Bilan sur les structures algébriques.

I Structures

Les structures que nous serons amenés à étudier en MPSI sont les structures de groupe (commutatif ou non), d'anneau (commutatif ou non), de corps, d'espace vectoriel, et d'algèbre. Toutes ces notions ont déjà été vues. Dressons un bilan des définitions assorties de quelques exemples, déjà rencontrés ou à venir.

I.1 Groupes

Définition 1 : Groupe.

Un groupe est un couple $(G, \cdot)$, où G est un ensemble et $\cdot : G \times G \to G$ une **loi de composition interne**, vérifiant les axiomes suivants :

1. $\cdot$ est associative, c'est-à-dire : $\forall (a,b,c) \in G^3, a \cdot (b \cdot c) = (a \cdot b) \cdot c$,
2. $\cdot$ a un élément neutre, c'est-à-dire : $\exists e \in G, \forall a \in G, a \cdot e = e \cdot a = a$,
3. tout élément de G a un symétrique pour $\cdot$, c'est-à-dire : $\forall x \in G, \exists y \in G, x \cdot y = y \cdot x = e$.

Remarque 1

C'est l'associativité de $\cdot$ qui nous autorise à écrire $a \cdot b \cdot c$ au lieu de $(a \cdot b) \cdot c$ ou $a \cdot (b \cdot c)$ (ces expressions étant égales).

Exemple 1 Ainsi :

⟶ $(\mathbb{Z}, +)$ forme un groupe : l'élément neutre est 0, les symétriques sont les opposés.

⟶ $(\mathbb{C} \setminus \{0\}, \times)$ forme un groupe : l'élément neutre est 1, les symétriques sont les inverses.

⟶ $(\{\pm 1\}, \times)$ forme un groupe : l'élément neutre est 1, les symétriques sont les éléments eux-même.
Cet exemple est intéressant : contrairement aux autres, ce groupe est fini.

En revanche :

⟶ $(\mathbb{N}, +)$ ne forme pas un groupe : il existe bien un élément neutre qui est 0, mais il n'est pas vrai que tout entier a un symétrique pour $+$. En fait, seul 0 a un symétrique.

⟶ $(\mathbb{R}, \times)$ ne forme pas un groupe : il existe bien un élément neutre qui est 1, mais il n'est pas vrai que tout réel a un symétrique pour $\times$ puisque 0 n'en a pas.

⟶ $(\mathbb{R}, \min)$ ne forme pas un groupe : il n'existe pas d'élément neutre.

Définition 2 : Commutativité.

Un groupe $(G, \cdot)$ est dit commutatif (ou abélien) lorsque la loi $\cdot$ est commutative, c'est-à-dire : $\forall (a,b) \in G^2, a \cdot b = b \cdot a$.

Exemple 2

⟶ Tous les exemples de l'exemple 1 sont des exemples de groupes commutatifs.

⟶ En revanche, si on note $S(\mathbb{R})$ l'ensemble des applications bijectives de $\mathbb{R}$ dans $\mathbb{R}$, $(S(\mathbb{R}), \circ)$ forme bien un groupe, mais ce groupe n'est pas commutatif.

Définition 3 : Groupe symétrique.

On appelle groupe symétrique le groupe $(S_n, \circ)$ où $S_n = S_{\{1,2,\dots,n\}}$ est l'ensemble des bijections de $\{1, 2, \dots, n\}$ dans $\{1, 2, \dots, n\}$.

Exercice ! Décrivons S_2 et S_3, et calculons quelques produits dans ces groupes.

1. On a déjà vu qu'on a $S_2 = \{\mathrm{id}, \tau_{1,2}\}$ où $\tau_{1,2} : \begin{cases} \{1,2\} & \to & \{1,2\} \\ 1 & \mapsto & 2 \\ 2 & \mapsto & 1 \end{cases}$. Sa "table de multiplication" est :

$\circ$	id	$\tau_{1,2}$
id	id	$\tau_{1,2}$
$\tau_{1,2}$	$\tau_{1,2}$	id

2. On a déjà vu qu'on a $S_3 = \{\mathrm{id}, \tau_{1,2}, \tau_{1,3}, \tau_{2,3}, c, c^{-1}\}$ où les $\tau_{i,j}$ permutent i et j, et où $c(1) = 2,\ c(2) = 3,\ c(3) = 1$. La "table de multiplication" est la suivante. Attention ! La lci $\circ$ n'est pas commutative ici, l'élément écrit en ligne f et colonne g correspond à $f \circ g$ (donc : d'abord g et ensuite f) et non pas à $g \circ f$.

$\circ$	id	$\tau_{1,2}$	$\tau_{1,3}$	$\tau_{2,3}$	c	c^{-1}
id	id	$\tau_{1,2}$	$\tau_{1,3}$	$\tau_{2,3}$	c	c^{-1}
$\tau_{1,2}$	$\tau_{1,2}$	id	c^{-1}	c	$\tau_{2,3}$	$\tau_{1,3}$
$\tau_{1,3}$	$\tau_{1,3}$	c	id	c^{-1}	$\tau_{1,2}$	$\tau_{2,3}$
$\tau_{2,3}$	$\tau_{2,3}$	c^{-1}	c	id	$\tau_{1,3}$	$\tau_{1,2}$
c	c	$\tau_{1,3}$	$\tau_{2,3}$	$\tau_{1,2}$	c^{-1}	id
c^{-1}	c^{-1}	$\tau_{2,3}$	$\tau_{1,2}$	$\tau_{1,3}$	id	c

Un des intérêts d'identifier qu'un ensemble muni d'une loi est un groupe est qu'on dispose alors gratuitement de toute une banque de théorèmes montrés une bonne fois pour toutes pour tous les groupes. Voyons deux exemples immédiats et évidents (pas explicitement dans le programme mais sans lesquels on ne peut énoncer les théorèmes du programme) :

Proposition 1 : Unicité du neutre et des symétriques.

1. Dans un groupe, l'élément neutre est en réalité unique.
2. De plus, tous les éléments ont en réalité un unique symétrique.

Démonstration. Soit $(G, \cdot)$ un groupe.

