Chapitre 3

Structures algébriques

3.1 Loi de composition interne (LCI)

Définition 3.1.
Soit E un ensemble non vide.

1. On appelle **loi de composition interne** sur E une application de $E \times E$ dans E. Si T désigne cette application, alors l'image du couple $(x, y) \in E \times E$ par T s'écrit xTy .
2. On appelle **ensemble structuré** tout couple (E, T) où E est un ensemble non vide et T une loi de composition interne sur E.

Exemple 3.1.
Les lois de compositions internes les plus courantes sont :

1. $+$ *dans* $\mathbb{N}, \mathbb{N}^*, \mathrm{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$. *et mais pas sur* $\mathrm{Z}^*, \mathbb{Q}^*, \mathbb{R}^*, \mathbb{C}^*$
2. $-$ *dans* $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$.
3. $\times$ *dans* $\mathbb{N}, \mathbb{N}^*, \mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$.
4. $/$ *dans* $\mathbb{Q}^*, \mathbb{R}^*, \mathbb{C}^*$.
5. 0 *(composition des applications) dans l'ensemble des applications de* E *dans* E.
6. *La loi* $\oplus$ *définie sur* $\mathbb{R}^2$ *par* $(x_1, y_1) \oplus (x_2, y_2) = (x_1 + x_2, y_1 + y_2)$.
7. *La loi* T *définie sur* $\mathbb{R}$ *par* $xTy = x + y - xy$.
8. *Les lois* $\cup$, $\cap$ *(union, intersection) définies sur* $P(E)$ *(ensemble des parties d'un ensemble* E*).*

Définition 3.2. (Propriétés des lois)
Soit (E, T) un ensemble structuré.

1. La loi T est dite **associative** sur E si $(xTy)Tz = xT(yTz)$ pour tous x, y, z appartenant à E.
2. La loi T est dite **commutative** sur E si $xTy = yTx$ pour tous x, y appartenant à E.

Exemple 3.2.
L'addition et la multiplication sont associatives et commutatives sur $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$.

Définition 3.3. (Propriétés des lois)
Soit (E, T) un ensemble structuré.

1. Un élément e de E est dit **neutre** pour la loi T si,

$$\forall x \in E,\ xTe = eTx = x.$$

.

2. Si (E, T) possède un élément neutre e alors un élément x de E est dit symétrisable pour la loi T s'il existe un élément x' de E tel que :

$$xTx' = x'Tx = e$$

.

L'élément x' est alors appelé élément symétrique de x pour la loi T.

Proposition 3.4.
Soit (E, T) un ensemble structuré. Si l'élément neutre de E pour la loi T existe, alors il est unique.

Démonstration. Supposons qu'ils existes deux éléments neutres e et e' alors $e' = eTe' = e$ d'où $e = e'$. □

Proposition 3.5.
Soit (E, T) un ensemble structuré pour lequel la loi T est associative et admet un élément neutre.

1. *Si $x \in E$ est symétrisable, alors son symétrique est unique.*
2. *Si $x \in E$ et $y \in E$ sont symétrisables alors xTy est symétrisable et son symétrique $(xTy)'$ est donné par $(xTy)' = y'Tx'$ où x' désigne le symétrique de x et y' celui de y.*

Démonstration.

1. Supposons qu'un éléments x a deux symétriques x' et x''. Alors $xTx' = e \Rightarrow x''T(xTx') = x'' \Rightarrow (x''Tx)Tx' = x'' \Rightarrow x' = x''$.
2. On a
$$(y'Tx')T(xTy) = y'T(x'Tx)Ty = y'Ty = e.$$
D'autre part
$$(xTy)T(y'Tx') = xT(yTy')Tx' = xTx' = e.$$
D'où $(xTy)' = y'Tx'$.

□

3.2 Groupes

3.2.1 Structure de groupe

Définition 3.6.
Soit (G, T) un ensemble structuré.

1. On dit que (G, T) est un **groupe** si
   (a) la loi T est associative sur G,
   (b) il existe un élément neutre pour la loi T dans G,
   (c) tout élément de G est symétrisable pour la loi T.

   On dit aussi que l'ensemble G possède une **structure de groupe** pour la loi T.
2. On dit que le groupe (G, T) est **commutatif (ou abélien)** si la loi T est commutative sur G.

