Cours : Structures algèbriques

Table des matières

1 Groupe

1.1 Loi de composition interne

Définition 1. *Soit E un ensemble. On appelle loi de composition interne toute application $\star$ de $E \times E$ dans E :*

$$\begin{array}{rcl} \star : E \times E & \longrightarrow & E \\ (x, y) & \longmapsto & x \star y \end{array}$$

Définition 2. *La loi $\star$ est dite*
— *associative lorsque :*

$$\forall x, y, z \in E \quad (x \star y) \star z = x \star (y \star z)$$

— *commutative lorsque :*

$$\forall x, y \in E \quad x \star y = y \star x$$

Remarque :

⇨ L'addition et la multiplication sont des lois de composition interne associatives et commutatives sur $\mathbb{C}$. Le pgcd est une loi de composition interne associative et commutative sur $\mathbb{Z}$. La composition est une loi de composition interne sur $\mathcal{F}(\mathbb{R}, \mathbb{R})$, associative mais pas commutative. Enfin, l'exponentiation est une loi de composition interne sur $\mathbb{N}$ qui n'est ni associative, ni commutative.

Définition 3. *Une partie A de E est dite stable par $\star$ lorsque :*

$$\forall x, y \in A \quad x \star y \in A$$

Remarque :

⇨ Si $\star$ est une loi de composition interne sur E et $A \in \mathcal{P}(E)$ est stable par $\star$, alors la loi

$$\begin{array}{rcl} \star_A : A \times A & \longrightarrow & A \\ (x, y) & \longmapsto & x \star y \end{array}$$

est une loi de composition interne sur A que l'on continuera à noter $\star$.

Définition 4. *On dit que $\star$ admet un élément neutre $e \in E$ lorsque :*

$$\forall x \in E \quad x \star e = e \star x = x$$

Si tel est la cas, il est unique et on l'appelle élément neutre de $\star$. Lorsque la loi est notée additivement, l'élément neutre est noté 0.

Exercice :

⇨ Parmi les lois de composition interne citées plus haut, lesquelles admettent un élément neutre ?

Remarque :

⇨ Dans toute la suite de ce cours, on supposera, sauf mention explicite du contraire, que les lois sont associatives et admettent un élément neutre.

Définition 5. *Soit $x \in E$. On définit x^n pour tout $n \in \mathbb{N}$ par récurrence :*
— $x^0 = e$
— $\forall n \in \mathbb{N} \quad x^{n+1} = x^n \star x$
Lorsque la loi est notée additivement, on le note $n \cdot x$. On a alors :
— $0 \cdot x = 0$
— $\forall n \in \mathbb{N} \quad (n+1) \cdot x = n \cdot x + x$

Proposition 1. *Soit $x \in E$. Alors :*

$$\forall m, n \in \mathbb{N} \qquad \begin{array}{l} x^{m+n} = x^m \star x^n \\ (x^m)^n = x^{mn} \end{array}$$

Si $x, y \in E$ commutent, c'est-à-dire si $x \star y = y \star x$, on a :

$$\forall n \in \mathbb{N} \quad (x \star y)^n = x^n \star y^n$$

Remarque :

⇨ Pour calculer x^4, on peut commencer par calculer $x \star x$, puis multiplier deux fois ce résultat par x. Cette méthode nécessite 3 multiplications. On peut cependant faire plus rapide et se limiter à 2 multiplications : il suffit de calculer $x \star x$ et de multiplier le résultat obtenu par lui-même. Plus généralement, pour calculer x^n pour $n \in \mathbb{N}$, on peut suivre l'algorithme récursif suivant :
—Si $n = 0$, alors la réponse est e.
—Si n est pair, alors il existe $k \in \mathbb{N}$ tel que $n = 2k$. On calcule alors de manière récursive x^k, résultat qu'il suffit de multiplier par lui-même pour obtenir x^n.
—Si n est impair, alors il existe $k \in \mathbb{N}$ tel que $n = 2k + 1$. On calcule alors de manière récursive x^k, résultat qu'il suffit de multiplier par lui-même, puis par x pour obtenir x^n.
On peut montrer que cet algorithme, appelé *méthode d'exponentiation rapide*, nécessite asymptotiquement $\log_2 n$ multiplications, contrairement à l'algorithme naïf qui s'effectue asymptotiquement en n multiplications.

Définition 6. *Soit $x \in E$. On dit que x est symétrisable pour la loi $\star$ lorsqu'il existe $y \in E$ tel que :*

$$x \star y = y \star x = e$$

Si tel est le cas, y est unique et est appelé symétrique de x. On l'appelle inverse de x et on le note x^{-1} lorsque la loi est notée multiplicativement et on l'appelle opposé de x et on le note $-x$ lorsque la loi est notée additivement.

