

Chapitre 0 - Définitions

Groupes - Anneaux - Corps

On se propose dans ce chapitre de donner les définitions de ce qu'on appelle un groupe, un anneau, un corps et d'en donner des exemples. Ces notions seront rappelées en cours, mais n'y seront pas développées, ce n'est pas notre programme. L'objectif de ces notes est seulement de pouvoir s'y référer quand besoin est.

Table des matières

1. Définition d'un groupe - Sous-groupes	1
2. Définition d'un anneau - Sous-anneaux	3
3. Groupe des éléments inversibles d'un anneau	5
4. Définition d'un corps - Sous-corps	6

1. Définition d'un groupe - Sous-groupes

Afin de définir un groupe, il convient de se donner un ensemble G et une loi de composition interne sur G vérifiant certaines conditions.

Définition 1 (Groupe). On appelle groupe un couple $(G, *)$ formé d'un ensemble G et d'une loi de composition interne $(x, y) \mapsto x * y$ sur G , tels que les trois conditions suivantes soient satisfaites :

- 1) quels que soient $x, y, z \in G$, on a $x * (y * z) = (x * y) * z$ (associativité).
- 2) Il existe un élément $e \in G$ tel que pour tout $x \in G$, on ait $e * x = x * e = x$ (existence d'un élément neutre).
- 3) Pour tout $x \in G$, il existe $y \in G$ tel que $x * y = y * x = e$ (existence d'un symétrique pour tout élément de G).

L'élément neutre d'un groupe est unique et tout élément possède un unique symétrique. Si de plus, quels que soient $x, y \in G$, on a $x * y = y * x$ (commutativité), on dit que G est un groupe commutatif ou abélien.

Notation. Dans la définition ci-dessus, on a utilisé la notation abstraite $*$ pour définir la loi de composition sur G . En théorie des groupes, on note la plupart du temps la

loi de composition sous-jacente multiplicativement $(x, y) \mapsto xy$, ou bien additivement $(x, y) \mapsto x + y$. En notation multiplicative, on emploie le mot inverse au lieu du mot symétrique et l'inverse d'un élément x se note x^{-1} . Pour tous $x, y \in G$, on a alors la formule $(xy)^{-1} = y^{-1}x^{-1}$. En notation additive, on dit opposé au lieu de symétrique, et l'on note généralement 0 l'élément neutre et $-x$ l'opposé de x . Dans la pratique, la notation additive est utilisée uniquement pour les groupes abéliens. Cela étant, la notation multiplicative est aussi très souvent employée pour les groupes abéliens. On appellera groupe multiplicatif, un groupe dont la loi de composition est notée multiplicativement, et groupe additif, un groupe dont la loi de composition est notée additivement.

Exemples 2.

1) L'ensemble réduit à un seul élément e , autrement dit un singleton, avec pour loi de composition $e * e = e$, est un groupe, appelé le groupe trivial.

2) L'ensemble \mathbb{Z} des entiers relatifs muni de la loi de composition $(x, y) \mapsto x + y$ est un groupe commutatif, d'élément neutre 0. On l'appelle le groupe additif des entiers relatifs. En remplaçant \mathbb{Z} par \mathbb{Q} , \mathbb{R} ou \mathbb{C} , on obtient respectivement le groupe additif des nombres rationnels, celui des nombres réels et celui des nombres complexes.

3) L'ensemble \mathbb{Q}^* des nombres rationnels non nuls, muni de la loi de composition $(x, y) \mapsto xy$, est un groupe commutatif, d'élément neutre 1. C'est le groupe multiplicatif des nombres rationnels non nuls. On définit de même les groupes multiplicatifs \mathbb{R}^* et \mathbb{C}^* .

4) Le groupe additif \mathbb{Z}^n est défini par la loi de composition

$$(x_1, \dots, x_n) + (y_1, \dots, y_n) = (x_1 + y_1, \dots, x_n + y_n).$$

On définit de même les groupes additifs \mathbb{Q}^n , \mathbb{R}^n et \mathbb{C}^n .

Définition 3 (Sous-groupe). Soit G un groupe additif d'élément neutre 0. Soit H une partie de G . On dit que H est un sous-groupe de G si les conditions suivantes sont remplies :

- 1) l'élément 0 appartient à H .
- 2) Pour tous $x, y \in H$, l'élément $x - y$ est dans H .