Exemple 3.3.
On fournit d'abord des exemples de groupes

1. $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ *munis de la somme.*
2. $\mathbb{Z}^*$, $\mathbb{Q}^*$, $\mathbb{R}^*$ *munis du produit.*

Exemple 3.4.
Pour diverses raisons (à déterminer), les couples suivants ne sont pas des groupes :

1. $(\mathbb{N}, +)$, $(\mathbb{R}, \times)$.
2. $(\mathcal{P}(E), \cup)$, $(\mathcal{P}(E), \cap)$.

3.2.2 Les sous groupe

Définition 3.7. (Sous groupes)
Un **sous-groupe** d'un groupe $(G, *)$ est une partie non vide H de G telle que :

1. $*$ induit sur H une loi de composition interne.
2. Muni de cette loi, H est un groupe. On note alors : $H < G$.

Proposition 3.8.
*L'ensemble $H \subset G$ est un **sous-groupe** d'un groupe $(G, *)$ si et seulement si*

1. $H \neq \varnothing$,
2. $\forall (x, y) \in H^2,\ x * y \in H$,
3. $\forall x \in H,\ x' \in H$.

Exemple 3.5.

1. *Soit $(G, *)$ un groupe. Alors G et $\{e_G\}$ sont des sous groupes de G.*
2. *$(\mathbb{Z}, +)$ est un sous groupe de $(\mathbb{R}, +)$.*

Proposition 3.9.
L'ensemble $H \subset G$ est un sous-groupe d'un groupe $(G, *)$ si et seulement si

1. $H \neq \varnothing$,
2. $\forall (x, y) \in H^2,\ x * y' \in H$,

Proposition 3.10.
L'intersection quelconque de sous groupes d'un groupe $(G, *)$ est un sous groupe de $(G, *)$.

Démonstration.
Soit donc (H_i) $i \in I$ une famille de sous groupes d'un groupe G . Posons $K = \bigcap_{i \in I} H_i$ l'intersection de tous les H_i. L'ensemble K est non-vide, car il contient le neutre e puisque celui-ci appartient à chacun des sous-groupes H_i. Soient x et y deux éléments de K. Pour tout $i \in I$, on a $x * y' \in H_i$ puisque H_i est un sous-groupe. Donc $x * y' \in K$. Ce qui prouve que K est un sous-groupe de G. □

Remarque 3.11.
L'union quelconque de sous groupes d'un groupe $(G, *)$, n'est pas nécessairement un sous groupe de $(G, *)$.

Exemple 3.6.
Soit T la loi de composition intèrne défini sur $\mathbb{R}^2$ par

$$\forall (x_1, y_1), (x_2, y_2) \in \mathbb{R}^2, \quad (x_1, y_1)T(x_2, y_2) = (x_1 + x_2, y_1 + y_2).$$

On a $(\mathbb{R}^2, T)$ est un groupe, $\mathbb{R} \times \{0\}$ et $\{0\} \times \mathbb{R}$ sont deux sous groupes de $(\mathbb{R}^2, T)$ mais $\mathbb{R} \times \{0\} \bigcup \{0\} \times \mathbb{R}$ ne forme pas un sous-groupe de $(\mathbb{R}^2, T)$.

Proposition 3.12.
L'union de deux sous-groupes H et K d'un même groupe $(G, *)$,est un sous-groupe $(H \cup K < G)$ si, et seulement si, $H \subset K$ ou $K \subset H$.

Démonstration.
Supposons que $H \cup K$ soit un sous-groupe de G et que H ne soit pas inclus dans K, c'est-à-dire, qu'il existe $h \in H$ tel que $h \notin K$. Montrons que $K \subset H$. Soit $k \in K$ quelconque. On a $h * k \in H \cap K$. Mais $h * k \notin K$ car sinon $h = (h * k) * k' \in K$. D'où $h * k \in H$ et donc $k = h' * (h * k) \in H$. □

3.2.3 Exemples de groupes

3.2.3.1 Le groupe $\mathbb{Z}/n\mathbb{Z}$

Il est d'abord clair que si n est un entier que l'on peut supposer positif et non nul, l'ensemble $n\mathbb{Z}$ des entiers relatifs de la forme nk, k décrivant $\mathbb{Z}$ (ensemble des multiples de n), est un sous-groupe additif de $(\mathbb{Z}, +)$.

Proposition 3.13.
Tout sous-groupe de $(\mathbb{Z}, +)$ est de la forme $n\mathbb{Z}$.