Proposition 2.
— *Si x est symétrisable, x^{-1} l'est et :*

$$\left(x^{-1}\right)^{-1} = x$$

— *Si x et y sont symétrisables, $x \star y$ l'est et :*

$$(x \star y)^{-1} = y^{-1} \star x^{-1}$$

Définition 7. *Soit $x \in E$. Si x est symétrisable, on étend la définition de x^n en posant :*

$$\forall n \in \mathbb{Z} \quad x^n = \begin{cases} x^n & si\ n \geqslant 0 \\ (x^{-n})^{-1} & si\ n \leqslant 0 \end{cases}$$

Proposition 3. *Soit $x \in E$. Si x est symétrisable :*

$$\forall m, n \in \mathbb{Z} \qquad x^{m+n} = x^m \star x^n$$
$$(x^m)^n = x^{mn}$$

Si $x, y \in E$ sont symétrisables et commutent, alors :

$$\forall n \in \mathbb{Z} \quad (x \star y)^n = x^n \star y^n$$

Définition 8. *On dit qu'un élément x de E est régulier lorsque :*

$$\forall y, z \in E \quad x \star y = x \star z \implies y = z$$
$$y \star x = z \star x \implies y = z$$

Proposition 4. *Les éléments inversibles sont réguliers.*

1.2 Groupe

Définition 9. *Soit G un ensemble muni d'une loi de composition interne $\star$. On dit que $(G, \star)$ est un groupe lorsque :*
— *$\star$ est associative*
— *$\star$ admet un élément neutre*
— *tout élément de G est symétrisable.*
Le groupe $(G, \star)$ est dit commutatif (ou abélien) lorsque la loi $\star$ est commutative.

Remarques :

⇨ $(\mathbb{C}, +)$ et $(\mathbb{C}^*, \cdot)$ sont des groupes commutatifs.

⇨ Si $(G, \star)$ est un groupe et $x \in G$, les applications

$$\tau_g : \begin{array}{ccc} G & \longrightarrow & G \\ g & \longmapsto & x \star g \end{array} \qquad \text{et} \qquad \tau_d : \begin{array}{ccc} G & \longrightarrow & G \\ g & \longmapsto & g \star x \end{array}$$

sont des bijections de G appelées respectivement translation à gauche et à droite.

⇨ Si $(G, \star)$ est un groupe fini, on appelle table de $(G, \star)$ le tableau à deux entrées dont les lignes et les colonnes sont toutes deux indexées par les éléments de G et qui contient les produits $g_1 \star g_2$. Puisque $(G, \star)$ est un groupe, un des ses éléments sera l'élément neutre, et puisque les translations à gauche et à droite sont des bijections, chaque ligne et chaque colonne contiendra une et une seule fois chaque élément de G.

Exercice :

⇨ Déterminer la table d'un groupe à 3 éléments.

Définition 10. *Soit $(G, \star)$ un groupe et H une partie de G. On dit que H est un sous-groupe de G lorsque :*
— $e \in H$
— $\forall x, y \in H \quad x \star y \in H$
— $\forall x \in H \quad x^{-1} \in H$
Si tel est le cas $(H, \star)$ est un groupe.

Remarques :

⇨ Si $(G, \star)$ est un groupe, G et $\{e\}$ sont des sous-groupes de G.

⇨ $(\mathbb{R}, +)$, $(\mathbb{Q}, +)$, $(\mathbb{Z}, +)$ sont des sous-groupes de $(\mathbb{C}, +)$. De même $(\mathbb{U}, \cdot)$, $(\mathbb{R}^*, \cdot)$, $(\mathbb{Q}^*, \cdot)$ sont des sous-groupes de $(\mathbb{C}^*, \cdot)$.

⇨ En pratique, pour montrer que $(G, \star)$ est un groupe, on le fera presque toujours apparaître comme sous-groupe d'un groupe connu.

⇨ Pour montrer que H est un sous-groupe de $(G,\star)$, il ne faut surtout pas oublier de vérifier que $H \subset G$. En pratique, on n'en parle pas lorsque c'est trivial, mais il ne faut surtout pas oublier de le vérifier lorsque l'inclusion est plus subtile.

⇨ On peut montrer qu'une partie H de G est un sous-groupe de $(G,\star)$ si et seulement si $e \in H$ et $\forall x,y \in H \quad x \star y^{-1} \in H$. Bien que cette méthode fait économiser quelques lignes dans un devoir, elle a l'inconvénient de concentrer les difficultés. On évitera donc de l'utiliser lorsque la démonstration demandée n'est pas immédiate.

