Chapitre premier
Structures algébriques

Précisons tout d'abord quelques notations qui seront utilisées tout au long de cet ouvrage :
$\mathbb{N}$ désigne l'ensemble des entiers naturels, $\mathbb{N}^*$ l'ensemble des entiers naturels non nuls.
$\mathbb{Z}$ désigne l'ensemble des entiers relatifs, $\mathbb{Z}^*$ l'ensemble des entiers relatifs non nuls.
$\mathbb{Q}$ désigne l'ensemble des rationnels, $\mathbb{Q}^*$ l'ensemble des rationnels non nuls.
$\mathbb{R}$ désigne l'ensemble des réels, $\mathbb{R}^*$ l'ensemble des réels non nuls.
$\mathbb{C}$ désigne l'ensemble des complexes, $\mathbb{C}^*$ l'ensemble des complexes non nuls.
Nous allons rappeler les définitions et les principales propriétés des structures algébriques que nous utiliserons dans cet ouvrage.

1. Groupes

La première structure algébrique que nous allons définir est celle de groupe.

1.1. Définition. — *On appelle groupe un ensemble G muni d'une loi de composition interne notée $*$ associative, qui possède un élément neutre noté e c'est-à-dire que*

$$\forall x \in G,\ x * e = e * x = x$$

et pour laquelle tout élément est symétrisable c'est-à-dire que

$$\forall x \in G,\ \exists y \in G\,,\ x * y = y * x = e\,.$$

Si, de plus, la loi est commutative, le groupe est commutatif ou abélien. Par exemple, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ sont des groupes additifs abéliens, $\mathbb{Z}^*$,$\mathbb{Q}^*$,$\mathbb{R}^*$,$\mathbb{C}^*$ sont des groupes multiplicatifs abéliens.
Si un groupe G a un nombre fini d'éléments, il est dit fini et son ordre est le nombre de ses éléments.

1.2. Proposition. — *Soit G un groupe.*
1. Son élément neutre est unique et tout élément de G a un unique symétrique.
2. Pour tout $x \in G$, le symétrique du symétrique de x est x.
3. Si x' (resp. y') désigne le symétrique de x (resp. y), le symétrique de $x * y$ est $y' * x'$.
4. Pour tout $(a, b) \in G^2$, l'équation $a * x = b$ a une solution unique dans G.

1.3. Définition. — *On appelle sous-groupe d'un groupe G, toute partie H de G non vide, stable pour la loi $*$, qui est elle-même un groupe pour la loi induite sur H par la loi de G.*
Par exemple, pour tout entier relatif n, $n\mathbb{Z}$ est un sous-groupe de $\mathbb{Z}$. Nous verrons en exercice que tout sous-groupe de $\mathbb{Z}$ est de la forme $n\mathbb{Z}$, où n est un élément de $\mathbb{N}$.

Si G est un groupe dont l'élément neutre est e, G et $\{e\}$ sont deux sous-groupes de G. Tout sous-groupe de G, distinct de G et $\{e\}$ est appelé sous-groupe propre de G.

1.4. Proposition. — *Soit G un groupe.*
1. Soit H une partie non vide de G ; H est un sous-groupe de G si, pour tout (x, y) appartenant à H^2, $x * y'$ appartient à H où y' désigne le symétrique de y.
2. Si H et H' sont deux sous-groupes de G, $H \cap H'$ est un sous-groupe de G.
3. Si A est une partie non vide de G, il existe un plus petit sous-groupe de G contenant A : c'est l'intersection de tous les sous-groupes de G contenant A. Ce sous-groupe est appelé sous-groupe engendré par A.

Si le sous-groupe engendré par A est G tout entier, on dit que A est une partie génératrice de G. Si A contient un seul élément, a, le groupe engendré par A est dit monogène et nous le noterons $< a >$. Un groupe monogène est toujours abélien. Si un groupe est monogène et fini, il est dit cyclique.