Démonstration. Soit S un sous-groupe de $\mathbb{Z}$ autre que $\{0\}$ et $\mathbb{Z}$. S ne contient donc pas 1. L'ensemble des entiers positifs de S, noté S^+, admet un plus petit élément n au moins égal à 2 (ensemble dénombrable, borné inférieurement). Tout élément de $\mathbb{Z}$ de la forme kn, k entier naturel, est un élément de S (évident par récurrence car $kn = n + n + ... + n$). Donc S contient $n\mathbb{Z}$. Par division euclidienne, tout entier de S^+ qui n'est pas de la forme kn s'écrit $a = kn + r$, $0 < r < n$. On

a alors $r = a - kn > 0$. Mais a et kn sont dans S^+, donc r aussi. Voilà un entier de S strictement plus petit que son plus petit élément (Pas possible), donc $r = 0$. Ce qui montre que $S = n\mathbb{Z}$. □

On montre très facilement que la relation de congruence modulo n, $n \in \mathbb{N}$, due à Gauss notée $\equiv$ définit par :

$$\forall x, y \in \mathbb{Z} \quad x \equiv y[n] \Leftrightarrow \quad (x - y) \in n\mathbb{Z} \Leftrightarrow \quad \exists k \in \mathbb{N}/ \quad y = x - nk.$$

($x \equiv y[n]$ on lit « x est congru à y modulo n » est une relation d'équivalence définie dans $(Z, +)$. L'ensemble quotient est fini et peut ainsi s'écrire :

$$\mathbb{Z}/n\mathbb{Z} = \{\dot{0}, \dot{1}, ..., \widehat{n-1}\}.$$

Par exemples : $\mathbb{Z}/2\mathbb{Z} = \{\dot{0}, \dot{1}\}$, $\mathbb{Z}/3\mathbb{Z} = \{\dot{0}, \dot{1}, \dot{2}\}$, $\mathbb{Z}/4\mathbb{Z} = \{\dot{0}, \dot{1}, \dot{2}, \dot{3}\}$ et $\mathbb{Z}/6\mathbb{Z} = \{\dot{0}, \dot{1}, \dot{2}, \dot{3}, \dot{4}, \dot{5}\}$.

• L'addition quotient sur $\mathbb{Z}/n\mathbb{Z}$ induite par celle de $\mathbb{Z}$, est :

$$\forall x, y \in \mathbb{Z}/n\mathbb{Z} \quad \dot{x} + \dot{y} = \widehat{x + y}.$$

• La multiplication quotient sur $\mathbb{Z}/n\mathbb{Z}$ induite par celle de $\mathbb{Z}$, est :

$$\forall x, y \in \mathbb{Z}/n\mathbb{Z} \quad \dot{x} \times \dot{y} = \widehat{x \times y}.$$

Proposition 3.14.
L'ensemble $(\mathbb{Z}/n\mathbb{Z}, \dot{+})$ est un groupe additif commutatif (groupe quotient de $\mathbb{Z}$ par la relation de congruence).

Démonstration. Laisser au lecteur. □

3.2.3.2 Groupe de permutation

Définition 3.15.
Soit E un ensemble. Une permutation de E est une bijection de E dans E. On note S_E l'ensemble des permutations de E. Si $E = \{1, ..., n\}$ on le note simplement S_n. L'ensemble S_E muni de la loi de composition des applications est un groupe de neutre $e = id$ appelé groupe symétrique sur l'ensemble E.

Exemple 3.7.
Supposons $E = \{1, 2, 3, 4, 5\}$ *on notera une permutation* $\sigma \in S_5$ *de la manière suivante :*

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 5 & 2 & 1 & 4 \end{pmatrix}$$

qui se traduit par $\sigma(1) = 3$, $\sigma(2) = 5$ *et ainsi de suite.*

3.2.4 Homomorphismes de groupes

Définition 3.16. (Homomorphismes de groupes)
Soient $(G, *)$ et (H, T) deux groupes. Une application f de G dans H est un **Homomorphisme de groupes** lorsque :

$$\forall x,\ y \in G, \quad f(x * y) = f(x) T f(y).$$

De plus

1. Si $G = H$ et $* = T$, on parle **d'endomorphisme**.
2. Si f est bijective, on parle **d'isomorphisme**.
3. Si f est un endomorphisme bijectif, on parle **d'automorphisme**.