Proposition 5. *Si $n \in \mathbb{N}^*$, $(\mathbb{U}_n,\cdot)$ est un groupe dont l'élément neutre est 1.*

Proposition 6. *Soit E un ensemble. On note $\sigma(E)$ l'ensemble des bijections de E dans E. Alors $(\sigma(E),\circ)$ est un groupe, appelé groupe des permutations de E, dont l'élément neutre est Id_E.*

Exercice :

⇨ Montrer que l'ensemble des bijections croissantes de $\mathbb{R}$ dans $\mathbb{R}$ est un sous-groupe de $(\sigma(\mathbb{R}),\circ)$.

Proposition 7. *L'intersection d'une famille de sous-groupes est un sous-groupe.*

Remarque :

⇨ Contrairement à l'intersection, l'union de deux sous-groupes n'est en général pas un sous-groupe.

Définition 11. *Soit $(G,\star)$ un groupe et A une partie de G. Alors, il existe un plus petit sous-groupe de G contenant A ; on l'appelle groupe engendré par A et on le note $\mathrm{Gr}(A)$.*

Remarque :

⇨ Si $(G,\star)$ est un groupe et x est un élément de G, le groupe engendré par $\{x\}$, appelé abusivement groupe engendré par x, est $\left\{x^k : k \in \mathbb{Z}\right\}$.

Exercice :

⇨ Soit $n \in \mathbb{N}^*$ et $\omega = e^{i\frac{2\pi}{n}}$. On se place dans le groupe $(\mathbb{U}_n,\cdot)$. Montrer que si $k \in \mathbb{Z}$, le groupe engendré par ω^k est égal à $\mathbb{U}_n$ si et seulement si k et n sont premiers entre eux.

Définition 12. *Soit $(G_1,\star_1)$ et $(G_2,\star_2)$ deux groupes. On dit qu'une application φ de G_1 dans G_2 est un morphisme de groupe lorsque :*

$$\forall x,y \in G_1 \quad \varphi(x \star_1 y) = \varphi(x) \star_2 \varphi(y)$$

Plus précisément, on dit que φ est un :
- *endomorphisme lorsque $(G_1,\star_1) = (G_2,\star_2)$.*
- *isomorphisme lorsque φ est bijective*
- *automorphisme lorsque φ est un endomorphisme et un isomorphisme.*

Remarque :

⇨ L'application φ de $\mathbb{R}$ dans $\mathbb{U}$ qui à θ associe $e^{i\theta}$ est un morphisme du groupe $(\mathbb{R},+)$ dans le groupe $(\mathbb{U},\cdot)$. L'application exp de $\mathbb{R}$ dans $\mathbb{R}_+^*$ est un isomorphisme du groupe $(\mathbb{R},+)$ dans le groupe $(\mathbb{R}_+^*,\cdot)$.

Exercices :

⇨ Déterminer les endomorphismes, puis les automorphismes de $(\mathbb{Z},+)$.

⇨ Quels sont les morphismes de $(\mathbb{Q},+)$ dans $(\mathbb{Z},+)$?

Proposition 8. *Soit φ un morphisme de groupe de $(G_1,\star_1)$ dans $(G_2,\star_2)$. Alors :*

$$\begin{array}{rl} & \varphi(e_1) = e_2 \\ \forall x \in G_1 & \varphi\left(x^{-1}\right) = [\varphi(x)]^{-1} \\ \forall x \in G_1 \quad \forall n \in \mathbb{Z} & \varphi(x^n) = [\varphi(x)]^n \end{array}$$

Proposition 9. *Soit φ un morphisme de $(G_1,\star_1)$ dans $(G_2,\star_2)$. Alors :*
- *L'image réciproque d'un sous-groupe de G_2 est un sous-groupe de G_1.*
- *L'image directe d'un sous-groupe de G_1 est un sous-groupe de G_2.*

Définition 13. *Soit φ un morphisme de $(G_1,\star_1)$ dans $(G_2,\star_2)$. On appelle noyau de φ et on note $\mathrm{Ker}\,\varphi$ l'ensemble :*

$$\mathrm{Ker}\,\varphi = \{x \in G_1 : \varphi(x) = e_2\}$$

C'est un sous-groupe de G_1.

Proposition 10. *Un morphisme φ de $(G_1,\star_1)$ dans $(G_2,\star_2)$ est injectif si et seulement si :*

$$\mathrm{Ker}\,\varphi = \{e_1\}$$

Exercice :

⇨ Soit $(G,\star)$ un groupe et φ l'application de G dans $\sigma(G)$ définie par

$$\begin{array}{rcl} \varphi : G & \longrightarrow & \sigma(G) \\ x & \longmapsto & \varphi(x) : G \longrightarrow G \\ & & \qquad g \longmapsto x \star g \end{array}$$

Montrer que φ est bien définie et que c'est un morphisme injectif de groupe. En déduire que $(G,\star)$ est isomorphe à un sous-groupe du groupe de ses permutations.