Remarquons que, si G et G' sont deux groupes munis respectivement des lois $*$ et $\circ$, d'éléments neutres e et e', le produit

$$G \times G' = \{(a, b) \ ; \quad a \in G, b \in G'\}$$

peut être muni d'une structure de groupe en définissant la loi de composition, notée $\otimes$ par

$$(a, b) \oplus (c, d) = (a * c, b \circ d)\,,$$

l'élément neutre étant (e, e'). Par exemple $\mathbb{Z}^n$ est un groupe.

1.5. Définition. — *Soit G et G' deux groupes munis respectivement des lois $*$ et $\circ$, d'éléments neutres e et e' et f une application de G dans G'. On dit que f est un homomorphisme de groupes si*

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

Si f est une bijection, f est un isomorphisme de groupes ; un homomorphisme de G dans lui-même est un endomorphisme de G et un isomorphisme de G dans lui-même est un automorphisme de G.

Par exemple, si a est un élément fixé d'un groupe G et si a' désigne le symétrique de a, l'application f de G dans G définie par

$$\forall x \in G\,,\ f(x) = a * x * a',$$

est un automorphisme de G appelé *automorphisme intérieur*.

1.6. Proposition. — *Soit G et G' deux groupes munis respectivement des lois $*$ et $\circ$, d'éléments neutres e et e' et f un homomorphisme de G dans G'. Alors*
1. $f(e) = e'$.
2. L'image du symétrique d'un élément est le symétrique de l'image de cet élément.
3. $f(G)$ est un sous-groupe de G'.
4. L'ensemble

$$\ker f = \{x \ \ ; \ \ x \in G, f(x) = e'\}$$

est un sous-groupe de G appelé noyau de l'homomorphisme f.
5. Si f est un isomorphisme de G sur G', f^{-1} est un isomorphisme de G' sur G.

La démonstration de cette proposition est laissée en exercice.

1.7. Classes suivant un sous-groupe

Soit G un groupe que nous supposerons multiplicatif pour simplifier les notations ; nous noterons e son élément neutre et x^{-1} le symétrique de x.

Soit H un sous-groupe de G. On vérifie facilement que la relation $x^{-1}y \in H$ est une relation d'équivalence sur G. En outre, cette relation d'équivalence est compatible à gauche avec la loi de groupe de G, c'est-à-dire que, quels que soient les éléments x, y, z de G, la relation $x^{-1}y \in H$ entraîne que $(zx)^{-1}(zy) \in H$.

La classe de x modulo cette relation d'équivalence est l'ensemble des xz lorsque z décrit H ; nous la noterons xH et nous l'appellerons *classe à gauche modulo le sous-groupe* H.

De la même façon, nous pouvons définir sur G la relation d'équivalence $yx^{-1} \in H$ qui est compatible à droite avec la loi de groupe de G. La classe de x est alors Hx appelée *classe à droite modulo le sous-groupe* H.

a) *Sous-groupe distingué d'un groupe*

En général, les relations $x^{-1}y \in H$ et $yx^{-1} \in H$ sont distinctes ; pour qu'elles coïncident, il faut que les partitions qu'elles définissent sur G soient identiques, c'est-à-dire que pour tout $x \in G$, les classes xH et Hx soient égales. Cela peut encore se traduire par l'égalité $H = x^{-1}Hx$. Un tel sous-groupe H est appelé *sous-groupe distingué* de G ou encore *sous-groupe invariant* de G. Ce qualificatif d'invariant est justifié par le fait qu'alors H est invariant par tous les automorphismes intérieurs de G.

Dans un groupe G, il existe toujours des sous-groupes distingués, par exemple $\{e\}$ et G. Si G est abélien, tout sous-groupe de G est distingué.

Si H est un sous-groupe distingué de G, l'ensemble quotient G/H est l'ensemble des classes d'équivalence modulo H, sans préciser à droite ou à gauche puisque ce sont les mêmes et il peut être muni d'une structure de groupe en définissant le composé de la classe de x et de la classe de y comme la classe de xy.