Exemple 3.8.
$x \longmapsto 2x$ *réalise un automorphisme de* $(R, +)$.

Exemple 3.9.
L'application $f : \mathbb{R} \to \mathbb{R}_+^*$ *qui à tout nombre réel associe son exponentielle est un morphisme de groupes de* $\mathbb{R}$ *muni de l'addition dans* $\mathbb{R}_+^*$ *muni de la multiplication, car :* $\exp(x + y) = \exp(x).\exp(y)$, *pour tous* $x, y \in \mathbb{R}$.

Proposition 3.17. *(Quelques propriétés élémentaires des Homomorphismes de groupes)*
Soit f *un Homomorphisme de* $(G, *)$ *dans* (H, T)

1. $f(e_G) = e_H$.
2. $\forall x \in G \quad f(x') = (f(x))'$ *(*x' *est le symétrique de* x *dans* G *et* $(f(x))'$ *est le symétrique de* $f(x)$ *dans* H*)*
3. *Si* f *est un isomorphisme, alors son application réciproque* f^{-1} *réalise un isomorphisme de* (H, T) *sur* $(G, *)$.
4. *Si* $G' < G$, *alors* $f(G') < H$.

5. *Si* $H' < H$, *alors* $f^{-1}(H') < G$.

Démonstration.

1. $f(e_G * e_G) = f(e_G)$ alors $f(e_G)Tf(e_G) = f(e_G)$ ce qui montre, en composant à droite par $(f(e_G))'$, que $f(e_G) = e_H$.
2. Soit $x \in G$,
$$f(x')Tf(x) = f(x' * x) = f(e_G) = e_H.$$
D'autre part
$$f(x)Tf(x') = f(x * x') = f(e_G) = e_H.$$
D'où $f(x') = (f(x))'$.
3. Soient y_1 et y_2 deux éléments quelconques de H. Posons $x_1 = f^{-1}(y_1)$ et $x_2 = f^{-1}(y_2)$. Parce que f est un morphisme de groupes, on a $f(x_1 * x_2) = f(x_1)Tf(x_2)$, donc $f(x_1 * x_2) = y_1 T y_2$, d'où $x_1 * x_2 = f^{-1}(y_1 T y_2)$, c'est-à-dire $f^{-1}(y_1) * f^{-1}(y_2) = f^{-1}(y_1 T y_2)$. Ceci prouve que f^{-1} est un morphisme de groupes de H sur G, ce qui achève la preuve.
4. Laisser au lecteur.
5. Considérons un sous-groupe H' de H, posons $G' = f^{-1}(H')$, et montrons que G' est un sous groupe de G. Comme $f(e_G) = e_H$ d'après (1) et que $e_H \in H'$ puisque H' est un sous groupe de H, on a $e_G \in G'$, donc G' n'est pas vide. Soient x et y deux éléments quelconques de G'. On a donc $f(x) \in H'$ et $f(y) \in H'$, d'où $f(x)T(f(y))' \in H'$ car H' est un sous groupe de H. Alors $f(x * y') \in H'$. On conclut que $(x * y') \in G'$, ce qui prouve le résultat voulu.

□

Définition 3.18.
Soit f un Homomorphisme de G dans H.

1. Le noyau de f, noté $Ker(f)$ est l'ensemble des antécédents par f de e_H :
$$Ker(f) = \{x \in G, \quad f(x) = e_H\} = f^{-1}\{e_H\}$$
(attention, f n'est pas supposée bijective ; il n'est donc pas question de la bijection réciproque de f).
2. L'image de f, noté $Im(f)$ est $f(G)$ (ensemble des images par f des éléments de G).

Remarque 3.19.
D'après les deux derniers points de la proposition (3.17), le noyau et l'image de f sont des sous-groupes respectifs de G et H.

Proposition 3.20.
Soit f un Homomorphisme de $(G, *)$ dans (H, T).

