2 = e$ implique que a, b et c sont symétrisables et que chacun d'eux est leur propre symétrique. Puisque la table est symétrique par rapport à la diagonale descendante, on en déduit que $*$ est commutative. Pour montrer que la table définit bien un groupe abélien à 4 éléments, il reste à établir que la loi $*$ est associative, ce qui se vérifie facilement.

1.2.3 Propriétés d'un groupe

Nous terminons la partie sur les groupes en résumant les différentes propriétés d'un groupe :

Proposition 1.26. *Soit $(G, *)$ un groupe alors G satisfait les propriétés suivantes :*

1. *G est non vide : il contient au moins l'élément neutre.*
2. *L'élément neutre est unique.*
3. *Le symétrique d'un élément est unique.*
4. *$\forall (x, y) \in G$, $(x * y)' = y' * x'$.*

5. *Pour $x, y, z \in G$, si $x * y = x * z$ alors $y = z$ (i.e. on peut simplifier à gauche). De même, si $y * x = z * x$ alors $y = z$ (i.e. on peut simplifier à droite). On dit que x est régulier.*
6. *En particulier, pour $x, y \in G$, si $x * y = e$ alors y est le symétrique de x et $x' = y$. De même, si $y * x = e$ alors $x' = y$.*
7. *En particulier encore, pour $x, y \in G$, si $x * y = x$ alors $y = e$. De même, si $y * x = x$ alors $y = e$.*

Démonstration. Les quatre premières propriétés ont déjà été prouvées précédemment. La propriété 6) est une application de la propriété 5) en remarquant que $e = x * x' = x' * x$. De même, la propriété 7) découle de 5) en remarquant que $x = x * e = e * x$. Il nous reste donc à prouver la propriété 5). Soit $x, y, z \in G$ tels que $x * y = x * z$. On a alors en multipliant à gauche par x' : $x' * (x * y) = x' * (x * z)$. Par associativité de la loi $*$, on obtient que $y = z$. De façon en analogue (en fait, en multipliant à droite par x'), on déduit de $y * x = z * x$ que $y = z$. □

Définition 1.27. *Soit x un élément d'un groupe $(G, *)$. On définit la suite $(x^{*n})_{n\in\mathbb{N}}$ des itérés de x par :*

$$x^{*0} = e, \quad \forall n \in \mathbb{N}, x^{*(n+1)} = x * x^{*n}.$$

L'élément x^{*n} s'appelle le n-ème itéré de x pour $*$. On notera pour $n \in \mathbb{N}^*$, $x^{*(-n)} = (x')^{*n} = (x^{*n})'$.

Proposition 1.28. *Soit x un élément d'un groupe $(G, *)$. Alors :*

1. *$\forall n \in \mathbb{Z}$, $(x^{*n})' = x^{*(-n)}$.*
2. *$\forall (n, m) \in \mathbb{Z}^2$, $x^{*(n+m)} = x^{*n} * x^{*m}$.*
3. *$\forall (n, m) \in \mathbb{Z}^2$, $(x^{*n})^{*m} = x^{*(nm)}$.*

Démonstration. Ces résultats se démontrent par récurrence (à m fixé pour le second) et leur preuve est laissée au lecteur. □

Remarque.

1. En notation additive, pour tout $n \in \mathbb{N}^*$, $x^{+n} = \underbrace{x + x + \cdots + x}_{n \text{ fois}} = nx$ avec $1.x = x$ et $0.x = 0$.
2. En notation multiplicative, pour tout $n \in \mathbb{N}^*$, $x^{\times n} \underbrace{x \times x \times \cdots \times x}_{n \text{ fois}} = x^n$ avec $x^1 = x$ et $x^0 = 1$.

1.2.4 Morphismes de groupes

Définition 1.29. *Soient $(E_1, *)$ et $(E_2, \perp)$ deux ensembles non vides munis des l.c.i. $*$ et $\perp$ respectivement. Soit f une application de E_1 dans E_2. On dit que f est un morphisme de $(E_1, *)$ dans $(E_2, \perp)$ si*

$$\forall (x, y) \in E_1^2, \quad f(x * y) = f(x) \perp f(y).$$

Vocabulaire : soient $(G_1, *)$ et $(G_2, \perp)$ deux groupes.

1. Si f est un morphisme de $(G_1, *)$ dans $(G_2, \perp)$ alors on dit que f est un morphisme de groupes.
2. Si de plus, f est bijective, on dit que f est un isomorphisme de $(G_1, *)$ dans $(G_2, \perp)$ et $(G_1, *)$ et $(G_2, \perp)$ sont alors dits isomorphes.
3. Un morphisme de $(G_1, *)$ dans $(G_1, *)$ est dit endomorphisme de $(G_1, *)$.
4. Un endomorphisme bijectif de $(G_1, *)$ est dit automorphisme de $(G_1, *)$.