Proposition 11.
- *La composée de deux morphismes de groupes est un morphisme de groupe.*
- *La bijection réciproque d'un isomorphisme de groupe est un isomorphisme de groupe.*

Proposition 12. *Si $(G,\star)$ est un groupe, on note $\mathrm{Aut}(G)$ l'ensemble des automorphismes de G. $(\mathrm{Aut}(G),\circ)$ est un groupe.*

Définition 14. *Soit $(G_1, \star_1)$ et $(G_2, \star_2)$ deux groupes. On définit la loi $\star$ sur $G_1 \times G_2$ par :*

$$\forall (x_1, x_2), (y_1, y_2) \in G_1 \times G_2 \quad (x_1, x_2) \star (y_1, y_2) = (x_1 \star_1 y_1, x_2 \star_2 y_2)$$

Alors $(G_1 \times G_2, \star)$ est un groupe d'élément neutre (e_1, e_2) et :

$$\forall (x_1, x_2) \in G_1 \times G_2 \quad (x_1, x_2)^{-1} = \left(x_1^{-1}, x_2^{-1}\right)$$

Exercice :

⇨ Montrer que $\mathbb{C}^*$ est isomorphe à $\mathbb{R}_+^* \times \mathbb{U}$.

1.3 Ordre d'un élément

Proposition 13. *Une partie H de $\mathbb{Z}$ est un sous-groupe de $(\mathbb{Z}, +)$ si et seulement si il existe $n \in \mathbb{N}$ tel que*

$$H = \{kn : k \in \mathbb{Z}\}$$

De plus, si tel est le cas, l'entier n est unique.

Remarque :

⇨ Si $n \in \mathbb{N}$, l'ensemble $\{kn : k \in \mathbb{Z}\}$ est noté $n\mathbb{Z}$.

Définition 15. *Soit $(G, \star)$ un groupe et $x \in G$. Alors, l'application*

$$\begin{array}{rcl} \varphi : \mathbb{Z} & \longrightarrow & G \\ n & \longmapsto & x^n \end{array}$$

est un morphisme du groupe $(\mathbb{Z}, +)$ dans $(G, \star)$.

— *Si $\operatorname{Ker}\varphi = \{0\}$, on dit que x n'a pas d'ordre. Dans ce cas*

$$\forall n \in \mathbb{Z} \quad x^n = e \iff n = 0$$

— *Sinon, il existe un unique $\omega \in \mathbb{N}^*$ tel que $\operatorname{Ker}\varphi = \omega\mathbb{Z}$. On dit que ω est l'ordre de x et on a*

$$\forall n \in \mathbb{Z} \quad x^n = e \iff \omega | n$$

Remarques :

⇨ Dans un groupe, e est l'unique élément d'ordre 1. Dans $(\mathbb{C}^*, \cdot)$, si $n \in \mathbb{N}^*$, l'élément $\omega = e^{i\frac{2\pi}{n}}$ est d'ordre n.

⇨ Soit $(G, \star)$ un groupe et x un élément de G d'ordre fini ω. Alors le groupe engendré par x est $\left\{e, x, x^2, \ldots, x^{\omega-1}\right\}$. En particulier, l'ordre de x est le cardinal du groupe qu'il engendre.

Exercice :

⇨ Soit $(G, \star)$ un groupe et $x \in G$ un élément d'ordre fini n. Pour tout $k \in \mathbb{Z}$, calculer l'ordre de x^k.

Théorème 1. *Soit $(G, \star)$ un groupe fini et x un élément de G. Alors l'ordre de x divise le cardinal de G.*

Remarques :

⇨ Si $(G, \star)$ est un groupe fini, la cardinal de G est aussi appelé ordre de G. La version faible du théorème de Lagrange nous dit donc que dans un groupe fini, l'ordre d'un élément divise l'ordre du groupe.

⇨ La version forte du théorème de Lagrange dit que si $(G, \star)$ est un groupe fini et H est un sous-groupe de $(G, \star)$, alors le cardinal de H divise le cardinal de G. De cette version forte découle la version faible : si $x \in G$, il suffit de remarquer que le cardinal du groupe H engendré par x est l'ordre de x.

Exercices :

⇨ Déterminer les sous-groupes finis de $(\mathbb{U}, \cdot)$.