1. *f est surjective si et seulement si $Im(f) = H$.*
2. *f est injectif si et seulement si $Ker(f) = \{e_G\}$.*

Démonstration.
Le point (1) est immédiat par définition même de la surjectivité. Pour montrer le (2), supposons d'abord que f est injective. Soit $x \in Ker(f)$. On a $f(x) = e_H$, et puisque $f(e_G) = e_H$ comme on déduit que $f(x) = f(e)$, qui implique $x = e_G$ par injectivité de f. On conclut que $Ker(f) = \{e_G\}$. Réciproquement, supposons que $Ker(f) = \{e_G\}$ et montrons que f est injective. Pour cela , considérons $x, y \in G$ tels que $f(x) = f(y)$. On a alors $f(x)Tf(y)' = e_H$, donc $f(x * y') = e_H$, c'est-à-dire $x * y' \in Ker(f)$. L'hypothèse $Ker(f) = \{e_G\}$ implique alors $x * y' = e_G$, d'où $x = y$. L'injectivité de f est ainsi montrée, ce qui achève la preuve. □

3.3 Structure d'anneaux

Définition 3.21.
Un anneau est un ensemble muni de deux LCI $(A, *, T)$ tels que :

1. $(A, *)$ est un groupe commutatif d'élément neutre noté 0_A.
2. La loi T est une LCI sur A associative et distributive à gauche et à droite par rapport à $*$:

$$\forall x,\ y,\ z \in A, \qquad xT(y * z) = xTy * xTz \ \ et \ \ (x * y)Tz = xTz * yTz.$$

3. La loi T admet un élément neutre différent de 0_A, noté 1_A.

Exemple 3.10.
$(\mathbb{Z}, +, \times)$, $(\mathbb{Q}, +, \times)$, $(\mathbb{R}, +, \times)$ et $(\mathbb{C}, +, \times)$ sont des anneaux bien connus.

Remarque 3.22.

1. Si la loi T est commutative, l'anneau est dit commutatif ou abélien.

2. L'ensemble $A - \{0_A\}$ est noté A^*.
3. Par souci de simplification, nous laissons de côté (provisoirement) les notations T et $*$ des deux lois internes définies sur A au profit des notations additive ($+$) et multiplicative ($\times$). Donc on dit l'anneau $(A, +, \times)$ au lieu de $(A, *, T)$.

Définition 3.23.

1. Un anneau commutatif $(A, +, \times)$ est dit **intègre** s'il est
   (a) différent de l'anneau nul (autrement dit : si $1_A \neq 0_A$),
   (b) $\forall (x, y) \in A^2, \quad x \times y = 0 \quad \Rightarrow \quad (x = 0 \ \ ou \ \ b = 0)$.
2. Lorsqu'un produit $a \times b$ est nul alors que ni a, ni b ne le sont, on dit que a et b sont des diviseurs de zéro.

Exemple 3.11.

1. $(\mathbb{Z}, +, \times)$ *des entiers relatifs est intègre : il ne possède aucun diviseur de zéro.*
2. *L'anneau* $\mathbb{Z}/6\mathbb{Z}$ *des classes résiduelles modulo* 6 *n'est pas intègre puisque* $\overset{\bullet}{2} \times \overset{\bullet}{3} = \overset{\bullet}{6}$, *donc* $\overset{\bullet}{2} \times \overset{\bullet}{3} = \overset{\bullet}{0}$. *De même* $\mathbb{Z}/4\mathbb{Z}$.

Proposition 3.24.
Soit $(A, +, \times)$ *un anneau. Les règles de calcul dans les anneaux sont les suivantes :*

1. $x \times 0_A = 0_A \times x = 0_A$. *L'élément* 0_A *est alors dit absorbant pour la loi* $\times$).
2. $\forall (x, y) \in A^2, \quad (-x) \times y = x \times (-y) = -(x \times y)$.
3. $\forall x \in A, \quad (-1_A) \times x = -x$.
4. $\forall (x, y) \in A^2, \quad (-x) \times (-y) = x \times y$.
5. $\forall (x, y, z) \in A^3, \quad x \times (y - z) = x \times y - x \times z$ *et* $(y - z) \times x = y \times x - z \times x$.

Démonstration.

1. $x \times 0_A = x \times (0_A + 0_A) = x \times 0_A + x \times 0_A$. D'où par régularité des éléments dans le groupe $(A, +)$, $x \times 0_A = 0_A$. De même de l'autre côté.
2. $x \times y + (-x) \times y = (x + (-x)) \times y = 0_A \times y = 0_A$. D'où $(-x) \times y = -(x \times y)$. De même pour l'autre égalité.
3. $(-1_A) \times x + x = (-1_A) \times x + 1_A \times x = (-1_A + 1_A) \times x = 0_A \times x = 0_A$. Doù $(-1_A) \times x = -x$.