Le groupe G/H est appelé *groupe quotient* et l'application de G dans G/H qui à un élément x de G associe sa classe modulo H est un homomorphisme surjectif, appelé *homomorphisme canonique* de G sur G/H.

Remarquons que si G est un groupe abélien et si H est un sous-groupe de G, le groupe quotient G/H est aussi abélien.

b) *Décomposition canonique d'un homomorphisme de groupes*

Soit G et G' deux groupes notés tous les deux multiplicativement, e et e' leurs éléments neutres et f un homomorphisme de G dans G'. Soit N le noyau de f ; il est facile de vérifier que N est un sous-groupe distingué de G.

Soit g l'homomorphisme canonique de G sur G/N. Nous pouvons définir une application h de G/N dans $f(G)$ en envoyant la classe de x sur $f(x)$ puisque si x et y ont la même classe modulo N, $f(x)$ et $f(y)$ sont égaux ; il est facile de vérifier que h est un isomorphisme de G/N sur $f(G)$. Soit alors i l'application identique de $f(G)$ dans G' : c'est un homomorphisme injectif et nous avons

$$f = i \circ h \circ g\,.$$

Cette écriture constitue la décomposition canonique de f.

c) *Exemple*
Soit n un entier relatif non nul; les sous-groupes $n\mathbb{Z}$ et $(-n)\mathbb{Z}$ sont identiques et, donc, nous pouvons supposer n strictement positif. Le groupe quotient $\mathbb{Z}/n\mathbb{Z}$ est appelé *groupe des entiers modulo* n.

1.8. Proposition. — *Considérons le groupe* $\mathbb{Z}/n\mathbb{Z}$ *:*
1. C'est un groupe monogène, fini d'ordre n *dont les éléments sont les classes de* $0, 1, \ldots, n-1$.
2. Si $a \in \{0, 1, \ldots, n-1\}$, *la classe de* a *est un générateur de* $\mathbb{Z}/n\mathbb{Z}$ *si et seulement si* a *et* n *sont premiers entre eux.*

La démonstration de cette proposition est laissée en exercice.
Cette proposition va nous permettre de donner une description des groupes monogènes.

1.9. Proposition. — *Soit* $G =< a >$ *un groupe monogène engendré par* a *que nous noterons multiplicativement. Alors :*
ou bien G *est infini et il est isomorphe à* $\mathbb{Z}$,
ou bien G *est fini d'ordre* n *et il est isomorphe à* $\mathbb{Z}/n\mathbb{Z}$.

Démonstration
Soit e l'élément neutre de G. Le groupe G peut s'écrire :

$$G = \{a^k \ ; \quad k \in \mathbb{Z}\}.$$

Soit alors f l'application de $\mathbb{Z}$ dans G définie par

$$f(k) = a^k.$$

C'est un homomorphisme surjectif et son noyau est un sous-groupe de $\mathbb{Z}$; il est donc de la forme $n\mathbb{Z}$,(*cf.* exercice I.1), où n est un entier naturel et d'après la décomposition d'un homomorphisme, G est isomorphe à $\mathbb{Z}/n\mathbb{Z}$.
Si $n = 0$, le noyau de f est réduit à 0 et G est isomorphe à $\mathbb{Z}$ donc G est infini; si $n \neq 0$, G est isomorphe à $\mathbb{Z}/n\mathbb{Z}$ et G est fini d'ordre n. □

1.10. Groupes finis
Soit G un groupe fini d'ordre g. Si H est un sous-groupe de G, il est aussi fini. Désignons par h son ordre. Toutes les classes à gauche selon H sont de la forme xH et ont donc le même nombre d'éléments, h. Elles réalisent une partition de G; si n désigne le nombre de classes à gauche, nous avons donc $g = hn$, ce qui montre que l'ordre de H est un diviseur de l'ordre de G.
Soit a un élément de G et H le sous-groupe engendré par a. L'ordre de H est appelé *ordre de* a *dans* G : c'est le plus petit entier naturel positif k tel que $a^k = e$. L'ordre de tout élément de G est donc un diviseur de l'ordre de G. Remarquons encore que pour tout a dans G, $a^g = e$.
Dans toute la fin de cette sous-section consacrée aux groupes, G est un groupe commutatif noté additivement d'élément neutre 0.
Si H et K désignent deux sous-groupes de G, définissons $H + K$ de la manière suivante

$$H + K = \{x + y \ ; \quad x \in H \, , \ y \in K\}.$$

Il est clair que $H + K$ est un sous-groupe de G contenant H et K.
Nous allons établir des théorèmes d'isomorphismes entre certains sous-groupes.