Exemple 1.30. Soit

$$f : \begin{cases} (\mathbb{R}, +) & \longrightarrow (\mathbb{R}_+^*, \times) \\ x & \longmapsto e^x. \end{cases}$$

On a pour tout réel x et y, $e^{x+y} = e^x \times e^y$ donc f est un morphisme de $(\mathbb{R}, +)$ dans $(\mathbb{R}_+^*, \times)$. De plus, on sait que f est bijective donc f est isomorphisme de groupes et les groupes $(\mathbb{R}, +)$ et $(\mathbb{R}_+^*, \times)$ sont alors isomorphes.

Exemple 1.31. L'application

$$\varphi : \begin{cases} (\mathbb{R}, +) & \longrightarrow (\mathbb{U}, \times) \\ x & \longmapsto e^{ix}. \end{cases}$$

est un morphisme de groupes. En effet, pour tout $(x, y) \in \mathbb{R}^2$, on a $\varphi(x+y) = e^{i(x+y)} = e^{ix} \times e^{iy} = \varphi(x) \times \varphi(y)$.

1.2.5 Sous-groupes

Définition 1.32. *Soient $(G, *)$ un groupe et H une partie de G. On dit que $(H, *)$ est un sous-groupe de $(G, *)$ si H est stable par la l.c.i. $*$ et si H muni de la l.c.i. $*$ induite est encore un groupe.*

Exemples 1.33.

1. $\{e\}$ et G sont des sous-groupes de G. Ils sont appelés sous-groupes triviaux de G.
2. Chacun des groupes additifs $\{0\}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ et $\mathbb{C}$ est un sous-groupe de lui même et de ses suivants.
3. Chacun des groupes multiplicatifs $\{-1, 1\}$, $\mathbb{Q}^*$, $\mathbb{R}^*$ et $\mathbb{C}^*$ est un sous-groupe de lui même et de ses suivants.
4. L'ensemble des nombres complexes de module 1, $(\mathbb{U}, \times)$ est un sous-groupe de $(\mathbb{C}^*, \times)$ (voir TD).

Remarque.

1. Attention, si $(H, \perp)$ et $(G, *)$ sont deux groupes tels qu'on a $H \subset G$, il n'y pas de raison en général que H soit un sous-groupe de $(G, *)$ (penser aux deux groupes $(\mathbb{U}, \times)$ et $(\mathbb{C}, +)$).

2. Tout sous-groupe d'un groupe abélien est abélien. Remarquons qu'un sous-groupe d'un groupe non abélien peut-être abélien. Par exemple, $\{e\}$ est un sous-groupe abélien de E que E soit abélien ou non.

Pour montrer que $(H, *)$ est un sous-groupe de $(G, *)$, on aimerait bénéficier du fait que $(G, *)$ est un groupe. On a la caractérisation suivante des sous-groupes :

Proposition 1.34. *Soient $(G, *)$ un groupe et H une partie de G. $(H, *)$ est un sous-groupe de $(G, *)$ si et seulement si :*

1. *$e \in H$ (en particulier, H est non vide) ;*
2. *$*$ est une l.c.i. sur H ;*
3. *pour tout x de H, l'inverse de x pour la loi $*$ de G est dans H.*

Démonstration. On montre le résultat par double implication.

1. Soit H une partie de G, stable pour $*$ telle que $(H, *)$ soit un groupe. Il est clair que 2) est satisfaite.
   Notons e_H l'élément neutre de $(H, *)$. On a $e_H * e_H = e_H = e_H * e$ donc en simplifiant à gauche par e_H, on obtient que $e_H = e$. Ainsi, 1) est satisfaite.
   Soit $x \in H$. Puisque $(H, *)$ est un groupe, x admet un symétrique y pour $*$ dans H : $x * y = y * x = e$. Alors y est le symétrique de x pour $*$ dans G. Par unicité du symétrique, on obtient que $y = x' \in H$ et 3) est satisfaite.
2. Réciproquement, soit H une partie de G satisfaisant 1), 2) et 3). D'après 2), $*$ définit une l.c.i. sur H.
   Sur H, $*$ est associative (car elle l'est dans G), admet e pour élément neutre (car d'après 1), $e \in H$) et tout élément de H admet un symétrique dans H pour $*$ d'après 3). Par conséquent, $(H, *)$ est un groupe et $(H, *)$ est donc bien un sous-groupe de $(G, *)$.

□

Remarque.

— En notation additive :
   1. $e \in H$
   2. $\forall (x, y) \in H^2$, $x + y \in H$
   3. $\forall x \in H$, $-x \in H$.

— En notation multiplicative :
   1. $e \in H$
   2. $\forall (x, y) \in H^2$, $x.y \in H$
   3. $\forall x \in H$, $x^{-1} \in H$.