4. Laisser au lecteur.
5. Laisser au lecteur.

□

Notations et conventions

Soit $(A, *, T)$ un anneau. Soient n un entier naturel non nul et x un élément de A.

1. On note nx l'élément de A qui est égal à la composition par la première loi $*$ de n termes égaux à x. Autrement dit, pour tous $n \in \mathbb{N}^*$ et $x \in A$,

$$nx = \underbrace{x * x * ... * x}_{\text{n termes}}.$$

   En particulier, en prenant $n = 1$, on a : $1x = x$ pour tout $x \in A$.

2. De même, on note x^n l'élément de A qui est égal à la composition par la seconde loi T de n termes égaux à x. Autrement dit, pour tous $n \in \mathbb{N}^*$ et $x \in A$,

$$x^n = \underbrace{xTxT...Tx}_{\text{n termes}}.$$

   En particulier, en prenant $n = 1$, on a : $x^1 = x$ pour tout $x \in A$.

3. Et pour $n = 0$? Désignons par 0_A l'élément zéro et par 1_A l'élément unité de $(A, *, T)$ (cette notation est ici un peu malheureuse car elle rappelle la notation additive et la notation multiplicative que nous essayons justement d'éviter). Alors, par convention, pour tout $x \in A$, $0x = 0_A$ et $x^0 = 1_A$.

3.3.1 Sous-anneaux

Définition 3.25.

Soit $(A, *, T)$ un anneau. Une partie non vide A_1 de A est un **sous-anneau** de A lorsque :

1. $1_A \in A_1$;
2. les lois $*$ et T induisent des LCI sur A_1, et, muni de ces lois, $(A_1, *, T)$ est un anneau.

Proposition 3.26.

Une partie A_1 de A est un sous-anneau si et seulement si

1. *$(A_1, *)$ est un sous-groupe de $(A, *)$;*
2. *$1_A \in A_1$;*

3. $\forall (x,y) \in A_1^2 \quad xTy \in A_1$ *(*T *induit une LCI sur* A_1*).*

Exemple 3.12.
$(\mathbb{Z},\ *,\ T)$ *est un sous anneau de* $(\mathbb{Q},\ *,\ T)$ *qui est un sous anneau de* $(\mathbb{R},\ *,\ T)$ *qui est un sous anneau de* $(\mathbb{C},\ *,\ T)$

3.3.2 Homomorphismes d'anneaux

Définition 3.27.
Soient $(A, +_A, \times_A)$ et $(B, +_B, \times_B)$ deux anneaux. Un homomorphisme d'anneaux de A vers B est une application de A vers B telle que :

1. $f(1_A) = 1_B$;
2. pour tout $x,\ y \in A,\ \ f(x +_A y) = f(x) +_B f(y)$ *et* $f(x \times_A y) = f(x) \times_B f(y)$.

3.3.3 Idéaux d'un anneau commutatif

Soit $(A, +, \times)$ un anneau commutatif

Définition 3.28. (Idéal)
Une partie I de A est un idéal d'un anneau $(A, +, \times)$ si

1. $(I, +)$ est un sous-groupes de $(A, +)$,
2. Pour tout $a \in A$, on a $aI \subset I$. En d'autres termes $\forall a \in A, \forall x \in I : ax \in I$.

Proposition 3.29.
Une partie I *de* A *est un idéal d'un anneau* $(A, +, \times)$ *ssi*

1. I *contient l'élément zéro* 0_A*,*
2. pour tous $x, y \in I : x - y \in I$*,*
3. $\forall a \in A, \forall x \in I : ax \in I$.

Exemple 3.13.

1. *Tout anneau non trivial a au moins deux idéaux, l'idéal trivial* $\{0\}$ *et* A *lui-même. Les idéaux de* A *distincts de* A *sont dits propres.*
2. *Tout élément* x *de* A *permet de définir un idéal principal :*

$$< x >= xA = \{ax / a \in A\}.$$

C'est le plus petit idéal qui contient a*, on dit qu'il est engendré par* a*. Si* a *est inversible (et seulement dans ce cas),* $aA = A$.