1. Soient e_1 et e_2 deux neutres. $e_1 = e_1 \cdot e_2 = e_2$. D'où l'unicité.
2. Soient $x \in G$ et y_1, y_2 deux symétriques de x. On a $y_2 = y_2 \cdot (x \cdot y_1) = (y_2 \cdot x) \cdot y_1 = y_1$. D'où l'unicité. □

Remarque 2

Ce théorème nous autorise à écrire x^{-1} pour dénoter **le** symétrique de x.

Théorème 1 : Symétrique d'un produit.

Dans un groupe, on a $(xy)^{-1} = y^{-1}x^{-1}$.

La démonstration consiste simplement à écrire l'associativité.

Définition 4 : Groupe produit.

Étant donnés deux groupes $(G_1, \cdot)$ et $(G_2, *)$, on appelle **groupe produit de** $(G_1, \cdot)$ **et** $(G_2, *)$ le couple $(G_1 \times G_2, \star)$ où $\star$ est définie par $(x_1, x_2) \star (y_1, y_2) = (x_1 \cdot y_1, x_2 * y_2)$

Exemple 3

⟶ Le groupe $(\mathbb{R}^2, +)$ est le groupe produit $(\mathbb{R}, +) \times (\mathbb{R}, +)$.

⟶ Voici un groupe produit en apparence artificiel (mais en apparence seulement) : $(\{\pm 1\}, \times) \times (\mathbb{Z}, +)$.
Les éléments de se groupe sont les couples (ε, n) avec $\varepsilon \in \{\pm 1\}$ et $n \in \mathbb{Z}$.
Et pour deux éléments (ε_1, n_1) et (ε_2, n_2) on a $(\varepsilon_1, n_1) \star (\varepsilon_2, n_2) = (\varepsilon_1\varepsilon_2, n_1 + n_2)$.

Proposition 2 : Groupe produit.

Les groupes produits sont des groupes.

La démonstration est immédiate : on raisonne "coordonnée par coordonnée".

I.2 Anneaux

Définition 5 : Anneaux.

Un anneau est un triplet $(A, +, \times)$, où A est un ensemble et $+, \times : A \times A \to A$ deux lois de composition internes, vérifiant les axiomes suivants :

1. $(A, +)$ forme un groupe commutatif,
2. $\times$ a un élément neutre,
3. $\times$ est associative,
4. $\times$ est distributive sur $+$, c'est-à-dire $\forall (a, b, c) \in A^3, a \times (b + c) = a \times b + a \times c$ (distributivité à gauche) et $\forall (a, b, c) \in A^3, (a + b) \times c = a \times c + b \times c$ (distributivité à droite).

Remarque 3

De la même façon que pour les groupes, le neutre de $+$ est unique, les symétriques pour $+$ sont uniques, le neutre pour $\times$ est unique, et les symétriques pour $\times$, lorsqu'ils existent, sont uniques.

On a donc coutume de toujours noter :

i/ 0_A ou 0 le neutre de $+$,

ii/ $-a$ le symétrique de a pour $+$, qu'on appelle opposé de a,

iii/ 1_A ou 1 le neutre de $\times$,

iv/ a^{-1} l'éventuel symétrique de a pour $\times$, s'il existe, qu'on appelle alors inverse de a.

Exemple 4 Ainsi :

$\longrightarrow$ $(\{0\},+,\times)$ forme un anneau : les lois sont définies de la seule façon possible et les deux neutres sont égaux.
On l'appelle **l'anneau nul**. C'est à cause de lui qu'on a la précision "non nul" pour les corps.

$\longrightarrow$ On a déjà vu de nombreux autres exemples.
Des gentils : $(\mathbb{Z},+,\times)$, $(\mathbb{D},+,\times)$, $(\mathbb{Q},+,\times)$, $(\mathbb{R},+,\times)$, $(\mathbb{C},+,\times)$, $(\mathbb{K}[X],+,\times)$.
Des plus méchants : $(\mathbb{Z}/n\mathbb{Z},+,\times)$, $(\mathcal{M}_n(\mathbb{R}),+,\times)$, $(\mathcal{C}^n(I,\mathbb{R}),+,\times)$ $(n\in\mathbb{N})$.

Définition 6 : Commutativité.

Un anneau est dit commutatif si la loi $\times$ est commutative.

Exemple 5 Tous les anneaux de l'exemple 4 sont commutatifs sauf $(\mathcal{M}_n(\mathbb{R}),+,\times)$ qui ne l'est pas pour $n\geqslant 2$.
Deux théorèmes évidents sur les anneaux :

Proposition 3 : 0_A est absorbant.

Dans un anneau $(A,+,\times)$, l'élément 0_A est absorbant pour la loi $\times$, c'est-à-dire $\forall a\in A, a\times 0_A = 0_A$.

Démonstration. Soit $(A,+,\times)$ un anneau et $a\in A$.
On a $a\times 0_A = a\times(0_A+0_A) = a\times 0_A + a\times 0_A$.
En rajoutant à chaque membre l'opposé de $a\times 0_A$, on trouve bien $0_A = a\times 0_A$. □

Corollaire immédiat : 0_A n'a jamais d'inverse, sauf dans l'anneau nul.

Proposition 4 : Opposé et multiplication.

Dans un anneau $(A,+,\times)$, on a, pour tout $a\in A$, $-a = (-1_A)\times a$.

Démonstration. Par unicité de l'opposé, il suffit de montrer que a et $(-1_A)\times a$ ont une somme nulle.
Or $a+(-1_A)\times a = 1_A\times a + (-1_A)\times a = (1_A+(-1_A))\times a = 0_A\times a$ □

Deux théorèmes importants sur les anneaux :

Théorème 2 : Binôme de Newton.

Soient $(A,+,\times)$ un anneau, $n\in\mathbb{N}$, et $a,b\in A$ qui commutent. Alors on a : $(a+b)^n = \sum_{k=0}^{n}\binom{n}{k}a^k b^{n-k}$.

Démonstration. En TD. □

Théorème 3 : Identité géométrique généralisée.