Un sous-groupe de G muni de la loi de composition induite par celle de G est un groupe.

Exemples 4.

1) Les parties G et $\{0\}$ sont des sous-groupes de G . Le sous-groupe $\{0\}$ s'appelle le sous-groupe trivial de G .

2) Le sous-ensemble de \mathbb{R}^* formé des nombres réels strictement positifs, ainsi que $\{\pm 1\}$, sont des sous-groupes de \mathbb{R}^* .

- 3) L'ensemble des nombres complexes de module 1 est un sous-groupe de \mathbb{C}^* .
 4) Soit n un entier relatif. L'ensemble

$$n\mathbb{Z} = \{nk \mid k \in \mathbb{Z}\}$$

est un sous-groupe de \mathbb{Z} . De plus, tous les sous-groupes de \mathbb{Z} sont de cette forme (c'est une conséquence du fait que toute partie non vide de \mathbb{N} possède un plus petit élément et du théorème de division euclidienne).

3. Définition d'un anneau - Sous-anneaux

Définition 5 (Anneau). On appelle anneau un triplet formé d'un ensemble A et de deux lois de composition sur A , une addition $(x, y) \mapsto x + y$ et une multiplication $(x, y) \mapsto xy$, tels que les conditions suivantes soient vérifiées :

- 1) le couple $(A, +)$ est un groupe commutatif.
- 2) La multiplication est associative et possède un élément neutre.
- 3) La multiplication est distributive par rapport à l'addition, ce qui signifie que l'on a

$$x(y + z) = xy + xz \quad \text{et} \quad (x + y)z = xz + yz \quad \text{quels que soient } x, y, z \in A.$$

Si de plus la multiplication est commutative, autrement dit si pour tous $x, y \in A$ on a $xy = yx$, on dit que A est un anneau commutatif.

Notons 0 l'élément neutre de $(A, +)$ et 1 l'élément neutre de A pour la multiplication. Rappelons que pour tout $x \in A$, il existe un unique élément de A , noté $-x$, tel que l'on ait $x + (-x) = 0$ ($-x$ est l'opposé de x).

Lemme 6. Pour tous $x, y, z \in A$, on a

$$x(y - z) = xy - xz \quad \text{et} \quad (y - z)x = yx - zx.$$

Démonstration : D'après la condition 3, on a $x(y - z) + xz = x(y - z + z) = xy$ et $(y - z)x + zx = (y - z + z)x = yx$, d'où le lemme.

On en déduit par exemple les formules $x0 = 0x = 0$, $x(-y) = -xy$ et $(-y)x = -yx$. En particulier, $(-1)x = -x$. Par convention, on a

$$x^0 = 1 \quad \text{pour tout } x \in A.$$

Un anneau réduit à un élément, i.e. pour lequel on a $1 = 0$, est dit nul.

Exemples 7.

1) En munissant \mathbb{Z} des deux lois de composition usuelles (addition et multiplication) on obtient l'anneau des entiers relatifs, qui est commutatif. Les ensembles \mathbb{Q} , \mathbb{R} et \mathbb{C} munis de l'addition et de la multiplication usuelles sont aussi des anneaux commutatifs.

2) **L'anneau $A[X]$.** Soit A un anneau commutatif. Un polynôme à une indéterminée à coefficients dans A est par définition une suite $(a_n)_{n \in \mathbb{N}}$ d'éléments de A qui est nulle à partir d'un certain rang. Les a_n sont appelés les coefficients du polynôme. Sur cet ensemble de polynômes, on définit deux lois de composition, une addition et une multiplication. Si $P = (p_0, p_1, \dots)$ et $Q = (q_0, q_1, \dots)$ sont des polynômes à coefficients dans A , on pose

$$P + Q = (p_0 + q_0, p_1 + q_1, \dots) \quad \text{et} \quad PQ = (s_0, s_1, \dots) \quad \text{avec} \quad s_n = \sum_{i+j=n} p_i q_j.$$