3. *Plus généralement, si* $x_1, ..., x_n \in A$, *le plus petit idéal contenant* $x_1, ..., x_n$ *est :*

$$< x_1, ..., x_n >= x_1A + ... + x_nA = \{a_1x_1 + ... + a_nx_n / a_1, ..., a_n \in A\}.$$

En effet, on vérifie immédiatement que $I = x_1A + ... + x_nA$ *est non vide et stable par combinaisons linéaires, donc est un idéal; et bien entendu, tout idéal contenant les* x_i *doit contenir* I. *On dit que* I *est engendré par* $\{x_1, ..., x_n\}$.

3.4 Structure de corps

Définition 3.30. Corps

1. **Un corps** est un anneau commutatif dans lequel tout élément non nul est inversible.
2. Si, de plus, la seconde loi $\times$ est commutative sur K alors on dit que le corps $(K, +, \times)$ est commutatif.

Exemple 3.14.
$(\mathbb{Q},\ +,\ \times)$ *et* $(\mathbb{R},\ +,\ \times)$ *sont des corps commutatif.*

Définition 3.31. Sous corps
Soit $(K, +, \times)$ un corps et soit K_1 un sous partie non vide de K.
On dit que K_1 est **un sous corps** de K si K_1 est stable pour $+$ et $\times$ de K et K_1 muni des lois induites par celles de K est lui-même un corps

Exemple 3.15.
$(\mathbb{Q},\ +,\ \times)$ *et un sous corps de*$(\mathbb{R},\ +,\ \times)$.

Proposition 3.32.
Soit $(K, +, \times)$. *Un sous partie* K_1 *de* K *est un sous corps si et seulement si*

1. $(K_1, +)$ *soit un sous-groupe de* K,
2. *pour tous* x *et* y *de* K_1, $x \times y \in K_1$ *(stabilité de* K_1 *pour la loi* $\times$*),*
3. K_1 *contient l'élément unité de* K *et l'inverse de tout* x *de* K_1 *dans* $(K, \times)$ *est élément de* K_1.

3.5 Exercices

Exercice 3.33.
On considère sur $\mathbb{R}$ *la loi de composition* $*$ *définie par* $x * y = x + y - xy$. *Cette loi est-elle associative, commutative ? Admet-elle un élément neutre ? Un réel* x *admet-il un inverse pour cette loi ? Donner une formule pour la puissance* $n-ime$ *d'un élément* x *pour cette loi.*

Exercice 3.34.
Soit $*$ *la loi définie sur* $\mathbb{R}$ *par* $x * y = x \times y + (x^2 - 1) \times (y^2 - 1)$. *avec* $+$ *et* $\times$ *les opérations usuelles sur* $\mathbb{R}$.

1. *La loi* $*$ *est-elle associative sur* $\mathbb{R}$ *? Commutative sur* $\mathbb{R}$ *? Vérifier que* $\mathbb{R}$ *possède un élément neutre pour la loi* $*$. *Cette loi confère-t-elle à* $\mathbb{R}$. *une structure de groupe ?*
2. *Calculer le(s) symétrique(s) du réel* 2 *pour la loi* $*$.
3. *Résoudre les équations suivantes :* $2 * x = 2, \quad 2 * x = 5$.

Exercice 3.35.
Soit G *un ensemble muni d'une loi de composition interne* $*$ *associative, qui possède un élément neutre à droite* e *(i.e.* $\forall x \in E, \ \ x * e = x$*) et tel que tout élément* x *possède un inverse à droite* x' *(ie* $x * x' = e$*).*
Montrer que G *est un groupe.*

Exercice 3.36.

1. *Soient* H_1 *et* H_2 *deux sous-groupes de* $(G, *)$. *Montrer que* $H_1 \cap H_2$ *est également un sous groupe. de* G.
2. *Posons* $C_G = \{x \in G \mid \forall y \in G, \quad x * y = y * x\}$. *Montrer que* G *est un sous groupe de* G *(*C_G *est dit centre de groupe* G*).*
3. *Soit* $(G, \ *)$ *un groupe commutatif d'élément neutre* e. *On pose* $B = \{x \in G, \exists n \in \mathrm{N}^* : x^n = e\}$. *Montrer que* B *est un sous-groupe de* G.

Exercice 3.37.
Soit $(G, .)$ *un groupe non commutatif d'élément neutre* e. *Pour* $a \in G$, *on définit une application* f_a *par*

$$f_a : G \to G$$

$$x \ \mapsto f_a(x) = a * x * a^{-1}$$