Soient $(A,+,\times)$ un anneau, $n\in\mathbb{N}$, $a,b\in A$ qui commutent. Alors on a : $a^n - b^n = (a-b)\sum_{k=0}^{n-1} a^{n-1-k}b^k$.

Démonstration. En TD. □

Définition 7 : Intégrité.

Un anneau commutatif non nul $(A,+,\times)$ est dit **intègre** lorsqu'on a $\forall (a,b)\in A, a\times b = 0_A \Leftrightarrow a = 0_A$ ou $b = 0_A$.

Les anneaux intègres sont donc précisément ceux pour lesquels le théorème "un produit est nul si et seulement si l'un de ses facteurs est nul" est vrai.

Remarque 4

Dans la littérature, on trouve parfois d'autres définitions de l'intégrité, qui rajoutent une hypothèse de commutativité et/ou une hypothèse de non nullité. Comme le programme n'est pas explicite sur la définition à prendre, je vous donne celle que j'utilise.

Exemple 6 On a déjà vu que les gentils exemples de l'exemple 4 sont intègres alors que les méchants exemples de l'exemple 4 le sont rarement.

Définition 8 : Divisibilité.

Dans tout anneau commutatif, pour tout couple (a,b) d'éléments de A, on dit que a divise b et on note $a|b$ lorsqu'on a $\exists k \in A, b = a \times k$.

Ceci signifie qu'on peut "faire de l'arithmétique" dans tout anneau commutatif [1], et pas seulement dans $\mathbb{Z}$. Par contre, tous les anneaux n'ont pas les mêmes propriétés arithmétiques que $\mathbb{Z}$. Par exemple, le théorème de division euclidienne n'est pas toujours vrai dans un anneau quelconque. Néanmoins, lorsqu'il sera vrai, on sera bien parti.

Exemple 7 Le théorème de division euclidienne est vrai dans $\mathbb{Z}$ mais aussi dans $\mathbb{K}[X]$.

Notation 1 Étant donné un anneau $(A, +_A, \times_A)$ on note $A^\times$ l'ensemble des inversibles de A (pour $\times_A$).

Remarque 5

Soit $(A, +_A, \times_A)$ un anneau. On a $\forall (a,b) \in A^\times,\ a \times_A b \in A^\times$. Autrement dit $\times_A$ peut être vue comme une lci sur $A^\times$.

Démonstration. Soient $a,\ b \in A^\times$, on a $b^{-1}a^{-1}ab = 1_A$ par associativité donc ab est inversible d'inverse $b^{-1}a^{-1}$. □

Théorème 4 : Groupe des inversibles d'un anneau.

$(A^\times, \times_A)$ forme un groupe, on l'appelle **groupe des inversibles de** $(A, +_A, \times_A)$.

Démonstration. On sait que $\times_A$ peut être vue comme une lci sur $A^\times$. Les axiomes d'anneau et la définition de $A^\times$ impliquent alors les axiomes de groupe. □

Exemple 8

1. Le groupe $(\mathbb{Z}^\times, \times)$ est le groupe $(\{\pm 1\}, \times)$.
2. $(\mathbb{R}^*, \times)$ est un groupe puisque c'est le groupe $(\mathbb{R}^\times, \times)$.
3. L'ensemble $\mathcal{M}_n(\mathbb{K})^\times$ des matrices inversibles se note $GL_n(\mathbb{K})$. Le groupe $(GL_n(\mathbb{K}), \times)$ s'appelle le groupe linéaire.

I.3 Corps

Définition 9 : Corps.

Un corps est un triplet $(\mathbb{K}, +, \times)$, où $\mathbb{K}$ est un ensemble et $+, \times : \mathbb{K} \times \mathbb{K} \to \mathbb{K}$ deux lois de composition internes, vérifiant les axiomes suivants :

1. $(\mathbb{K}, +, \times)$ forme un anneau **commutatif et non nul**.
2. Tout élément de $\mathbb{K} \setminus \{0\}$ a un inverse.

Ce qui peut se reformuler :

1. $(\mathbb{K}, +)$ forme un groupe commutatif.
2. $(\mathbb{K} \setminus \{0\}, \times)$ forme un groupe commutatif.
3. $\times$ est distributive sur $+$

Exemple 9 Ainsi :

⟶ $(\mathbb{C}, +, \times)$ forme un corps.

⟶ $(\mathbb{Z}/5\mathbb{Z}, +, \times)$ forme un corps.

1. Dans les anneaux non commutatifs c'est plus compliqué : on va avoir des diviseurs à gauche et des diviseurs à droite. Beurk.

En revanche :

⟶ $(\mathbb{Z}, +, \times)$ ne forme pas un corps : seuls 1 et -1 ont un inverse.

⟶ $(\mathbb{Z}/4\mathbb{Z}, +, \times)$ ne forme pas un corps : 2 n'a pas d'inverse.

⟶ $(\mathcal{M}_2(\mathbb{R}), +, \times)$ ne forme pas un corps, par exemple parce qu'il n'est pas commutatif.

La proposition immédiate la plus intéressante sur les corps est la suivante :

Proposition 5 .

Un corps est un anneau intègre.

Notons que la réciproque est fausse puisque $\mathbb{Z}$ est intègre.

Démonstration. Soit $(\mathbb{K}, +, \times)$ un corps. Soient $x,\ y \in \mathbb{K}$ tels que $xy = 0_{\mathbb{K}}$.

On veut montrer « $x = 0_{\mathbb{K}}$ ou $y = 0_{\mathbb{K}}$ », c'est-à-dire « $x \neq 0_{\mathbb{K}} \Rightarrow y = 0_{\mathbb{K}}$ ».
Supposons $x \neq 0_K$, alors x^{-1} existe et est dans $\mathbb{K}$. On a donc $y = x^{-1}xy = x^{-1}0_K = 0_K$. Et boum. □

I.4 Espaces vectoriels sur un corps

On va les étudier à fond (mais vraiment à fond) ce semestre et en deuxième année. Donc allons vite.

Définition 10 : K-ev.