1.11. Théorème. — *Soit H et K deux sous-groupes de G tels que $H \subset K \subset G$. Désignons par α l'homomorphisme canonique de G sur G/H et par β l'homomorphisme canonique de G sur G/K.*
1. Il existe un unique homomorphisme φ de G/H dans G/K tel que $\varphi \circ \alpha = \beta$.
2. φ est surjectif et son noyau est K/H.
3. Il existe un isomorphisme ϕ de $(G/H)/(K/H)$ sur G/K.

Démonstration
1. Soit X un élément de G/H. Si x et y sont deux représentants de X, nous avons $x - y \in H$ donc $X = \alpha(x) = \alpha(y)$.
D'autre part, comme $H \subset K$, $(x-y)$ appartient à K et $\beta(x) = \beta(y)$. Nous pouvons alors définir φ par $\varphi(X) = \beta(x) = \beta(y)$. Le fait que φ soit un homomorphisme résulte immédiatement des propositions de α et β et la définition de φ donne la relation $\varphi \circ \alpha = \beta$.
2. Comme β est surjectif, il en est de même de φ.
Un élément X de G/H appartient au noyau de φ si et seulement si $\beta(x) = 0$ où x désigne un représentant de X donc $x \in K$ et $X \in K/H$.
3. Ceci résulte alors de la décomposition d'un homomorphisme. □

1.12. Théorème. — *Soit H et K deux sous-groupes de G. Désignons par α l'homomorphisme canonique de G sur G/H, par α' la restriction de α à K et par α'' la restriction de α à $H + K$.*
1. Le noyau de α' est $H \cap K$ et celui de α'' est H.
2. $(H + K)/H$ est isomorphe à $K/(H \cap K)$.

Démonstration
1. La démonstration est immédiate.
2. Nous savons, d'après la décomposition d'un homomorphisme, que $\alpha'(K)$ est isomorphe à $K/(H \cap K)$. Soit X un élément de $\alpha'(K)$; il existe x dans K tel que $X = \alpha'(x)$; comme $K \subset H + K$, $X \in (H + K)/H$.
Si maintenant $Y \in (H + K)/H$, il existe $z \in H$ et $y \in K$ tels que $\alpha(y + z) = Y = \alpha'(y)$ donc $\alpha'(K) = (H + K)/H$ d'où la conclusion. □

2. Anneaux

2.1. Définition. — *On appelle anneau un ensemble A muni de deux lois de compositions internes, la première notée additivement en fait un groupe abélien, la seconde notée multiplicativement est associative, possède un élément neutre noté* 1 *et est distributive par rapport à l'addition :*

$$\forall (x, y, z) \in A^3,\ x(y + z) = xy + xz \text{ et } (y + z)x = yx + zx\,.$$

Si la seconde loi est commutative, l'anneau est dit commutatif. Par exemple, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ sont des anneaux commutatifs.

Si pour $a \in A$, il existe $a' \in A$ tel que $aa' = a'a = 1$, l'élément a est dit *inversible* dans A. Il est facile de vérifier que l'ensemble A^* des éléments inversibles dans A est un groupe multiplicatif.

Dans toute la suite, nous ne considérerons que des anneaux commutatifs : quand nous dirons A est un anneau, cela signifiera A est un anneau commutatif et nous noterons A^* l'ensemble des éléments inversibles de A. Une exception est faite pour l'anneau $\mathbb{Z}$ des entiers relatifs : l'ensemble des entiers relatifs inversibles est réduit à $\{\pm 1\}$ mais nous noterons $\mathbb{Z}^*$ l'ensemble des entiers relatifs non nuls pour se conformer à une écriture usuelle.

