Bilan sur les structures algébriques.

I Structures

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).

Définition 2 : Commutativité.

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

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 $\{1, 2, \dots, n\}$.

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.

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 $(xy)^{-1} = y^{-1}x^{-1}$.

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 $(x_1, x_2) \star (y_1, y_2) = (x_1 \cdot y_1, x_2 * y_2)$

Proposition 2 : Groupe produit.

Les groupes produits sont des groupes.

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.

Définition 6 : Commutativité.

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

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 $\forall a \in A, a \times 0_A = 0_A$.

Proposition 4 : Opposé et multiplication.

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

Théorème 2 : Binôme de Newton.

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

Théorème 3 : Identité géométrique généralisée.

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

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 $b = 0_A$.

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.

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 $\exists k \in A, b = a \times k$.

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 $A^\times$.

Théorème 4 : Groupe des inversibles d'un anneau.

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

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 $+$

Proposition 5 .

Un corps est un anneau intègre.

I.4 Espaces vectoriels sur un corps

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 $\mathbb{Q}$.

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 $\forall \lambda \in \mathbb{K}, \lambda \cdot 0_E = 0_E$.

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 $x = 0_E$.

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 : $(a \cdot x) \times (b \cdot y) = (a \times_{\mathbb{K}} b) \cdot (x \times y)$.

II Sous-structures

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.

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. $\forall (x, y) \in B^2, x \times y \in B$.

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.

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 Ł $\setminus \{0\}$ **est dans** L.

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. $\forall x \in F, \forall \lambda \in \mathbb{K}, \lambda x \in F$.

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.

II.5 Sous-algèbres

III Morphismes

III.1 Morphismes de groupe

Définition 16 : Morphisme de groupe.

Étant donnés deux groupes $(G_1,\star)$ et $(G_2,\Box)$, on appelle **morphisme de groupe** (mdg) de $(G_1,\star)$ dans $(G_2,\Box)$ 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/ $\forall (x,y) \in G_1^2, f(x \star y) = f(x) \Box f(y)$

Théorème 6 : Morphisme de groupe.

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

Définition 17 : Isomorphisme de groupe.

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

Théorème 7 : Isomorphisme de groupe.

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

Proposition 15 : Préservation des propriétés par isomorphisme.

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

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.

Définition 18 : Image, Noyau.

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

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 $\mathrm{Ker}(f) = \{e_1\}$.

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

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

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

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

III.2 Morphismes d'anneau

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

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

Définition 20 : Isomorphisme d'anneau.

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

Proposition 17 : Isomorphisme d'anneau.

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

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

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

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

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.

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 $\mathrm{Ker}(f) = \{0_A\}$.

III.3 Applications linéaires

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

Théorème 11 : Application linéaire.

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

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.

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