Étant donné un corps $\mathbb{K}$, en contexte une bonne fois pour toute [a], un espace vectoriel sur $\mathbb{K}$ (ou $\mathbb{K}$-ev) est un triplet $(E, +, \cdot)$, où E est un ensemble, $+ : E \times E \to E$ une loi de composition interne et $\cdot : \mathbb{K} \times E \to E$ une loi de composition *externe* vérifiant les axiomes suivants :

1. $(E, +)$ forme un groupe **commutatif** (on note 0_E ou parfois $\overrightarrow{0}$ son élément neutre),
2. $\cdot$ est distributive à gauche et à droite sur $+$,
3. $\cdot$ est compatible avec $\times$ et 1_K.

a. C'est du pipo. En pratique on suppose $\mathbb{K} = \mathbb{R}$ ou $\mathbb{C}$... très éventuellement $\mathbb{Q}$.

Exemple 10 Cf les 4 chapitres sur les espaces vectoriels qu'on a déjà fait !

Comme $(E, +)$ forme un groupe (commutatif), toutes les règles de calcul au sein d'un groupe présentées sur les groupes sont également valables dans un espace vectoriel.

Les théorèmes suivants se démontrent à l'aide de la distributivité :

Proposition 6 : $\mathbf{0_K}$ et $\mathbf{0_E}$ sont absorbants.

1. Dans un $\mathbb{K}$-ev E, on a $\forall x \in E, 0_K \cdot x = 0_E$.
2. Dans un $\mathbb{K}$-ev E, on a $\forall \lambda \in \mathbb{K}, \lambda \cdot 0_E = 0_E$.

En corollaire :

Corollaire 1 : Opposé et multiplication externe.

Dans un $\mathbb{K}$-ev E, on a, pour tout $x \in E$, $-x = (-1_{\mathbb{K}}) \cdot x$.

Proposition 7 : Produit nul dans un espace vectoriel.

Dans un $\mathbb{K}$-ev E, on a, pour tout $x \in E$ et tout $\lambda \in \mathbb{K}$, on a : $\lambda \cdot x = 0_E \Leftrightarrow \lambda = 0_{\mathbb{K}}$ ou $x = 0_E$.

Démonstration. Soient $x \in E$ et $\lambda \in \mathbb{K}$. On veut montrer $\lambda \cdot x = 0_E \Leftrightarrow \lambda = 0_{\mathbb{K}}$ ou $x = 0_E$. L'implication réciproque résulte la proposition 6. Montrons l'implication directe. Supposons $\lambda \cdot x = 0_E$. Soit λ est nul, et le résultat est démontré, soit on a $\lambda \neq 0_K$, et λ est inversible car $\mathbb{K}$ est un corps, mais dans ce second cas on a $x = \lambda^{-1} \cdot \lambda \cdot x = \lambda^{-1} \cdot 0_E = 0_E$ d'après la proposition 6. □

I.5 Algèbre (unitaire, sur un corps)

Définition 11 : $\mathbb{K}$-algèbre.

Étant donné un corps $(\mathbb{K}, +_{\mathbb{K}}, \times_{\mathbb{K}})$ (comprendre : $\mathbb{R}$ ou $\mathbb{C}$), une algèbre unitaire sur $\mathbb{K}$ (abrégeons : une $\mathbb{K}$-alg) est un quadruplet $(\mathcal{A}, +, \times, \cdot)$, où $\mathcal{A}$ est un ensemble, $+, \times : \mathcal{A} \times \mathcal{A} \to \mathcal{A}$ deux lois de composition internes et $\cdot : \mathbb{K} \times \mathcal{A} \to \mathcal{A}$ une loi de composition externe vérifiant les axiomes suivants :

1. $(\mathcal{A}, +, \times)$ forme un anneau (on notera $0_{\mathcal{A}}$ et $1_{\mathcal{A}}$ ses éléments neutres),
2. $(\mathcal{A}, +, \cdot)$ est un $\mathbb{K}$-ev,
3. $\cdot$ et $\times$ sont compatibles : $(a \cdot x) \times (b \cdot y) = (a \times_{\mathbb{K}} b) \cdot (x \times y)$.

Exemple 11 $(\mathcal{M}_n(\mathbb{K}), +, \times, \cdot)$, $(\mathbb{K}^{\mathbb{N}}, +, \times, \cdot)$, $(\mathcal{C}(I, \mathbb{K}), +, \times, \cdot)$, $(\mathbb{K}[X], +, \times, \cdot)$, ...

II Sous-structures

Pour résumer cette section :

1. un sous-truc est un machin inclus dans le truc *stable pour la structure de truc* ;
2. un sous-truc, muni des lois induites par le truc, forme un truc.

II.1 Sous-groupes

Définition 12 : Sous-groupe.

Soit $(G, \cdot)$ un groupe. On appelle sous-groupe de G un ensemble H inclus dans G stable pour la structure de groupe de G c'est-à-dire tel que :

1. $e \in H$ (en notant e le neutre de G),
2. $\forall (x, y) \in H^2, x \cdot y \in H$,
3. $\forall x \in H, x^{-1} \in H$ (en notant x^{-1} le symétrique de x pour $\cdot$).

Théorème 5 : Sous-groupe.

Si H est un sous-groupe de G, alors les lois de G induisent des lois sur H et H, muni des lois induites, forme un groupe.

Démonstration. C'est fait pour ! □

Exemple 12

⟶ On a déjà vu (?) que les sous-groupes de $(\mathbb{Z}, +)$ sont exactement les $n\mathbb{Z}$ pour $n \in \mathbb{N}$.

⟶ On a déjà vu (? ? ?) que les sous-groupes de $(\mathbb{R}, +)$ sont soit de la forme $\gamma\mathbb{Z}$ ($\gamma \in \mathbb{R}_+$), soit denses dans $\mathbb{R}$.

⟶ On a déjà vu que pour tout entier $n \geqslant 1$, $\mathbb{U}_n$ est un sous-groupe de $(\mathbb{C}^\times, \times)$.

Une autre remarque intéressante :

Proposition 8 : Transitivité de "être un sous-groupe de".

Un sous-groupe d'un sous-groupe est un sous-groupe.

