18. STRUCTURES ALGÉBRIQUES

1 Lois de composition internes.

1.1 Introduction : le rôle des définitions «axiomatiques».

On a pu remarquer au cours des chapitres d'Analyse des «analogies» diverses entre des domaines variés, par exemple la réapparition sous divers déguisements de la relation de Chasles, ou la similitude entre la résolution d'équations différentielles et l'étude de certaines suites numériques. Le cas le plus évident (et dont, historiquement, l'importance fut, de ce fait, la plus difficile à percevoir) est la quasi-identité des règles de calcul dans $\mathbf{Q}$, $\mathbf{R}$, $\mathbf{C}$, $\mathbf{R}(X)$, $\mathcal{C}^\infty(\mathbf{R},\mathbf{R})$, etc. Les premiers exemples analogues non «triviaux» furent étudiés par Gauss (vers 1810), mais il fallut attendre le milieu du $19^{\text{ème}}$ siècle pour que l'on sente la nécessité de définitions précises. La notion de fonction (non-numérique) allait servir de guide, les analogies précédentes étant (comme on le verra plus loin) expliquées comme résultant de l'existence de certaines bijections (les *isomorphismes*) ayant des caractéristiques remarquables; de plus, les «opérations» du calcul usuel furent également interprétées comme des fonctions (ayant certaines propriétés particulières intéressantes); c'est par leur étude que nous allons commencer.

1.2 Lois de composition.

Comme on l'a vu au chapitre 16, une «opération» est une application $(x,y)\mapsto f(x,y)$ qui, à deux objets, en associe un troisième. Toutefois, on utilise, dans l'étude des «structures algébriques», une notation spéciale, généralisant celle des «quatre opérations» : l'image par f de (x,y) se note $x\ f\ y$ (les informaticiens disent qu'il s'agit d'une notation *infixée*, par opposition à la notation *préfixée* usuelle, $f(x,y)$), et le «nom» de l'application f est en fait choisi parmi une (petite) liste de symboles rappelant les opérations usuelles (le plus souvent, $+$, $\times$, $\cdot$, $\star$, $\perp$, $\bullet$, ...); ainsi, une telle application se notera, par exemple, $\star : (x,y)\mapsto x\star y$ (il arrive même fréquemment qu'on utilise tout simplement les conventions usuelles d'écriture des sommes et des produits, comme on l'a vu pour les notations de calcul dans les espaces vectoriels). On dit que $\star$ est une *loi de composition*, allant de $E\times F$ dans G; si $E=F=G$ (le cas le plus fréquent), la loi est dite *loi de composition interne*. Quand les ensembles sont distincts, on parle souvent de loi *externe* (c'est par exemple le cas du produit scalaire associant à deux vecteurs $\mathbf{u}$ et $\mathbf{v}$ le réel $\mathbf{u}\cdot\mathbf{v}$), et plus spécialement, si on étudie une application de $K\times E$ dans E, on dira souvent que K est un ensemble d'opérateurs, ou que K *opère sur* E.

1.3 Propriétés des lois de composition.

L'intérêt des lois de composition étant de permettre des «calculs» analogues aux opérations usuelles, seules les lois présentant certaines des propriétés «évidentes» de l'arithmétique sont utilisées en pratique. Ce sont donc ces propriétés qui ont été dégagées, et auxquelles on a donné des noms; comme on le verra plus loin, des raisonnements généraux permettent alors souvent de déduire d'autres propriétés qui en découlent nécessairement. En un certain sens, la liste qui suit est d'ailleurs «optimale»,

c'est-à-dire que les diverses propriétés données sont *indépendantes* (une loi peut les posséder toutes, sauf une), et qu'elle couvre (à peu près) tout ce qui a été jugé intéressant par les utilisateurs.