2.2. Définition. — *Soit A un anneau. On dit que A est un anneau intègre si le produit de deux éléments de A n'est nul que si l'un d'entre eux l'est*

$$\forall (x,y) \in A^2,\ xy = 0 \Rightarrow\ x = 0 \text{ ou } y = 0\,.$$

2.3. Définition. — *Soit A un anneau et B une partie de A. On dit que B est un sous-anneau de A si B est un sous-groupe additif de A stable pour la multiplication et si 1 appartient à B.*

2.4. Définition. — *Soit A et A' deux anneaux et f une application de A dans A'. On dit que f est un homomorphisme d'anneaux si f est un homomorphisme de groupes additifs, si $f(1) = 1$ et si*

$$\forall (x,y) \in A^2,\ f(xy) = f(x)f(y).$$

Si f est une bijection, f est un *isomorphisme* de A sur A'. Un isomorphisme de A sur lui-même est un *automorphisme* de A.

2.5. Définition. — *Soit A un anneau ; une partie I de A est un idéal si c'est un sous-groupe additif de A et si*

$$\forall (x,y) \in I \times A\,,\ xy \in I\,.$$

Un anneau A a toujours des idéaux : $\{0\}$ et A sont des idéaux de A. Un idéal I de A est dit *propre* s'il est différent des idéaux $\{0\}$ et A.
Les idéaux de $\mathbb{Z}$ sont les $n\mathbb{Z}$ pour $n \in \mathbb{Z}$ (*cf.* exercice I.1).
Si A est un anneau et si $a \in A$, l'ensemble

$$\{ax\ ;\quad x \in A\}$$

est un idéal de A ; c'est l'idéal de A engendré par a. Un tel idéal est appelé *principal*.

2.6. Définition. — *Un anneau A est dit principal s'il est intègre et si tout idéal de A est principal.*

2.7. Proposition. — *Soit A et A' deux anneaux et f un homomorphisme de A dans A'. Alors*
1. $f(A)$ est un sous-anneau de A'.
2. L'ensemble

$$\ker f = \{x/x \in A \ ; \quad f(x) = 0\}$$

est un idéal de A appelé noyau de f.
3. f est injectif si et seulement si son noyau est réduit à $\{0\}$.

2.8. Anneaux quotients

Soit A un anneau et I un idéal de A. Nous avons vu que A/I est un groupe.
Si α et β sont deux éléments de A/I et si a et a' sont deux représentants de α, b et b' deux représentants de β, $a - a'$ et $b - b'$ appartiennent à I donc

$$ab - a'b' = a(b - b') + b'(a - a') \in I \ ,$$

ce qui montre que ab et $a'b'$ ont même classe modulo I.
Nous pouvons donc définir une multiplication sur A/I en posant $\alpha\beta$ égal à la classe de ab; il est facile de vérifier que cette multiplication fait de A/I un anneau, appelé *anneau quotient de A par I* et que l'application de A dans A/I qui, à un élément x de A associe sa classe modulo I, est un homomorphisme surjectif, appelé *homomorphisme canonique* de A sur A/I.
Remarquons que $\mathbb{Z}/n\mathbb{Z}$ est un anneau pour tout entier relatif n.

2.9. Décomposition canonique d'un homomorphisme d'anneaux
Soit A et A' deux anneaux et f un homomorphisme de A dans A'.
Soit N le noyau de f et g l'homomorphisme canonique de A sur A/N. L'application h de A/N dans $f(A)$ envoyant la classe de x sur $f(x)$, où $x \in A$, est un isomorphisme de A/N sur $f(A)$ et si i désigne l'application identique de $f(A)$ dans A' qui est un homomorphisme injectif, nous avons

$$f = i \circ h \circ g \, .$$

Cette écriture est la décomposition canonique de f.