Remarque 6

Un sous-groupe d'un groupe commutatif est commutatif.

II.2 Sous-anneaux

Définition 13 : Sous-anneau.

Soit $(A, +, \times)$ un anneau. On appelle sous-anneau de A un ensemble B inclus dans A stable pour la structure d'anneau de A c'est-à-dire tel que :

1. $0_A,\ 1_A \in B$,
2. $\forall (x, y) \in B^2, x + y \in B$,
3. $\forall x \in B, -x \in B$,
4. $\forall (x, y) \in B^2, x \times y \in B$.

Là encore :

Proposition 9 : Sous-anneau.

Si B est un sous-anneau de A, alors les lois de A induisent des lois sur B, et B, muni des lois induites, forme un anneau.

Proposition 10 .

Un sous-anneau d'un sous-anneau est un sous-anneau.

Remarque 7

1. Un sous-anneau d'un anneau commutatif est commutatif.
2. Un sous-anneau d'un anneau intègre est intègre.

Attention, la réciproque est fausse : par exemple l'ensemble $\{\lambda I_n,\ \lambda \in \mathbb{R}\}$ est un sous-anneau de $\mathcal{M}_n(\mathbb{K})$ et $\mathcal{M}_n(\mathbb{K})$ n'est ni intègre ni commutatif, mais ce sous-anneau est intègre et commutatif puisque c'est un corps (ce sous-anneau est essentiellement $\mathbb{K}$, à renommage près).

II.3 Sous-corps

Définition 14 : Sous-corps.

Soit $(\mathbb{K}, +, \times)$ un anneau. On appelle sous-corps de $\mathbb{K}$ un ensemble L inclus dans $\mathbb{K}$ stable pour la structure de corps de $\mathbb{K}$ c'est-à-dire tel que :

1. $(L, +, \times)$ forme un sous-anneau de $\mathbb{K}$ (reprendre les 4 axiomes).
2. L'inverse de tout élément de $\mathrm{L} \setminus \{0\}$ **est dans** L.

Là encore :

Proposition 11 : Sous-corps.

Si L est un sous-corps de K, alors les lois de K induisent des lois sur L, et L muni des lois induites forme un corps.

Proposition 12 .

Un sous-corps d'un sous-corps est un sous-corps.

II.4 Sous-espace vectoriel

Définition 15 : Sous-espace vectoriel.

Soit $(E, +, \cdot)$ un $\mathbb{K}$-ev. On appelle sev de E un ensemble F inclus dans E stable pour la structure de $\mathbb{K}$-ev de E c'est-à-dire tel que :

1. $0 \in F$,
2. $\forall (x, y) \in F^2, x + y \in E$,
3. $\forall x \in F, -x \in F$,
4. $\forall x \in F, \forall \lambda \in \mathbb{K}, \lambda x \in F$.

Remarquons que 3 est un cas particulier de 4 (pourquoi ?). Ce qui explique qu'on ne mentionne jamais cet axiome.
On a donné des caractérisations équivalentes et plus synthétiques dans le chapitre sur les espaces vectoriels.

Là encore :

Proposition 13 : Sev.

Si F est un sev de E, alors les lois de E induisent des lois sur F, et F, muni des lois induites, forme un $\mathbb{K}$-ev.

Proposition 14 .

Un sev d'un sev est un sev.

On n'épilogue pas parce qu'on en a déjà mangé, et qu'on va bientôt en réingurgiter par kilos, des sevs...

II.5 Sous-algèbres

Une sous-algèbre est simultanément un sev et un sous-anneau (pour les lois correspondantes), ce qui en ramène l'étude à celle des sev et des sous-anneaux.

Exemple 13 On a par exemple déjà vu que l'ensemble des suites bornées est une sous-algèbre de l'algèbre de toutes les suites à valeurs dans $\mathbb{K}$.

III Morphismes

III.1 Morphismes de groupe

(a) Définition

Définition 16 : Morphisme de groupe.

Étant donnés deux groupes $(G_1,\star)$ et $(G_2,\square)$, on appelle **morphisme de groupe** (mdg) de $(G_1,\star)$ dans $(G_2,\square)$ une application $f : G_1 \to G_2$ qui préserve la structure de groupe, c'est-à-dire telle que :

i/ $f(e_1) = e_2$

ii/ $\forall x \in G_1, f(x^{-1}) = f(x)^{-1}$

iii/ $\forall (x,y) \in G_1^2, f(x\star y) = f(x)\square f(y)$

Donnons tout de suite une caractérisation plus simple des morphismes de groupe :

Théorème 6 : Morphisme de groupe.

Étant donnés deux groupes $(G_1,\star)$ et $(G_2,\square)$, une application $f : G_1 \to G_2$ est un mdg si et seulement si elle préserve les produits, c'est-à-dire $\forall (x,y) \in G_1^2, f(x\star y) = f(x)\square f(y)$.

Démonstration. L'implication directe est évidente. Reste à montrer qu'une application qui préserve les produits préserve l'élément neutre et les symétriques. Soit f une telle application d'un groupe $(G_1,*)$ dans un groupe $(G_2,\square)$.

1. On a $f(e_1) = f(e_1 * e_1) = f(e_1)\square f(e_1)$. Comme on peut « simplifier »une égalité au sein d'un groupe (on multiplie par l'inverse), on obtient : $e_2 = f(e_1)$. Ainsi f préserve bien les éléments neutres.
2. On sait maintenant que f préserve les éléments neutres.
   Soit $x \in G_1$. On a $f(x)\square f(x^{-1}) = f(x*x^{-1}) = f(e_1) = e_2$. Par unicité du symétrique , on a donc $f(x^{-1}) = f(x)^{-1}$.
   Ainsi f préserve bien les symétriques.

□

Exemple 14 Ainsi :

⟶ $\varphi : \left\{ \begin{array}{ccc} \mathbb{R} & \to & \mathbb{U} \\ t & \mapsto & \mathrm{e}^{it} \end{array} \right.$ est un morphisme de groupe.

⟶ $\varphi : \left\{ \begin{array}{ccc} \mathbb{R}^\times & \to & \mathbb{R}_+^\times \\ x & \mapsto & |x| \end{array} \right.$ est un morphisme de groupe.