On peut condenser la caractérisation précédente d'un sous-groupe en :

Proposition 1.35. *Soient $(G,*)$ un groupe et H une partie de G. $(H,*)$ est un sous-groupe de $(G,*)$ si et seulement si :*

1. *H est non vide ;*
2. *$\forall (x,y) \in H^2$, $x * y' \in H$.*

Démonstration.
1. On suppose que H est un sous-groupe de $(G,*)$. D'après la proposition précédente, $e \in H$ donc H est non vide. Soit $x, y \in H$. D'après la proposition précédente, puisque H est un sous-groupe de G, on a $y' \in H$ puis, comme $*$ est une l.c.i. pour H, $x * y' \in H$.
2. Réciproquement, soit H une partie de G satisfaisant 1) et 2). Soit $x \in H$ et posons $y = x$. Alors $x * x' = e \in H$ d'après le point 2) et donc $e \in H$.
   De plus, en appliquant 2) avec $x = e$, on a $e * x' = x' \in H$ donc tout élément x de H admet un symétrique dans H pour $*$.
   Enfin, si l'on se donne deux éléments x et y de H, on a $y' \in H$ d'après ce qui précède et donc $x * (y')' = x * y \in H$.

On a ainsi montré que H est un sous-groupe de $(G,*)$. □

Exemple 1.36. Pour $n \in \mathbb{N}$, le groupe $n\mathbb{Z} = \{n \times a : a \in \mathbb{Z}\}$ est un sous-groupe de $(\mathbb{Z},+)$. En effet, soit $n \in \mathbb{N}$.

1. On vérifie que $n\mathbb{Z} \subset \mathbb{Z}$.
2. Puisque $0 = n \times 0$ donc $0 \in n\mathbb{Z}$ donc $n\mathbb{Z}$ est non vide.
3. Soient x et y deux éléments de $n\mathbb{Z}$. Alors il existe deux entiers relatifs k_1 et k_2 tels que $x = nk_1$ et $y = nk_2$. Alors
$$x - y = nk_1 - nk_2 = n\underbrace{(k_1 - k_2)}_{\in \mathbb{Z}} \in n\mathbb{Z}.$$

On a donc bien montré que $n\mathbb{Z}$ est un sous-groupe de $(\mathbb{Z},+)$.

Proposition 1.37. *Soit $(G,*)$ un groupe. L'intersection de deux sous-groupes H et K de $(G,*)$ est un sous-groupe de $(G,*)$.*

Démonstration. La preuve sera faite en TD. □

Remarque. Attention, la réunion de deux sous-groupes n'est pas en général un sous-groupe (cf TD).

1.3 Structure d'anneau

1.3.1 Définition d'un anneau et exemples

Définition 1.38. *Soit E un ensemble muni de deux l.c.i. $*$ et $\top$. On dit que $*$ est distributive par rapport à $\top$ si $\forall (x,y,z) \in E^3$, $x*(y\top z) = (x*y)\top(x*z)$ et $(y\top z)*x = (y*x)\top(z*x)$.*

Exemples 1.39.

1. Dans $(\mathbb{R}, +, \times)$, la multiplication $\times$ est distributive par rapport à l'addition $+$.
2. Dans $(\mathcal{P}(E), \cup, \cap)$, l'intersection $\cap$ est distributive par rapport à la réunion $\cup$ et a réunion $\cup$ est distributive par rapport à l'intersection $\cap$.

Contre-exemple 1.40. Dans $\mathcal{A}(\mathbb{R}, \mathbb{R})$ la loi de composition o n'est pas distributive par rapport à l'addition $+$. Considérons par exemple, trois fonctions f, g h définies de $\mathbb{R}$ dans $\mathbb{R}$ par $f(x) = e^x$, $g(x) = x$ et $h(x) = -x$. Alors pour tout réel x, on a :

$$(fo(g+h))(x) = f((g+h)(x)) = f(g(x)+h(x)) = f(x-x) = f(0) = 1$$

tandis que,

$$\begin{aligned}((fog)+(foh))(x) &= (fog)(x)+(foh)(x)\\ &= f(g(x))+f(h(x)) = f(x)+f(-x) = e^x+e^{-x}.\end{aligned}$$

Ainsi, $fo(g+h) \neq (fog)+(foh)$.

Définition 1.41. *Soit A un ensemble muni de deux lois de composition $+$ et $\times$. A est un anneau si les lois $+$ et $\times$ satisfont les propriétés suivantes :*

1. *$(A, +)$ est un groupe abélien. L'élément neutre est noté 0_A ;*
2. *$\times$ est une l.c.i. ;*
3. *$\times$ est associative ;*
4. *$\times$ admet un élément neutre, appelé l'unité de l'anneau et noté 1_A ;*
5. *$\times$ est distributive par rapport à $+$.*

Si de plus $\times$ est commutative, A est dit anneau commutatif.

