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 la loi $\cdot$ qui nous autorise à écrire $a \cdot b \cdot c$ au lieu de $(a \cdot b) \cdot c$ ou $a \cdot (b \cdot c)$ (puisque ces expressions sont égales).

Exemple 1 Exemples ? Contre-exemples ? ?

Définition 2 : Commutativité.

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

Exemple 2 Exemples ? Contre-exemples ? ?

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.

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 ci-dessous deux exemples immédiats et évidents :

Théorème 4 : 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. ....
2. ....
   ....

Remarque 2

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

Théorème 5 : Symétrique d'un produit.

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

La démonstration consiste simplement à écrire l'associativité.

Définition 6 : 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

Théorème 7 : Groupe produit.

Les groupes produits sont des groupes.

I.2 Anneaux

Définition 8 : 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 :

Définition 9 : Commutativité.

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

Exemple 5 Exemples ? Contre-exemples ? ?

Deux théorèmes évidents sur les anneaux :

Théorème 10 : 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.

Théorème 11 : 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 12 : Binôme de Newton.

Démonstration. En TD.

Théorème 13 : Identité géométrique généralisée.

Démonstration. En TD.

Définition 14 : Intégrité.

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

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 : 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 Exemples ? Contre-exemples ? ?

Définition 15 : 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 ....

Proposition-Définition 16 : Groupe des inversibles d´un anneau.

Étant donné un anneau $(A, +_A, \times_A)$ on note $A^\times$ l'ensembles des inversibles de A (pour $\times_A$).
$(A^\times, \times_A)$ forme un groupe, on l'appelle **groupe des inversibles de** $(A, +_A, \times_A)$.

Exemple 8

I.3 Corps

Définition 17 : 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 de la façon qu'on a déjà vue :

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

Exemple 9 Exemples ? Contre-exemples ? ?

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

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

Théorème 18 .

Un corps est un anneau intègre.

Ceci nous donne un argument rapide pour voir que $\mathcal{M}_n(\mathbb{R})$ n'est pas un corps, puisqu'on sait qu'il n'est pas intègre. Notons que la réciproque est fausse puisque $\mathbb{Z}$ est intègre.

DÉMONSTRATION.

I.4 Espaces vectoriels sur un corps

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

Définition 19 : 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 Exemples ?

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 :

Théorème 20 : $\mathbf{0_K}$ 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 21 : Opposé et multiplication externe.

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

Théorème 22 : 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 :

$$\lambda \cdot x = 0_E \Leftrightarrow \lambda = 0_{\mathbb{K}} \text{ ou } x = 0_E.$$

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 du thèorème 20. 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 le thèorème 20.

I.5 Algèbre (unitaire, sur un corps)

Définition 23 : $\mathbb{K}$-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 Exemple ?

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 24 : 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 25 : 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

Une autre remarque intéressante :

Théorème 26 : Transitivité de "être un sous-groupe de".

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

Remarque 4

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

II.2 Sous-anneaux

Définition 27 : 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. $\forall (x, y) \in B, x \times y \in B$.

Là encore :

Théorème 28 : 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.

Théorème 29 .

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

Remarque 5

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 : pourquoi ?

II.3 Sous-corps

Définition 30 : 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 A 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 Ł $\setminus \{0\}$ **est dans** L.

Là encore :

Théorème 31 : 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.

Théorème 32 .

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

II.4 Sous-espace vectoriel

Définition 33 : 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.

Là encore :

Théorème 34 : 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.

Théorème 35 .

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

III Morphismes

III.1 Morphismes de groupe

(a) Définition

Définition 36 : 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 37 : 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.

Exemple 14

Définition 38 : Isomorphisme de groupe.

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

Exemple 15 Exemples ? Contre-exemples ?

....

....

....

....

....

....

....

....

....

....

....

....

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 39 : 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.

Proposition 40 : 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 41 : 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 42 : 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 : $Ker(f) = \{x \in G_1,\ f(x) = e_2\} =$ ....
- Image de f la partie de G_2 suivante : $Im(f) = \{f(x),\ x \in G_1\} =$ ....

Théorème 43 : 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 $Im(f) = G_2$

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

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

Démonstration.

i/

ii/

iii/ = i/+ii/.

Exemple 16

Théorème 44 : Structure d'un noyau, d'une image.

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

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

ii/ $Im(f)$ est un sous-groupe de $(G_2, \star)$

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.

III.2 Morphismes d'anneau

(a) Morphisme d'anneau et de corps

Définition 45 : 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 :

Théorème 46 : 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

Définition 47 : Isomorphisme d'anneau.

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

Comme pour les groupes :

Théorème 48 : Isomorphisme d'anneau.

L'application réciproque d'un isomorphisme d'anneau est un morphisme 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 49 : 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 :

Théorème 50 : 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 51 : 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

Théorème 52 : 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 53 : Image, Noyau.

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

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

Théorème 54 : 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 $Im(f) = B$

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

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

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 55 : 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 56 : 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 !

(b) Structure catégorielle

Théorème 57 : 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 58 : Image, Noyau.

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

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

Théorème 59 : 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 $Im(f) = E_2$

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

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

Théorème 60 : Structure d'un noyau, d'une image.

$Ker(f)$ et $Im(f)$ 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.