1.4 Groupe $(\mathbb{Z}/n\mathbb{Z}, +)$

Définition 16. *Soit $n \in \mathbb{N}^*$ et $\mathcal{R}$ la relation d'équivalence définie sur $\mathbb{Z}$ par*

$$\forall a, b \in \mathbb{Z} \quad a\mathcal{R}b \iff a \equiv b \ [n]$$

On appelle $\mathbb{Z}/n\mathbb{Z}$ l'ensemble des classes d'équivalence pour cette relation.

Proposition 14. *Soit $n \in \mathbb{N}^*$. Pour tout $k \in \mathbb{Z}$, on note $\overline{k}$ la classe d'équivalence de k. Alors, les éléments $\overline{0}, \overline{1}, \ldots, \overline{n-1}$ sont deux à deux distincts et :*

$$\mathbb{Z}/n\mathbb{Z} = \left\{\overline{0}, \overline{1}, \ldots, \overline{n-1}\right\}$$

Définition 17. *Soit $n \in \mathbb{N}^*$. On définit la loi de composition interne $+$ sur $\mathbb{Z}/n\mathbb{Z}$ par*

$$\forall k_1, k_2 \in \mathbb{Z} \quad \overline{k_1} + \overline{k_2} = \overline{k_1 + k_2}$$

Alors $(\mathbb{Z}/n\mathbb{Z}, +)$ est un groupe commutatif de cardinal n et d'élément neutre $\overline{0}$.

Remarque :

⇨ Du groupe $(\mathbb{Z}/n\mathbb{Z}, +)$, on retiendra essentiellement le fait que l'application

$$\begin{array}{rcl} \varphi : \mathbb{Z} & \longrightarrow & \mathbb{Z}/n\mathbb{Z} \\ k & \longmapsto & \overline{k} \end{array}$$

est un morphisme surjectif de groupe et que : $\forall k_1, k_2 \in \mathbb{Z} \quad \overline{k_1} = \overline{k_2} \iff k_1 \equiv k_2 \ [n]$.

Exercice :

⇨ Soit $(G, \star)$ un groupe et $x \in G$ un élément d'ordre $n \in \mathbb{N}^*$. Montrer que l'application

$$\begin{array}{rcl} \varphi : \mathbb{Z}/n\mathbb{Z} & \longrightarrow & G \\ \overline{k} & \longmapsto & x^k \end{array}$$

est bien définie et qu'elle réalise un isomorphisme de $\mathbb{Z}/n\mathbb{Z}$ sur le groupe engendré par x.

2 Anneau, corps

2.1 Anneau

Définition 18. *Soit $(A,+)$ un groupe commutatif (d'élément neutre 0_A) et $\times$ une loi de composition interne sur A. On dit que $(A,+,\times)$ est un anneau lorsque :*
- *$\times$ est associatif*
- *$\times$ admet un élément neutre 1_A*
- *$\times$ est distributive par rapport à $+$:*

$$\forall a,b,c\in A \qquad \begin{aligned} a\times(b+c) &= a\times b + a\times c \\ (a+b)\times c &= a\times c + b\times c \end{aligned}$$

Un élément $a\in A$ est dit inversible lorsqu'il est inversible pour la loi $\times$. Un anneau $(A,+,\times)$ est dit commutatif lorsque $\times$ est commutative.

Remarques :

⇨ $(\mathbb{C},+,\cdot)$ et $(\mathbb{R},+,\cdot)$ sont des anneaux.

⇨ Si $(A,+,\cdot)$ est un anneau et X est un ensemble non vide, l'ensemble $\mathcal{F}(X,A)$ muni des lois $+$ et $\cdot$ définies par

$$\forall f,g\in\mathcal{F}(X,A)\quad \forall x\in X\quad \begin{aligned} (f+g)(x) &= f(x)+g(x) \\ (f\cdot g)(x) &= f(x)\cdot g(x) \end{aligned}$$

est un anneau. En particulier $(\mathcal{F}(\mathbb{R},\mathbb{R}),+,\cdot)$ et $(\mathbb{R}^{\mathbb{N}},+,\cdot)$ sont des anneaux.