Usuellement, on appelle addition la loi $+$, d'élément neutre 0_A et dont le symétrique d'un élément a de A par $+$ est appelé opposé de a et est noté $-a$. Usuellement, on appelle multiplication la loi $\times$, d'élément neutre 1_A et dont le symétrique **éventuel** d'un élément a de A par $\times$ est appelé inverse et est noté a^{-1}.

Exemples 1.42.

1. Les anneaux commutatifs $(\mathbb{Z}, +, \times)$, $(\mathbb{Q}, +, \times)$, $(\mathbb{R}, +, \times)$ et $(\mathbb{C}, +, \times)$.
2. L'anneau commutatif $(\mathbb{R}^{\mathbb{N}}, +, \times)$ des suites réelles.
3. L'anneau commutatif $(\mathcal{A}(\mathbb{R}, \mathbb{R}), +, \times)$ des fonctions de $\mathbb{R}$ dans $\mathbb{R}$.
4. Les anneaux non commutatifs $(\mathcal{M}_n(A), +, \times)$ pour $n \geq 2$ et où A est égal à $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ ou $\mathbb{C}$.

Contre-exemples 1.43.

1. $(\mathbb{N}, +, \times)$ n'est pas un anneau car $(\mathbb{N}, +)$ n'est pas un groupe.
2. $(\mathcal{A}(\mathbb{R}, \mathbb{R}), +, o)$ n'est pas un anneau car la composition des applications n'est pas distributive par rapport à l'addition (cf contre-exemple précédent).

Remarque. On ne demande pas que $(A, \times)$ soit un groupe.

Par définition, pour tout $a \in A$ et $n \in \mathbb{N}^*$, on a :

$$na = \underbrace{a + a + \cdots + a}_{n \text{ fois}} \quad \text{et} \quad n^a = \underbrace{a \times a \times \cdots \times a}_{n \text{ fois}}.$$

1.3.2 Propriétés d'un anneau

Proposition 1.44. *Soit $(A, +, \times)$ un anneau. Les propriétés suivantes sont vérifiées :*

1. $\forall a \in A$, $a \times 0_A = 0_A \times a = 0_A$. *On dit que 0_A est absorbant pour la loi $\times$.*
2. $\forall (a, b) \in A^2$, $(-a) \times b = -(a \times b) = a \times (-b)$. *C'est la règle des signes.*
3. $\forall a \in A$, $\forall (x_1, \ldots, x_n) \in A^n$, $a \left(\sum_{i=1}^n x_i\right) = \sum_{i=1}^n a x_i$ *et* $\left(\sum_{i=1}^n x_i\right) a = \sum_{i=1}^n x_i a$.
4. $\forall (a, b, c) \in A^3$, $a \times (b - c) = a \times b - a \times c$ *et* $(b - c) \times a = b \times a - c \times a$ *($\times$ est distributive par rapport à $-$).*

Démonstration.

1. Soit $a \in A$. Puisque $\times$ est distributive par rapport à $+$, on a $a \times 0_A = a \times (0_A + 0_A) = a \times 0_A + a \times 0_A$. En ajoutant à chaque membre l'opposé de $a \times 0_A$, on trouve bien $0_A = a \times 0_A$. L'autre égalité se prouve de même.
2. Puisque $\times$ est distributive par rapport à $+$, on a $(-a) \times b + a \times b = (-a + a) \times b = 0_A \times b = 0_A$ d'après 2). Par définition de l'opposé d'un élément, on obtient que $(-a) \times b$ est l'opposé de $a \times b$ et que $(-a) \times b = -(a \times b)$. Un raisonnement similaire fournit l'égalité : $-(a \times b) = a \times (-b)$.
3. Il s'agit d'un raisonnement par récurrence reposant sur la distributivité de la multiplication par rapport à l'addition.
4. Soient $a, b, c \in A^3$. On a :

$$\begin{aligned} a \times (b - c) + a \times c = a \times [(b - c) + c] &= a \times [b + (-c + c)] \\ &= a \times (b + 0_A) = a \times b \end{aligned}$$

d'où $[a \times (b - c) + a \times c] + (-a \times c) = a \times b + (-a \times c)$ soit $a \times (b - c) + (a \times c - a \times c) = a \times b - a \times c$ et finalement $a \times (b - c) = a \times b - a \times c$. L'autre égalité se montre de manière similaire.

□

Remarque. Soit $(A, +, \times)$ un anneau. Si $1_A = 0_A$ alors $\forall a \in A, a \times 0_A = a \times 1_A$ d'où $0_A = 1_A$. Ainsi, $A = \{0_A\}$ et A est appelé anneau nul.

Proposition 1.45. *Soit $(A, +, \times)$ un anneau. Soient a et b deux éléments de A qui commutent alors, on a :*

1. *Formule du binôme de Newton : $\forall n \in \mathbb{N}$,*

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

2. *Égalité de Bernoulli : $\forall n \in \mathbb{N}^*$,*

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

Remarque. Les points 1) et 2) de la proposition précédente sont donc toujours vérifiés pour tout couple d'éléments d'un anneau commutatif.