⟶ $\varphi : \left\{ \begin{array}{ccc} \mathbb{R}^\times & \to & \{\pm 1\} \\ x & \mapsto & \mathrm{sg}(x) \end{array} \right.$ est un morphisme de groupe.

⟶ Si H est un sous-groupe strict de $(G,\cdot)$, l'injection canonique $\iota : \left\{ \begin{array}{ccc} H & \to & G \\ x & \mapsto & x \end{array} \right.$ est un morphisme de groupe.

Définition 17 : Isomorphisme de groupe.

On appelle **isomorphisme de groupe** un morphisme de groupe bijectif.

Exemple 15 Aucun des exemples de 14 n'est un morphisme de groupe.
Par contre :

$$\longrightarrow \varphi : \left\{ \begin{array}{ccc} \mathbb{Z}/4\mathbb{Z} & \to & \mathbb{U}_4 \\ 0 & \mapsto & 1 \\ 1 & \mapsto & i \\ 2 & \mapsto & -1 \\ 3 & \mapsto & -i \end{array} \right. \text{ est un isomorphisme de groupe.}$$

$$\longrightarrow \varphi : \left\{ \begin{array}{ccc} \mathbb{R}^\times & \to & \mathbb{R}_+^\times \times \{\pm 1\} \\ x & \mapsto & (|x|, \mathrm{sg}(x)) \end{array} \right. \text{ est un isomorphisme de groupe.}$$

Lorsqu'il existe un isomorphisme entre deux groupes $(G_1, \star)$ et $(G_2, \square)$, on dit que ces deux groupes sont **isomorphes** et on note $(G_1, \star) \simeq (G_2, \square)$.

D'après un théorème du cours, un isomorphisme de groupe a une application réciproque. Le théorème suivant est un raffinement de ce théorème :

Théorème 7 : Isomorphisme de groupe.

L'application réciproque d'un isomorphisme de groupe est un isomorphisme de groupe.

C'est d'ailleurs la "bonne" définition d'un isomorphisme.

Démonstration. Soit $(G_1, \star)$ et $(G_2, \square)$ deux groupes et $f : G_1 \to G_2$ un isomorphisme de groupe.

Ainsi f^{-1} existe et est bijectif. Reste à montrer que f^{-1} est un morphisme de groupe, c'est-à-dire d'après le théorème 6 qu'on a $\forall X, Y \in G_2,\ f^{-1}(X \square Y) = f^{-1}(X) \star f^{-1}(Y)$.

Soient $X, Y \in G_2$. On a :

$$\begin{array}{rcll} f^{-1}(X \square Y) & = & f^{-1}(f(f^{-1}(X)) \square f(f^{-1}(Y))) & \\ & = & f^{-1}(f(f^{-1}(X) \star f^{-1}(Y))) & \text{car } f \text{ est un morphisme} \\ & = & f^{-1}(X) \star f^{-1}(Y) & \text{car } f^{-1} \circ f = \mathrm{id} \end{array}$$

Et boum. □

Proposition 15 : Préservation des propriétés par isomorphisme.

Si $(G_1, \star)$ et $(G_2, \square)$ sont isomorphes, alors $(G_1, \star)$ est commutatif si et seulement si $(G_2, \square)$ l'est.

(b) Structure catégorielle

Théorème 8 : Structure catégorielle.

i/ L'identité d'un groupe est toujours un morphisme de groupe.

ii/ La composée de deux morphismes de groupes est un morphisme de groupe.

(c) Image et noyau

Définition 18 : Image, Noyau.

Étant donné un morphisme de groupe $f : (G_1, \star) \to (G_2, \square)$, on appelle :

- Noyau de f la partie de G_1 suivante : $\mathrm{Ker}(f) = \{x \in G_1,\ f(x) = e_2\} = f^{\leftarrow}(\{e_2\})$.
- Image de f la partie de G_2 suivante : $\mathrm{Im}(f) = \{f(x),\ x \in G_1\} = f^{\rightarrow}(G_1)$.

Théorème 9 : Caractérisation de l'injectivité et la surjectivité.

Soit f un mdg de $(G_1, \star)$ dans $(G_2, \square)$

i/ f est surjective si et seulement si $\mathrm{Im}(f) = G_2$

ii/ f est injective si et seulement si $\mathrm{Ker}(f) = \{e_1\}$

iii/ f est un isomorphisme si et seulement si $\mathrm{Im}(f) = G_2$ et $\mathrm{Ker}(f) = \{e_1\}$.

Démonstration.

i/ Déjà vu dans le chapitre sur l'ordre supérieur.

ii/ Implication directe : supposons f injective.
Alors comme f est un morphisme de groupes, on a $f(e_1) = e_2$, ce qui signifie qu'on a $e_1 \in \mathrm{Ker}(f)$. Mais par définition $\mathrm{Ker}(f) = f^{-1}\big(\{e_2\}\big)$ et, par injectivité de f, tout élément de G_2 possède au plus un antécédent par f. Ainsi e_2 en particulier possède au plus un antécédent par f. On en connaît déjà un ; il s'agit de e_1. C'est donc le seul. Ainsi $\mathrm{Ker}(f) = \{e_1\}$.

Réciproquement, supposons qu'on ait $\mathrm{Ker}(f) = \{e_1\}$. Montrons que f est injective. Soient x, y dans G et supposons $f(x) = f(y)$. On a alors : $f\big(x * y^{-1}\big) = f(x)\square f(y = f(x)\square f(y)^{-1} = f(y)\square f(y)^{-1} = e_2$.
Ainsi $x * y^{-1} \in \mathrm{Ker}(f)$ et donc $x * y^{-1} = e_1$, d'où en composant à droite par y : $x = y$.

iii/ = i/+ii/. □

Exemple 16 Lorsqu'on a montré que $P \mapsto \widetilde{P}$ est injective, on a en fait montré sans le dire que son noyau était réduit au polynôme nul !

Théorème 10 : Structure d'un noyau, d'une image.