Proposition 15. *Soit $(A,+,\times)$ un anneau. Alors :*

$$\begin{aligned} \forall a\in A \qquad & 0_A\times a = 0_A \\ \forall a,b\in A \qquad & a\times(-b) = (-a)\times b = -(a\times b) \\ \forall a,b\in A\quad \forall n\in\mathbb{Z} \qquad & (n\cdot a)\times b = a\times(n\cdot b) = n\cdot(a\times b) \end{aligned}$$

Proposition 16. *Soit $(A,+,\times)$ un anneau et $a,b\in A$ tels que $a\times b = b\times a$. Alors :*
- *Si $n\in\mathbb{N}$:*

$$(a+b)^n = \sum_{k=0}^{n}\binom{n}{k}\cdot\left(a^{n-k}\times b^k\right)$$

- *Si $n\in\mathbb{N}^*$:*

$$a^n - b^n = (a-b)\times\left[\sum_{k=0}^{n-1} a^{(n-1)-k}\times b^k\right]$$

Remarques :

⇨ Ces relations peuvent être fausses lorsque a et b ne commutent pas. Par exemple, si a et b sont deux éléments d'un anneau, alors

$$(a+b)^2 = a^2 + 2\cdot a\times b + b^2 \iff a\times b = b\times a$$

⇨ Remarquons que si a est un élément d'un anneau, alors a commute avec 1_A, donc ces formules sont valables pour développer $(1_A+a)^n$ et factoriser $a^n - 1_A$.

Exercice :

⇨ On dit qu'un élément x d'un anneau est nilpotent lorsqu'il existe $n\in\mathbb{N}^*$ tel que $x^n = 0_A$. Montrer que si x est nilpotent, alors $1_A - x$ est inversible.

Définition 19. *Soit $(A,+,\times)$ un anneau. L'ensemble U_A des éléments inversibles de A est un groupe pour la multiplication.*

Définition 20. *On dit qu'un anneau $(A,+,\times)$ est intègre lorsque :*
- *$\times$ est commutative*
- *$\forall a,b\in A \quad a\times b = 0_A \Longrightarrow [a = 0_A \quad ou \quad b = 0_A]$*

Exercice :

⇨ L'anneau $(\mathcal{F}(\mathbb{R},\mathbb{R}),+,\cdot)$ est-il intègre ?

Définition 21. *Soit $(A,+,\times)$ un anneau et B une partie de A. On dit que B est un sous-anneau de A lorsque :*
- *$0_A\in B \quad et \quad 1_A\in B$*
- *$\forall b_1,b_2\in B \quad b_1+b_2\in B, \quad -b_1\in B \quad et \quad b_1\times b_2\in B$*

Si tel est le cas $(B,+,\times)$ est un anneau.

Remarques :

⇨ Si B est un sous-anneau de $(A,+,\times)$, B est un sous-groupe de $(A,+)$.

⇨ Si B est un sous-anneau de $(\mathbb{C},+,\cdot)$, alors $\mathbb{Z}\subset B$.

Exercice :

⇨ Montrer que $\mathbb{Z}[i] = \{a+ib : a,b\in\mathbb{Z}\}$ est un sous-anneau de $\mathbb{C}$.

Définition 22. *Soit $(A,+,\times)$ et $(B,+,\times)$ deux anneaux. On dit qu'une application φ de A dans B est un morphisme d'anneau lorsque :*

$$\begin{aligned} & \varphi(1_A) = 1_B \\ \forall a_1,a_2\in A \qquad & \varphi(a_1+a_2) = \varphi(a_1)+\varphi(a_2) \\ \forall a_1,a_2\in A \qquad & \varphi(a_1\times a_2) = \varphi(a_1)\times\varphi(a_2) \end{aligned}$$

Proposition 17. *Soit φ un morphisme d'anneau de $(A,+,\times)$ dans $(B,+,\times)$. Alors :*

$$\begin{aligned} \forall a\in A\quad \forall n\in\mathbb{Z} \qquad & \varphi(n\cdot a) = n\cdot\varphi(a) \\ \forall a\in A\quad \forall n\in\mathbb{N} \qquad & \varphi(a^n) = [\varphi(a)]^n \end{aligned}$$

De plus, si $a\in A$ est inversible, il en est de même pour $\varphi(a)$ et :

$$\forall n\in\mathbb{Z}\quad \varphi(a^n) = [\varphi(a)]^n$$

Proposition 18.
— *La composée de deux morphismes d'anneaux est un morphisme d'anneau.*
— *La bijection réciproque d'un isomorphisme est un isomorphisme.*

2.2 Corps

Définition 23. *On dit qu'un anneau $(\mathbb{K}, +, \times)$ est un corps lorsque :*
— *$\times$ est commutative*
— *Tout élément non nul de $\mathbb{K}$ admet un inverse pour la loi $\times$*

Proposition 19. *Un corps est intègre.*

Définition 24. *Soit $(\mathbb{L}, +, \times)$ un corps et $\mathbb{K}$ une partie de $\mathbb{L}$. On dit que $\mathbb{K}$ est un sous-corps de $\mathbb{L}$ lorsque :*
— *$\mathbb{K}$ est un sous-anneau de $\mathbb{L}$*
— *$\forall x \in \mathbb{K} \setminus \{0\} \quad x^{-1} \in \mathbb{K}$*
Si tel est le cas, $(\mathbb{K}, +, \times)$ est un corps.