Démonstration.

1. La formule du binôme de Newton se montre par récurrence sur n.
2. Montrons l'égalité de Bernoulli. On a :

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

qui se réécrit en utilisant la distributivité de $\times$ par rapport à $-$,

$$(a^n + a^{n-1}b + \cdots + a^2 b^{n-2} + ab^{n-1}) - (a^{n-1}b + a^{n-2}b^2 + \cdots + ab^{n-1} + b^n),$$

puis $a^n - b^n$ par télescopage. D'où le résultat. L'autre égalité se montre de la même façon.

□

Puisque 1_A commute avec tout élément d'un anneau A, la proposition suivante est une application directe de l'égalité de Bernoulli :

Proposition 1.46. *Soit $(A, +, \times)$ un anneau. Alors $\forall n \in \mathbb{N}^*$ et $\forall a \in A$, on a :*

$$1_A - a^n = (1_A - a) \left(\sum_{k=0}^{n-1} a^k \right).$$

Remarque. Attention, en général $ab = 0_A$ n'implique pas que $a = 0_A$ ou $b = 0_A$. Par exemple, dans l'anneau $(\mathcal{M}_2(\mathbb{R}), +, \times)$, si on considère les matrices $A = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$ et $B = \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}$, on a $A \times B = 0_2$ et pourtant ni A ni B sont des matrices nulles.

Cette dernière remarque amène à la définition suivante :

Définition 1.47. *Un anneau intègre $(A, +, \times)$ est un anneau non nul tel que $\forall (a, b) \in A^2$, $a \times b = 0_A \Longrightarrow a = 0_A$ ou $b = 0_A$.*

Exemples 1.48.

1. $(\mathbb{Z}, +, \times)$, $(\mathbb{Q}, +, \times)$, $(\mathbb{R}, +, \times)$ et $(\mathbb{C}, +, \times)$ sont des anneaux intègres.
2. $(\mathcal{M}_n(A), +, \times)$ est anneau non intègre pour $n \geq 2$ et où A est égal à $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ ou $\mathbb{C}$.

Proposition 1.49. *Soit $(A, +, \times)$ un anneau intègre. Pour tout a de A^* (i.e. $a \neq 0_A$) et tout (x, y) de A^2, on a :*

$$ax = ay \Rightarrow x = y \quad \text{et} \quad xa = ya \Rightarrow x = y.$$

Autrement dit, tout élément non nul d'un anneau intègre est simplifiable à gauche et à droite pour la multiplication.

Démonstration. Soient $a \in A^*$ et $(a, b) \in A^2$. On a :

$$ax = ay \Leftrightarrow ax - ay = 0 \Leftrightarrow a(x - y) = 0.$$

Puisque A est intègre et que $a \neq 0_A$, cela implique que $x - y = 0_A$ i.e. $x = y$. La deuxième implication se montre de la même manière. □

Remarque. Soient $(A, +, \times)$ un anneau et $(a, b) \in A^2$. On fera attention aux fautes usuelles suivantes :

$$\begin{aligned} a^2 = b^2 &\Leftrightarrow a^2 - b^2 = 0_A \\ &\Leftrightarrow (a - b)(a + b) = 0_A \quad \text{vrai que si } ab = ba \\ &\Leftrightarrow a = b \text{ ou } a = -b \quad \text{vrai que si } A \text{ est intègre.} \end{aligned}$$

1.3.3 Groupe des éléments inversibles d'un anneau

Définition 1.50. *Un élément a d'un anneau $(A, +, \times)$ est dit inversible, s'il possède un symétrique a^{-1} pour la l.c.i. $\times$:*

$$a^{-1} \in A \text{ et } a \times a^{-1} = a^{-1} \times a = 1_A.$$

On note $\mathcal{U}(A)$ l'ensemble de ces éléments inversibles.

Théorème 1.51. *Soit $(A+, \times)$ un anneau non non nul. L'ensemble $(\mathcal{U}(A), \times)$ est un groupe, appelé le groupe des inversibles de l'anneau A.*

Démonstration. Soit $(A+, \times)$ un anneau non nul. Montrons que $(\mathcal{U}(A), \times)$ est un groupe.

1. On commence par remarquer que $\times$ est bien une l.c.i. sur $\mathcal{U}(A)$ puisque le produit d'éléments inversibles est inversible d'après la proposition 1.19.
2. Puisque $\times$ est associative sur A, elle l'est en particulier sur $\mathcal{U}(A)$.
3. Le fait que $1_A \times 1_A = 1_A$ implique que 1_A est inversible et donc que $1_A \in \mathcal{U}(A)$.
4. Enfin, par définition de $\mathcal{U}(A)$, tout élément a de $\mathcal{U}(A)$ est inversible et son inverse a^{-1} appartient à $\mathcal{U}(A)$ puisque $(a^{-1})^{-1} = a$.