On vérifie que l'on obtient ainsi un anneau commutatif. Pour tout $a \in A$, on note a le polynôme $(a, 0, \dots, 0, \dots)$. Posons $X = (0, 1, 0, \dots, 0, \dots)$. Pour tout entier $n \geq 1$, et tout $a \in A$, on vérifie alors que l'on a $aX^n = (0, \dots, 0, a, 0, \dots)$, où le $n + 1$ -ième terme de la suite est a et où tous les autres sont nuls. Tout polynôme $P = (p_0, p_1, \dots, p_n, 0, \dots)$, dont les coefficients d'indices strictement plus grands que n sont nuls, s'écrit alors

$$P = p_0 + p_1 X + \dots + p_n X^n,$$

qui est la notation polynômiale de P et que l'on utilise exclusivement. On note $A[X]$ l'anneau ainsi obtenu. Bien entendu, on peut désigner le polynôme $(0, 1, 0, \dots)$ par d'autres lettres que X , pourvu que la lettre choisie n'ait pas été utilisée par ailleurs.

Définition 8 (Sous-anneau). Soient A un anneau et B une partie de A . On dit que B est un sous-anneau de A si les conditions suivantes sont vérifiées :

- 1) B est un sous-groupe additif de A .
- 2) Quels que soient x et y dans B , le produit xy est dans B .
- 3) L'élément neutre multiplicatif de A appartient à B .

On vérifie que si B est un sous-anneau de A , alors B muni des deux lois de composition induites par celles de A est un anneau.

Exemples 9.

- 1) \mathbb{Z} est un sous-anneau de \mathbb{Q} .
- 2) \mathbb{Q} est un sous-anneau de \mathbb{R} , lui même étant un sous-anneau de \mathbb{C} .
- 3) L'ensemble $\mathbb{Z}[i]$ formé des $a + ib$ avec a et b dans \mathbb{Z} , est un sous-anneau de \mathbb{C} . On l'appelle l'anneau des entiers de Gauss.

4. Groupe des éléments inversibles d'un anneau

Soit A un anneau (pas nécessairement commutatif).

Définition 10. Soit a un élément de A . On dit que a est un élément inversible de A s'il possède un inverse pour la multiplication, autrement dit, s'il existe $b \in A$ tel que l'on ait $ab = ba = 1$. On notera A^* l'ensemble des éléments inversibles de A .

Si $a \in A$ est inversible, il existe b unique dans A tel que $ab = ba = 1$ et on le note a^{-1} .

Lemme 11. Soit a un élément de A . Les conditions suivantes sont équivalentes :

- 1) a est inversible.
- 2) Il existe b et c dans A tels que l'on ait $ab = 1$ et $ca = 1$.

Démonstration : Supposons qu'il existe b et c dans A tels que l'on ait $ab = 1$ et $ca = 1$. On a alors, en tenant compte de l'associativité de la multiplication,

$$b = (ca)b = c(ab) = c,$$

ce qui montre que a est inversible. L'implication réciproque résulte de la définition.

Ce lemme signifie qu'un élément d'un anneau est inversible si et seulement si il est inversible à droite et à gauche.

Remarque 12. Dans un anneau non commutatif, un élément inversible à droite ne l'est pas nécessairement à gauche. En effet, considérons l'ensemble A des endomorphismes du \mathbb{R} -espace vectoriel $\mathbb{R}[X]$ (voir le chapitre II du cours ; un endomorphisme de $\mathbb{R}[X]$ est une application $f : \mathbb{R}[X] \rightarrow \mathbb{R}[X]$ telle que pour tous $P, Q \in \mathbb{R}[X]$ et $\lambda \in \mathbb{R}$, on ait $f(P + Q) = f(P) + f(Q)$ et $f(\lambda P) = \lambda f(P)$). Il est muni d'une structure d'anneau, avec comme loi additive celle définie, pour tous $f, g \in A$ et $P \in \mathbb{R}[X]$, par l'égalité

$$(f + g)(P) = f(P) + g(P),$$

et comme loi multiplicative la composition des applications, l'élément neutre étant l'identité de $\mathbb{R}[X]$.

Soient f l'application qui à un polynôme associe son polynôme dérivé et g l'application définie par (où N est le degré)

$$g\left(\sum_{k=0}^N a_k X^k\right) = \sum_{k=0}^N \frac{a_k}{k+1} X^{k+1}.$$

Ce sont des éléments de A . L'application $f \circ g$ est l'identité de $\mathbb{R}[X]$, autrement dit g est un inverse à droite de f . Cela étant, f n'a pas d'inverse à gauche, sinon f serait une injection, ce qui n'est pas.