Remarque :

⇨ Si $\mathbb{K}$ est un sous-corps de $(\mathbb{C}, +, \cdot)$, alors $\mathbb{Q} \subset \mathbb{K}$.

Définition 25. *Si $(\mathbb{K}, +, \times)$ et $(\mathbb{L}, +, \times)$ sont deux corps, on appelle morphisme de corps de $\mathbb{K}$ dans $\mathbb{L}$ tout morphisme d'anneau pour les structures sous-jacentes.*

Remarque :

⇨ Les morphismes de corps sont injectifs.

Exercice :

⇨ Déterminer les morphismes de corps φ de $\mathbb{C}$ dans $\mathbb{C}$ tels que : $\forall x \in \mathbb{R} \quad \varphi(x) = x$.

2.3 Anneau $(\mathbb{Z}/n\mathbb{Z}, +, \cdot)$

Définition 26. *Soit $n \in \mathbb{N}^*$. On définit la loi de composition interne $\cdot$ sur $\mathbb{Z}/n\mathbb{Z}$ par*

$$\forall k_1, k_2 \in \mathbb{Z} \quad \overline{k_1} \cdot \overline{k_2} = \overline{k_1 \cdot k_2}$$

Alors $(\mathbb{Z}/n\mathbb{Z}, +, \cdot)$ est un anneau commutatif dont l'élément neutre pour la multiplication est $\overline{1}$.

Proposition 20. *Soit $n \in \mathbb{N}^*$ et $k \in \mathbb{Z}$. Alors $\overline{k}$ est inversible dans $\mathbb{Z}/n\mathbb{Z}$ si et seulement si k est premier avec n.*

Remarque :

⇨ En pratique, si k est premier avec n et que l'on cherche un inverse de $\overline{k}$ dans $\mathbb{Z}/n\mathbb{Z}$, il suffit de trouver une relation de Bézout entre k et n. En effet, si on a trouvé $a, b \in \mathbb{Z}$ tels que $ak + bn = 1$, alors $\overline{a} \cdot \overline{k} = \overline{1}$ donc $\overline{a}$ est l'inverse de $\overline{k}$ dans $\mathbb{Z}/n\mathbb{Z}$.

Proposition 21. *Soit $n \in \mathbb{N}^*$. Alors $(\mathbb{Z}/n\mathbb{Z}, +, \cdot)$ est un corps si et seulement si n est premier.*

Remarque :

⇨ Remarquons que si n n'est pas premier, alors $\mathbb{Z}/n\mathbb{Z}$ n'est pas intègre. En effet, si il existe $p, q \geqslant 2$ tels que $n = p \cdot q$, alors $\overline{p} \cdot \overline{q} = \overline{0}$ alors que $\overline{p}$ et $\overline{q}$ sont non nuls. L'anneau $(\mathbb{Z}/n\mathbb{Z}, +, \cdot)$ est donc soit un corps, soit un anneau non intègre.

Exercice :

⇨ Soit p un nombre premier et $k \in \mathbb{Z}$ tel que $k \wedge p = 1$. Montrer que $k^{p-1} \equiv 1\ [p]$.

3 Espace vectoriel, Algèbres

3.1 Espace vectoriel

Définition 27. *Soit $\mathbb{K}$ un corps, $(E, +)$ un groupe commutatif d'élément neutre 0_E et $\cdot$ une loi de composition externe :*

$$\begin{array}{rcl} \cdot : \mathbb{K} \times E & \longrightarrow & E \\ (\lambda, x) & \longmapsto & \lambda \cdot x \end{array}$$

On dit que $(E, +, \cdot)$ est un $\mathbb{K}$-espace vectoriel lorsque :

$$\begin{array}{lll} \forall x, y \in E \quad \forall \lambda \in \mathbb{K} & \lambda \cdot (x + y) = \lambda \cdot x + \lambda \cdot y \\ \forall x \in E \quad \forall \lambda, \mu \in \mathbb{K} & (\lambda + \mu) \cdot x = \lambda \cdot x + \mu \cdot x \\ \forall x \in E \quad \forall \lambda, \mu \in \mathbb{K} & \lambda \cdot (\mu \cdot x) = (\lambda\mu) \cdot x \\ \forall x \in E & 1_{\mathbb{K}} \cdot x = x \end{array}$$

Les éléments de $\mathbb{K}$ sont appelés scalaires, ceux de E, vecteurs.