On a donc bien montré que $(\mathcal{U}(A), \times)$ est un groupe. □

Exemples 1.52.

1. Le groupe des éléments inversibles de $\mathbb{Z}$ est $(\{-1, 1\}, \times)$.
2. Le groupe des éléments inversibles de $\mathbb{Q}$ est $(\mathbb{Q}^*, \times)$.
3. Le groupe des éléments inversibles de $\mathbb{R}$ est $(\mathbb{R}^*, \times)$.
4. Le groupe des éléments inversibles de $\mathbb{C}$ est $(\mathbb{C}^*, \times)$.
5. Le groupe des inversibles de $\mathcal{A}(\mathbb{R}, \mathbb{R})$ est l'ensemble des fonctions qui ne s'annulent pas.

1.3.4 Corps

Définition 1.53. *On appelle corps, tout anneau $(\mathbb{K}, +, \times)$ non nul, tel que tout élément de $\mathbb{K}$ différent de $0_\mathbb{K}$ admet un inverse pour $\times$. Si de plus, $\times$ est commutative, $\mathbb{K}$ est dit corps commutatif.*

Remarque. Concrètement, il faut retenir que dans un corps, on peut inverser tous les éléments sauf 0.

Exemples 1.54.
1. $(\mathbb{Q}, +, \times)$, $(\mathbb{R}, +, \times)$ et $(\mathbb{C}, +, \times)$ sont des corps.
2. $(\mathbb{Z}, +, \times)$ n'est pas un corps car seuls -1 et 1 sont inversibles.

Théorème 1.55. *Tout corps commutatif est un anneau intègre.*

Démonstration. Soit $(\mathbb{K}, +, \times)$ un corps commutatif et soient $x, y \in \mathbb{K}$. On suppose que $xy = 0_\mathbb{K}$. On veut montrer que $x = 0_\mathbb{K}$ ou $y = 0_\mathbb{K}$. On traite deux cas :

1. Si $x \neq 0_\mathbb{K}$ alors x est inversible et son inverse x^{-1} est dans $\mathbb{K}$. On a donc $y = 1_\mathbb{K} \times y = x^{-1} \times x \times y = x^{-1} \times 0_\mathbb{K} = 0_\mathbb{K}$ car $0_\mathbb{K}$ est absorbant.
2. Sinon $x = 0_\mathbb{K}$.

Ainsi, dans tous les cas, x ou y est nul. □

Remarque. Attention, la réciproque est fausse ! $(\mathbb{Z}, +, \times)$ est un anneau intègre mais n'est pas un corps. En effet, seuls -1 et 1 sont inversibles dans cet anneau.

1.4 Étude des anneaux $(\mathbb{Z}/n\mathbb{Z}, +, \times)$ pour $n \in \mathbb{N}^*$

Soit n un entier naturel supérieur ou égal à 2. On rappelle que $n\mathbb{Z}$ désigne l'ensemble des multiples de n et que $(n\mathbb{Z}, +)$ est un sous-groupe de $(\mathbb{Z}, +)$.

Définition 1.56. *Si x et y sont dans $\mathbb{Z}$, on dit que x est congru à y modulo n si $x - y$ est divisible par n, i.e. si*

$$\exists k \in \mathbb{Z} \, : \, x - y = kn.$$

On écrit

$$x \equiv y \, [n] \quad (ou \; x \equiv y \; (mod \; n)).$$

Il est facile de vérifier que cette relation est une relation d'équivalence (i.e. réflexive, symétrique et transitive).

Exemples 1.57.
$125 \equiv 2 \, [3]$ car $125 - 2 = 123$ est un multiple de 3.
$-2 \equiv 1 \, [3]$ car $-2 - 1 = -3$ est un multiple de 3.

Proposition 1.58. *Deux entiers relatifs sont congrus modulo n si et seulement si ils ont le même reste dans leur division euclidienne par n.*

Démonstration. Soient x et y dans $\mathbb{Z}$. On effectue la division euclidienne de x et y par n :

$$x = nk_1 + r_1 \text{ où } (k_1, r_1) \in \mathbb{Z}^2 \text{ et } 0 \leq r_1 \leq n - 1$$
$$y = nk_2 + r_2 \text{ où } (k_2, r_2) \in \mathbb{Z}^2 \text{ et } 0 \leq r_2 \leq n - 1$$

On veut montrer que $x \equiv y \, [n] \Leftrightarrow r_1 = r_2$. On procède par double implication :

1. On suppose que $x \equiv y \, [n]$. Alors $x - y$ est un multiple de n. Puisque $x - y = n(k_1 - k_2) + r_1 - r_2$, on en déduit que $n(k_1 - k_2) + r_1 - r_2$ est un multiple de n et donc que $r_1 - r_2$ est aussi un multiple de n puisqu'il s'écrit comme la différence de deux éléments divisibles par n. Or $0 \leq r_1 \leq n - 1$ et $0 \leq r_2 \leq n - 1$ impliquent que $-(n - 1) \leq r_1 - r_2 \leq n - 1$. Le seul multiple de n compris entre $-(n - 1)$ et $n - 1$ est 0 donc $r_1 - r_2 = 0$ i.e. $r_1 = r_2$.
2. Réciproquement, on suppose que $r_1 = r_2$. Alors $x - y = n(k_1 - k_2)$ avec $k_1 - k_2 \in \mathbb{Z}$. Ainsi, $x \equiv y \, [n]$.