Soit f un mdg de $(G_1, \star)$ dans $(G_2, \square)$

i/ $\mathrm{Ker}(f)$ est un sous-groupe de $(G_1, \star)$

ii/ $\mathrm{Im}(f)$ est un sous-groupe de $(G_2, \square)$

Démonstration. On va montrer les deux résultats plus généraux suivants :

i/ L'image directe d'un sous-groupe par un morphisme de groupe est un sous-groupe ;

ii/ L'image réciproque d'un sous-groupe par un morphisme de groupe est un sous-groupe.

C'est parti.

i/ Soit H_1 un sous-groupe de $(G_1, *)$ et notons $H_2 = \{f(h),\ h \in H_1\}$ son image directe par f. Montrons que H_2 est un sous-groupe de $(G_2, \square)$.

- $e_1 \in H_1$ car H_1 est un sous-groupe, donc $e_2 = f(e_1) \in H_2$.
- Soit $x \in H_2$. Il existe alors $h \in H_1$ tel que $x = f(h)$ et par suite on a $x^{-1} = f(h)^{-1} = f(h^{-1}) \in H_2$ car $h^{-1} \in H_1$ puisque H_1 est un sous-groupe.
- Soient $x, x' \in H_2$. Il existe alors $h, h' \in H_1$ tels que $x = f(h)$ et $x' = f(h')$. Par suite on a $x\square x' = f(h)\square f(h') = f(h * h') \in H_2$ car $h * h' \in H_1$ puisque H_1 est un sous-groupe.

ii/ Soit H_2 un sous-groupe de $(G_2, \square)$ et notons $H_1 = \{g \in G_1,\ f(g) \in H_2\}$ son image réciproque par f. Montrons que H_1 est un sous-groupe de $(G_1, *)$.

- $f(e_1) = e_2 \in H_2$ car H_2 est un sous-groupe, donc $e_1 \in H_1$.
- Soit $x \in H_1$. On a alors $f(x) \in H_2$ et donc $f(x^{-1}) = f(x)^{-1} \in H_2$ puisque H_2 est un sous-groupe. On a donc bien $x^{-1} \in H_1$, par définition.
- Soient $x, x' \in H_1$. On a alors $f(x) \in H_2$ et $f(x') \in H_2$ d'où, puisque H_2 est un sous-groupe, $f(x * x') = f(x)\square f(x') \in H_2$. On a donc bien $x * x' \in H_1$. □

III.2 Morphismes d'anneau

(a) Morphisme d'anneau et de corps

Définition 19 : Morphisme d'anneau.

Étant donnés deux anneaux $(A,+_A,\times_A)$ et $(B,+_B,\times_B)$, on appelle **morphisme d'anneau** (mda) de $(A,+_A,\times_A)$ dans $(B,+_B,\times_B)$ une application $f:A\to B$ qui préserve la structure d'anneau, c'est-à-dire tq :

i/ $f(0_A)=0_B$

ii/ $\forall x\in A, f(-x)=-f(x)$

iii/ $\forall (x,y)\in A^2, f(x+_A y)=f(x)+_B f(y)$

iv/ $f(1_A)=1_B$

v/ $\forall (x,y)\in A^2, f(x\times_A y)=f(x)\times_B f(y)$

Donnons tout de suite une caractérisation plus simple des morphismes d'anneau :

Proposition 16 : Morphisme d'anneau.

Étant donnés deux anneaux $(A,+_A,\times_A)$ et $(B,+_B,\times_B)$, une application $f:A\to B$ est un mda ssi

i/ $\forall (x,y)\in A^2, f(x+_A y)=f(x)+_B f(y)$

ii/ $f(1_A)=1_B$

iii/ $\forall (x,y)\in A^2, f(x\times_A y)=f(x)\times_B f(y)$

Démonstration. Résulte immédiatement de la caractérisation des morphismes de groupe. □

Exemple 17 Ainsi :

⟶ L'application $\varphi:\left\{\begin{array}{ccc}\mathbb{R}[X]&\to&\mathbb{R}\\ P(X)&\mapsto&P(42)\end{array}\right.$ est un morphisme d'anneau.

⟶ Si A est un sous-anneau strict de $(B,+,\times)$, l'injection canonique $\iota:\left\{\begin{array}{ccc}A&\to&B\\ x&\mapsto&x\end{array}\right.$ est un morphisme d'anneau.

Définition 20 : Isomorphisme d'anneau.

On appelle **isomorphisme d'anneau** un morphisme d'anneau bijectif.

Comme pour les groupes :

Proposition 17 : Isomorphisme d'anneau.

L'application réciproque d'un isomorphisme d'anneau est un isomorphisme d'anneau.

Lorsque deux anneaux $(A,+_A,\times_A)$ et $(B,+_B,\times_B)$ sont isomorphes on note $(A,+_A,\times_A)\simeq(B,+_B,\times_B)$.

Définition 21 : Morphisme de corps.

Étant donnés deux corps $(\mathbb{K}_A,+_A,\times_A)$ et $(\mathbb{K}_B,+_B,\times_B)$, on appelle **morphisme de corps** de $(\mathbb{K}_A,+_A,\times_A)$ dans $(\mathbb{K}_B,+_B,\times_B)$ une application $f:\mathbb{K}_A\to\mathbb{K}_B$ qui préserve la structure de corps, c'est-à-dire telle que :

i/ $f(0_A)=0_B$

ii/ $\forall x\in A, f(-x)=-f(x)$

iii/ $\forall (x,y)\in \mathbb{K}_A^2, f(x+_A y)=f(x)+_B f(y)$

iv/ $f(1_A)=1_B$

v/ $\forall (x,y)\in \mathbb{K}_A^2, f(x\times_A y)=f(x)\times_B f(y)$

vi/ $\forall x\in \mathbb{K}_A^\times, f(x^{-1})=f(x)^{-1}$

Donnons tout de suite deux caractérisations plus simples des morphismes de corps :

Proposition 18 : Morphisme de corps.