2.10. Caractéristique d'un anneau
Soit A un anneau. Définissons l'application f de $\mathbb{Z}$ dans A par

$$\forall n \in \mathbb{Z}, \ f(n) = n.1$$

Il est facile de démontrer que f est un homomorphisme d'anneaux dont le noyau N est un idéal de $\mathbb{Z}$. Il existe donc $n \in \mathbb{N}$ tel que $N = n\mathbb{Z}$.
Si $n = 0$, f est injective; le seul entier relatif k tel que $k.1 = 0$ est 0; on dit que A est de caractéristique 0.
Si $n \neq 0$, n est le plus petit entier positif tel que $n.1 = 0$, l'anneau $f(\mathbb{Z})$ est isomorphe à $\mathbb{Z}/n\mathbb{Z}$; on dit que A est de caractéristique n.

3. Corps

3.1. Définition. — *Soit K un anneau. C'est un corps si tout élément non nul de K est inversible dans K.*

Notons K^* l'ensemble des éléments de K inversibles dans K ; nous avons donc $K^* = K - \{0\}$.

3.2. Définition. — *Soit K un corps ; une partie H de K est un sous-corps de K si c'est un sous-anneau de K et si tout élément non nul de H est inversible dans H.*

Si H est un sous-corps de K, on dit aussi que K est une *extension* de H.
Il est clair qu'un corps K est intègre et que ses seuls idéaux sont $\{0\}$ et K.
Les définitions d'homomorphismes et d'isomorphismes de corps sont les mêmes que pour les anneaux. Si f est un homomorphisme d'un corps K dans un corps K', $f(K)$ est un sous-corps de K'.

3.3. Proposition. — *Tout homomorphisme f d'un corps K dans un corps K' est injectif.*

En effet, le noyau N de f est un idéal de K ; ce ne peut pas être K car $f(1) = 1$, c'est donc $\{0\}$.
S'il existe un homomorphisme d'un corps K dans un corps K', c'est que K' contient un sous-corps isomorphe à K.
Soit K un corps ; sa caractéristique est la caractéristique de K considéré comme anneau.

3.4. Proposition. — *Un corps K est ou bien de caractéristique 0, ou bien de caractéristique p où p est un nombre premier.*

Démonstration
Considérons l'application f de $\mathbb{Z}$ dans K définie par

$$\forall n \in \mathbb{Z}, \quad f(n) = n.1$$

Nous avons vu que le noyau de f est un idéal de $\mathbb{Z}$ donc de la forme $n\mathbb{Z}$ où $n \in \mathbb{N}$.
Si n est nul, K est de caractéristique 0 .
Sinon, montrons que n est premier (*cf.* la définition d'un nombre premier dans l'exercice I.7) : supposons que $n = lm$ où l et m sont des entiers naturels. Nous avons $f(n) = f(lm) = f(l)f(m) = 0$ donc $f(l)$ ou $f(m)$ est nul. Comme n est le plus petit entier naturel non nul tel que $f(n) = 0$, l ou m est égal à n, ce qui montre que n est premier. □

3.5. Corps des fractions d'un anneau intègre
Soit A un anneau intègre. Cherchons à construire un corps K contenant un sous-anneau isomorphe à A. Pour cela, notons E :

$$E = \{(a, b) \ ; \quad a \in A \ ; \ b \in A \ ; \quad b \neq 0\}.$$

Définissons sur E la relation $\mathfrak{R}$:

$$(a, b)\mathfrak{R}(a', b') \Longleftrightarrow ab' = a'b\,.$$

Cette relation est réflexive, symétrique ; montrons qu'elle est transitive : si $(a, b)\mathfrak{R}(a', b')$ et $(a', b')\mathfrak{R}(a'', b'')$, nous avons $ab' = a'b$ et $a'b'' = a''b'$ donc $ab'b'' = a'bb'' = a''b'b$; comme A est intègre et que $b' \neq 0$, nous en déduisons que $ab'' = a''b$ donc $(a, b)\mathfrak{R}(a'', b'')$.