□

Définition 1.59. *Pour tout entier relatif x, on appelle classe de x modulo n, l'ensemble des entiers relatifs qui lui sont congrus modulo n. On la note $\overline{x}$:*

$$\overline{x} = \{y \in \mathbb{Z} : x \equiv y \, [n]\}.$$

Ainsi,

$$\forall (x,y) \in \mathbb{Z}^2, x \equiv y\ [n] \Leftrightarrow y \in \overline{x} \Leftrightarrow x \in \overline{y} \Leftrightarrow \overline{x} = \overline{y}.$$

Tout élément d'une classe peut être choisi comme représentant de celle-ci. Par exemple, modulo 4, $\overline{2} = \overline{-2} = \overline{54}$ car $2 = 4 \times 0 + 0$, $-2 = 4 \times 1 - 2$ et $54 = 4 \times 13 + 2$. D'après la proposition 1.58, $\overline{x}$ est l'ensemble des entiers relatifs qui ont le même reste que x dans leur division par n.

Proposition 1.60. *Soit $x \in \mathbb{Z}$. L'entier relatif x est congru modulo n à un unique entier naturel y tel que $0 \leq y \leq n-1$.*

Démonstration. C'est la preuve de la division euclidienne. □

Ainsi, lorsqu'on divise par n, il y a n restes possibles : $0, 1, \ldots, n-1$. On en déduit que $\{0, 1, \ldots, n-1\}$ forme une famille de représentants des classes distinctes modulo n et donc que tout entier relatif x appartient à une et une seule des classes (modulo n) : $\{\overline{0}, \overline{1}, \ldots, \overline{n-1}\}$

Définition 1.61. *On note*

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

C'est l'ensemble des classes distinctes modulo n.

Exemple 1.62. $\mathbb{Z}/3\mathbb{Z} = \{\overline{0}, \overline{1}, \overline{2}\}$ avec

$\overline{0} = \{3k : k \in \mathbb{Z}\}$: ensemble des multiples de 3.
$\overline{1} = \{3k+1 : k \in \mathbb{Z}\}$: ensemble des entiers relatifs de reste 1 dans la division euclidienne par 3.
$\overline{2} = \{3k+2 : k \in \mathbb{Z}\}$: ensemble des entiers relatifs de reste 2 dans la division euclidienne par 3.

Exemples 1.63. Dans $\mathbb{Z}/4\mathbb{Z}$:

1. $\mathbb{Z}/4\mathbb{Z} = \{\overline{0}, \overline{1}, \overline{2}, \overline{3}\}$.
2. Dire à quelle classe appartiennent les entiers relatifs suivants : 1, 4, 9, 12, 7, -3, -19, -15, -5. Il suffit d'effectuer la division euclidienne par

4 :

$$\begin{aligned}
1 \in \overline{1} \text{ car } 1 &= 4 \times 0 + \boxed{1} \\
4 \in \overline{0} \text{ car } 4 &= 4 \times 1 + \boxed{0} \\
9 \in \overline{1} \text{ car } 9 &= 4 \times 2 + \boxed{1} \\
12 \in \overline{0} \text{ car } 12 &= 4 \times 3 + \boxed{0} \\
7 \in \overline{3} \text{ car } 7 &= 4 \times 1 + \boxed{3} \\
-3 \in \overline{1} \text{ car } -3 &= 4 \times (-1) + \boxed{1} \\
-19 \in \overline{1} \text{ car } -19 &= 4 \times (-5) + \boxed{1} \\
-15 \in \overline{1} \text{ car } -15 &= 4 \times (-4) + \boxed{1} \\
-5 \in \overline{3} \text{ car } -5 &= 4 \times (-2) + \boxed{3}.
\end{aligned}$$

Opérations dans $\mathbb{Z}/n\mathbb{Z}$. On a déjà vu que l'ensemble des entiers relatifs $\mathbb{Z}$ peut-être muni de deux opérations : l'addition notée "+" et la multiplication notée ".". Nous souhaitons étendre de manière naturelle ces deux opérations à $\mathbb{Z}/n\mathbb{Z}$. Les deux propositions suivantes définissent la loi addition "+" et la loi multiplication "×" sur $\mathbb{Z}/n\mathbb{Z}$. Attention, nous gardons les mêmes notations pour l'addition sur les deux ensembles $\mathbb{Z}$ et $\mathbb{Z}/n\mathbb{Z}$.