Étant donnés deux corps $(\mathbb{K}_A,+_A,\times_A)$ et $(\mathbb{K}_B,+_B,\times_B)$ et une application $f:\mathbb{K}_A\to\mathbb{K}_B$, sont équivalentes :

a. f est un morphisme de corps

b. f est un morphisme d'anneau de $\mathbb{K}_A$ dans $\mathbb{K}_B$

c. i/ $f(1_A)=1_B$

ii/ $\forall (x,y)\in A^2, f(x+_A y)=f(x)+_B f(y)$

iii/ $\forall (x,y)\in A^2, f(x\times_A y)=f(x)\times_B f(y)$

Exercice : S'en convaincre.

Proposition 19 : Préservation des propriétés par isomorphisme.

Soient $(A, +_A, \times_A)$ et $(B, +_B, \times_B)$ deux anneaux isomorphes.

i/ A est commutatif si et seulement si B est commutatif

ii/ A est intègre si et seulement si B est intègre

iii/ A est un corps si et seulement si B est un corps

(b) Structure catégorielle

Proposition 20 : Structure catégorielle.

i/ L'identité d'un anneau est toujours un morphisme d'anneau.

ii/ La composée de deux morphismes d'anneaux est un morphisme d'anneau.

(c) Image et noyau

Même définition que pour les groupes, même utilité que pour les groupes :

Définition 22 : Image, Noyau.

Pour f un mda de $(A, +_A, \times_A)$ dans $(B, +_B, \times_B)$

- Noyau de f : $\mathrm{Ker}(f) = \{x \in A,\ f(x) = 0_B\}$.
- Image de f : $\mathrm{Im}(f) = \{f(x),\ x \in A\}$.

Proposition 21 : Caractérisation de l'injectivité et la surjectivité.

Pour f un mda de $(A, +_A, \times_A)$ dans $(B, +_B, \times_B)$

i/ f est surjective si et seulement si $\mathrm{Im}(f) = B$

ii/ f est injective si et seulement si $\mathrm{Ker}(f) = \{0_A\}$

iii/ f est un isomorphisme si et seulement si $\mathrm{Im}(f) = B$ et $\mathrm{Ker}(f) = \{0_A\}$.

Attention, le noyau d'un morphisme d'anneau n'est jamais un sous-anneau, sauf si B est l'anneau nul.

III.3 Applications linéaires

(a) Définition

Définition 23 : Application linéaire.

Étant donnés un corps $\mathbb{K}$ et deux $\mathbb{K}$-espaces vectoriels $(E_1, +, \cdot)$ et $(E_2, +, \cdot)$, on appelle **application linéaire** ("morphisme d'espace vectoriel") de $(E_1, +, \cdot)$ dans $(E_2, +, \cdot)$ une application $f : E_1 \to E_2$ qui préserve la structure d'espace vectoriel, c'est-à-dire telle que :

i/ $f(0) = 0$

ii/ $\forall x \in E_1, \forall \lambda \in \mathbb{K} f(\lambda x) = \lambda f(x)$

iii/ $\forall (x, y) \in E_1^2, f(x + y) = f(x) + f(y)$

On a là aussi une caractérisation équivalente des applications linéaires :

Théorème 11 : Application linéaire.

$f : E_1 \to E_2$ est une application linéaire ssi on a : $\forall (x, y) \in E_1^2, \forall (\lambda, \mu) \in \mathbb{K}^2, f(\lambda x + \mu y) = \lambda f(x) + \mu f(y)$.

Exemple 18 On ne peut pas dire qu'on n'en a jamais vu ! Entre mille :

⟶ Les applications $M \mapsto {}^tM$ ou $M \mapsto Tr(M)$ sont linéaires !

⟶ La dérivation est linéaire. Une application de la forme $f \mapsto \int_a^b f$ est linéaire.

⟶ Étant donné un $\mathbb{K}$-ev E de dimension finie n et une base $\mathcal{B}$ de E, l'application "décomposition dans la base $\mathcal{B}$" : $\vec{u} \mapsto \begin{vmatrix} \\ \vec{u} \\ \\ \end{vmatrix}_{\mathcal{B}}$ est linéaire.

(b) Structure catégorielle

Théorème 12 : Structure catégorielle.

i/ L'identité d'un espace vectoriel est toujours une application linéaire.

ii/ La composée de deux application linéaires est une application linéaire.

(c) Image et noyau

Définition 24 : Image, Noyau.

Pour $f : E_1 \to E_2$ une application linéaire, on appelle :

- Noyau de f la partie de E_1 suivante : $\mathrm{Ker}(f) = \{x \in E_1,\ f(x) = 0\}$.
- Image de f la partie de E_2 suivante : $\mathrm{Im}(f) = \{f(x),\ x \in E_1\}$.

Théorème 13 : Caractérisation de l'injectivité et la surjectivité.

Pour $f : E_1 \to E_2$ une application linéaire :

i/ f est surjective si et seulement si $\mathrm{Im}(f) = E_2$

ii/ f est injective si et seulement si $\mathrm{Ker}(f) = \{0\}$

iii/ f est un isomorphisme si et seulement si $\mathrm{Im}(f) = E_2$ et $\mathrm{Ker}(f) = \{0\}$.

Théorème 14 : Structure d'un noyau, d'une image.

$\mathrm{Ker}(f)$ et $\mathrm{Im}(f)$ sont des sous-espaces vectoriels .

IV Conclusion

On a donc fait un bilan des différentes structures déjà rencontrées ou à venir. On retiendra particulièrement :

Sur les structures :
- Les définitions de groupe, anneau, corps, espace vectoriel, algèbre.
- Quelques exemples de groupes, notamment S_n.
- La version générale du binôme de Newton et de l'identité géométrique dans un anneau.

Sur les sous-structures :
- Qu'un sous-truc est un machin inclus dans le truc *stable pour la structure de truc.*
- Qu'un sous-truc est un truc.
- Qu'un sous-truc d'un sous-truc est un sous-truc.

Sur les morphismes :
- Qu'un morphisme de truc est une application entre trucs *qui préserve la structure de truc.*
- Le fait qu'un isomorphisme préserve les propriétés remarquables.
- Les définitions et propriétés du noyau et de l'image d'un morphisme de truc.