Proposition 22. *On a :*

$$\begin{array}{lll} \forall x \in E & 0_{\mathbb{K}} \cdot x = 0_E \\ \forall \lambda \in \mathbb{K} & \lambda \cdot 0_E = 0_E \\ \forall x \in E \quad \forall \lambda \in \mathbb{K} & (-\lambda) \cdot x = \lambda \cdot (-x) = -(\lambda \cdot x) \end{array}$$

Remarque :

⇨ En particulier, si $x \in E$, $(-1) \cdot x = -x$.

Proposition 23. *On a :*

$$\forall x \in E \quad \forall \lambda \in \mathbb{K} \quad \lambda \cdot x = 0_E \quad \Longrightarrow \quad [\lambda = 0_{\mathbb{K}} \quad ou \quad x = 0_E]$$

Définition 28. *Soit $\mathbb{K}$ un corps et $n \in \mathbb{N}^*$. On définit sur $E = \mathbb{K}^n$:*

— *la loi de composition interne $+$ par :*

$$\forall (x_1, \ldots, x_n), (y_1, \ldots, y_n) \in \mathbb{K}^n$$

$$(x_1, \ldots, x_n) + (y_1, \ldots, y_n) = (x_1 + y_1, \ldots, x_n + y_n)$$

— *la loi de composition externe $\cdot$ par :*

$$\forall (x_1, \ldots, x_n) \in \mathbb{K}^n \quad \forall \lambda \in \mathbb{K} \quad \lambda \cdot (x_1, \ldots, x_n) = (\lambda x_1, \ldots, \lambda x_n)$$

Alors $(\mathbb{K}^n, +, \cdot)$ est un $\mathbb{K}$-espace vectoriel d'élément neutre $(0, \ldots, 0)$.

Remarque :

⇨ En particulier, $\mathbb{K}$ est un $\mathbb{K}$-espace vectoriel.

Définition 29. *Soit E un $\mathbb{K}$-espace vectoriel et X un ensemble non vide. On définit sur $\mathcal{F}(X, E)$:*

— *la loi de composition interne $+$ par :*

$$\forall f, g \in \mathcal{F}(X, E) \quad \forall x \in X \quad (f + g)(x) = f(x) + g(x)$$

— *la loi de composition externe $\cdot$ par :*

$$\forall f \in \mathcal{F}(X, E) \quad \forall \lambda \in \mathbb{K} \quad (\lambda \cdot f)(x) = \lambda f(x)$$

Alors $(\mathcal{F}(X, E), +, \cdot)$ est un $\mathbb{K}$-espace vectoriel dont l'élément neutre est l'application de X dans E qui à tout $x \in X$ associe 0_E. En particulier, $(\mathcal{F}(X, \mathbb{K}), +, \cdot)$ est un $\mathbb{K}$-espace vectoriel.

Remarque :

⇨ Muni des lois usuelles, $\mathcal{F}(\mathbb{R}, \mathbb{R})$ et $\mathbb{R}^{\mathbb{N}}$ (l'ensemble des suites réelles) sont des $\mathbb{R}$-espaces vectoriels dont les « zéros » sont respectivement la fonction nulle de $\mathbb{R}$ dans $\mathbb{R}$ et la suite nulle.

Proposition 24. *Soit $(E, +, \cdot)$ un $\mathbb{L}$-espace vectoriel et $\mathbb{K}$ un sous-corps de $\mathbb{L}$. Alors $(E, +, \cdot)$ est un $\mathbb{K}$-espace vectoriel. En particulier $\mathbb{L}$ est un $\mathbb{K}$-espace vectoriel.*

Remarques :

⇨ Muni des lois usuelles, $\mathcal{F}(\mathbb{R}, \mathbb{C})$ est un $\mathbb{C}$-espace vectoriel. Comme $\mathbb{R}$ est un sous-corps de $\mathbb{C}$, $\mathcal{F}(\mathbb{R}, \mathbb{C})$ est aussi un $\mathbb{R}$-espace vectoriel.

⇨ $\mathbb{C}$ est un $\mathbb{R}$-espace vectoriel.

3.2 Algèbre

Proposition 25. *On dit qu'un anneau $(A, +, \times)$ muni d'une loi de composition externe $\cdot$ sur un corps $\mathbb{K}$ est une $\mathbb{K}$-algèbre lorsque :*

— *$(A, +, \cdot)$ est un $\mathbb{K}$-espace vectoriel*

— *$\times$ est compatible avec la loi de composition externe :*

$$\forall x, y \in A \quad \forall \lambda \in \mathbb{K} \quad (\lambda \cdot x) \times y = x \times (\lambda \cdot y) = \lambda \cdot (x \times y)$$

On dit que l'algèbre $(A, +, \cdot, \times)$ est commutative lorsque $\times$ est commutatif.