Proposition 1.64. *L'application*

$$\begin{cases} (\mathbb{Z}/n\mathbb{Z})^2 & \longrightarrow \mathbb{Z}/n\mathbb{Z} \\ (\overline{x}, \overline{y}) & \longmapsto \overline{x} + \overline{y} = \overline{x+y} \end{cases}$$

est une loi de composition interne sur $\mathbb{Z}/n\mathbb{Z}$.

Démonstration. Il faut vérifier que le résultat est indépendant des représentants choisis. Soient, $x, x', y, y' \in \mathbb{Z}$ tels que $\overline{x} = \overline{x'}$ et $\overline{y} = \overline{y'}$, i.e. tels que

$$x \equiv x' \ [n] \quad \text{et} \quad y \equiv y' \ [n].$$

On veut montrer que $x + y \equiv x' + y' \ [n]$. Par hypothèse, il existe $k_1, k_2 \in \mathbb{Z}$ tels que $x - x' = nk_1$ et $y - y' = nk_2$. En additionnant ces deux égalités, on obtient que $(x + y) - (x' + y') = (k_1 + k_2)n$ où $k_1 + k_2 \in \mathbb{Z}$. Ainsi, on a bien $x + y \equiv x' + y' \ [n]$, i.e. $\overline{x + y} = \overline{x' + y'}$. □

Proposition 1.65. $(\mathbb{Z}/n\mathbb{Z}, +)$ *est un groupe commutatif à n éléments.*

Démonstration.

1. Le fait que $0 \in \mathbb{Z}$ est un élément neutre pour $+$ implique que $\forall x \in \mathbb{Z}$, $\overline{x} + \overline{0} = \overline{x + 0} = \overline{x}$ et de même pour $\overline{0} + \overline{x}$. Ainsi, $\overline{0}$ est l'élément neutre de $\mathbb{Z}/n\mathbb{Z}$ pour la loi $+$.
2. On montrerait de même l'associativité, la commutativité et l'existence d'un opposé ($\overline{-x}$ est l'opposé de $\overline{x}$).

3. Enfin, on a vu que $\mathbb{Z}/n\mathbb{Z}$ possède n éléments.

□

Proposition 1.66. *L'application*

$$\begin{cases} (\mathbb{Z}/n\mathbb{Z})^2 & \longrightarrow \mathbb{Z}/n\mathbb{Z} \\ (\overline{x}, \overline{y}) & \longmapsto \overline{x} \times \overline{y} = \overline{x.y} \end{cases}$$

est une loi de composition interne sur $\mathbb{Z}/n\mathbb{Z}$.

Démonstration. Comme pour l'addition, il faut vérifier que le résultat est indépendant des représentants choisis. Soient $x, x', y, y' \in \mathbb{Z}$ tels que $\overline{x} = \overline{x'}$ et $\overline{y} = \overline{y'}$ i.e. tels que

$$x \equiv x' \,[n] \quad \text{et} \quad y \equiv y' \,[n].$$

Il faut montrer que $x.y \equiv x'.y' \,[n]$. Par hypothèse, il existe $k_1, k_2 \in \mathbb{Z}$ tels que $x - x' = nk_1$ et $y - y' = nk_2$. On trouve que $x.y - x'.y' = (x - x')y + x'(y - y') = kn$ avec $k = k_1 y + k_2 x' \in \mathbb{Z}$ d'où $x.y \equiv x'.y' \,[n]$. On a montré que $\overline{x.y} = \overline{x'.y'}$. □

Proposition 1.67. $(\mathbb{Z}/n\mathbb{Z}, +, .)$ *est un anneau commutatif.*

Démonstration. Comme pour le groupe $(\mathbb{Z}/n\mathbb{Z}, +)$, toutes les propriétés (associativité, distributivité, éléments neutres, ...) se déduisent des lois correspondantes sur l'anneau commutatif $(\mathbb{Z}, +, \times)$. L'élément $\overline{1}$ est l'élément neutre pour . dans $\mathbb{Z}/n\mathbb{Z}$. □

Exemples 1.68.

1. Dans $\mathbb{Z}/5\mathbb{Z}$, $\overline{2} + \overline{4} = \overline{2+4} = \overline{6} = \overline{1}$ et $\overline{3} \times \overline{5} = \overline{3 \times 5} = \overline{15} = \overline{0}$.
2. Dans $\mathbb{Z}/6\mathbb{Z}$, $\overline{3} + \overline{5} = \overline{3+5} = \overline{8} = \overline{2}$ et $\overline{3} \times \overline{3} = \overline{3 \times 3} = \overline{9} = \overline{3}$.