Si x et y sont dans A^* , le produit xy l'est aussi et son inverse est $y^{-1}x^{-1}$. La multiplication induit ainsi sur A^* une loi de composition. Plus précisément, on vérifie l'énoncé suivant.

Proposition 13. *L'ensemble A^* , muni de la multiplication induite par celle de A , est un groupe. On l'appelle le groupe des éléments inversibles de A .*

Exemples 14.

- 1) On a $\mathbb{Z}^* = \{-1, 1\}$.
- 2) Les groupes des éléments inversibles des anneaux \mathbb{Q} , \mathbb{R} et \mathbb{C} sont \mathbb{Q}^* , \mathbb{R}^* et \mathbb{C}^* .
- 3) On a $\mathbb{Z}[i]^* = \{\pm 1, \pm i\}$.

4. Définition d'un corps - Sous-corps

Définition 15 (Corps). *Un anneau A est un corps si l'on a $1 \neq 0$, et si tout élément non nul de A est inversible i.e. si l'on a $A^* = A \setminus \{0\}$.*

Par définition, un corps possède donc au moins deux éléments, à savoir 0 et 1. Si A est un anneau commutatif et est un corps, on dit que A est un corps commutatif.

Exemples 16.

- 1) Les anneaux \mathbb{Q} , \mathbb{R} et \mathbb{C} sont des corps commutatifs.
- 2) On peut démontrer que tout corps fini est commutatif. Ce résultat a été établi par Wedderburn en 1905.

Un exemple de corps fini est l'anneau $\mathbb{Z}/p\mathbb{Z}$, formé des classes d'entiers modulo p , où p est un nombre premier.

3) Il existe des corps non commutatifs. Historiquement, le premier corps non commutatif a été découvert par Hamilton vers 1843. On l'appelle le corps des quaternions d'Hamilton. On le note souvent \mathbb{H} . On peut le décrire comme suit. Soit $\mathbb{M}_2(\mathbb{C})$ l'ensemble des matrices ayant deux lignes et deux colonnes à coefficients dans \mathbb{C} (voir le chapitre I du cours). Alors \mathbb{H} est le sous-ensemble de $\mathbb{M}_2(\mathbb{C})$ formé des matrices

$$\begin{pmatrix} u & -\bar{v} \\ v & \bar{u} \end{pmatrix} \quad \text{où } u, v \in \mathbb{C}.$$

La notation \bar{u} désigne le nombre complexe conjugué de u . On peut démontrer que \mathbb{H} est un corps (exercice sur les matrices de $\mathbb{M}_2(\mathbb{C})$). Il n'est pas commutatif, car par exemple en posant (avec $i^2 = -1$)

$$P = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix} \quad \text{et} \quad Q = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix},$$

on a

$$PQ = \begin{pmatrix} 0 & -i \\ -i & 0 \end{pmatrix} \quad \text{et} \quad QP = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix},$$

en particulier, PQ est distinct de QP .

Définition 17 (Sous-corps). Soit K un corps. On appelle sous-corps de K tout sous-anneau de K qui est un corps.

Exemples 18.

- 1) \mathbb{Q} est un sous-corps de \mathbb{R} , lui même étant un sous-corps de \mathbb{C} .
- 2) L'ensemble des éléments de la forme $a + ib$ où $a, b \in \mathbb{Q}$, est un sous-corps de \mathbb{C} . On le note $\mathbb{Q}(i)$. C'est le plus petit sous-corps de \mathbb{C} contenant i .
- 3) L'ensemble des éléments de la forme $a + b\sqrt{2}$ où $a, b \in \mathbb{Q}$, est un sous-corps de \mathbb{R} . On le note $\mathbb{Q}(\sqrt{2})$. C'est le plus petit sous-corps de \mathbb{R} contenant $\sqrt{2}$.
- 4) L'application $\mathbb{C} \rightarrow \mathbb{H}$ qui à $z \in \mathbb{C}$ associe la matrice $\begin{pmatrix} z & 0 \\ 0 & \bar{z} \end{pmatrix}$ permet d'identifier \mathbb{C} à un sous-corps de \mathbb{H} . Nous n'irons pas plus loin dans cette direction.