Soit donc $\star$ une loi de composition interne sur E (c'est-à-dire que $(x,y) \mapsto x \star y$ est une application de $E \times E$ dans E). On dira que $\star$ est *associative* (ou qu'elle possède la propriété d'*associativité*) si

$$\forall (x,y,z) \in E^3,\ (x \star y) \star z = x \star (y \star z).$$

(ce qui implique qu'on puisse regrouper arbitrairement les calculs «partiels»); ainsi, l'addition (ordinaire) et la multiplication sont associatives, mais pas la soustraction, ni la division, puisque $x-(y-z) = x-y+z \neq (x-y)-z$, et que $(x/y)/z \neq x/(y/z)$. On «oublie» souvent de noter les parenthèses dans les calculs utilisant une loi associative.

On dira que $\star$ est *commutative* (ou qu'elle possède la propriété de *commutativité*) si

$$\forall (x,y) \in E^2,\ x \star y = y \star x.$$

Les lois associatives et commutatives nous sont les plus familières, mais on a vu au précédent chapitre un important exemple de loi non commutative, la multiplication des matrices; une grande prudence s'impose dans de tels cas, pour ne pas se laisser entraîner à des «réflexes» de calcul devenus incorrects.

On dit que $e \in E$ est un *élément neutre* (de E) pour la loi $\star$ si

$$\forall x \in E,\ x \star e = e \star x = x.$$

On démontre (facilement, en appliquant la définition à $e \star e'$, où e et e' sont deux éléments neutres) qu'il ne peut exister qu'un élément neutre (au plus). Dans $\mathbf{C}$, 0 est élément neutre pour $+$, et 1 est élément neutre pour $\times$; dans $\mathcal{M}_2(\mathbf{R})$, $O_2 = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$ est élément neutre pour $+$, et $I_2 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ est élément neutre pour $\times$.

Si la loi $\star$ possède un élément neutre e, on dit que $x \in E$ possède un *symétrique* x' (pour la loi $\star$) si $x \star x' = x' \star x = e$. On démontre comme précédemment que x ne peut posséder qu'un seul symétrique si la loi $\star$ est associative; on note souvent x^{-1} le symétrique de x dans ce cas (et on l'appelle souvent alors l'inverse de x). Dans $\mathbf{C}$, $-x$ est le symétrique de x pour l'addition; si $x \neq 0$, $1/x$ est le symétrique de x pour la multiplication, et 0 n'a pas de symétrique.

On dit que la loi $\star$ est *régulière* si (pour tout a, x et y de E) $a \star x = a \star y \Rightarrow x = y$ et $x \star a = y \star a \Rightarrow x = y$. Cette propriété de «simplification» est en particulier vraie pour une loi associative, pour laquelle a possède un symétrique.

Enfin, la propriété la plus intéressante concernant **deux** lois de composition internes (sur le même ensemble E) est la *distributivité* : si $\star$ et $\perp$ sont ces deux lois, on dit que $\star$ est distributive sur $\perp$ (à droite et à gauche) si, pour tout x, y et z de E,

$$x \star (y \perp z) = (x \star y) \perp (x \star z)$$
$$\text{et}$$
$$(x \perp y) \star z = (x \star z) \perp (y \star z);$$

c'est cette propriété qui justifie les calculs «algébriques» usuels de développements et factorisations.

2 Structures algébriques usuelles.

2. 1 Structures algébriques.

La façon la plus naturelle de généraliser les «calculs» usuels consiste à munir un ensemble d'une ou plusieurs lois de composition, vérifiant certaines des propriétés définies plus haut. On dit alors que l'ensemble est muni d'une certaine *structure*, et les propriétés qui doivent être vérifiées s'appellent les *axiomes* de la structure; ainsi, la phrase «$(E, \perp, \star)$ est un anneau» signifie que $\perp$ et $\star$ sont deux lois de composition interne sur E, et qu'elles vérifient une certaine liste de propriétés (qu'on énoncera plus bas). La théorie se préoccupe alors de deux types de questions : déterminer les autres propriétés qu'on peut déduire, et classifier les différents ensembles ayant la même structure. On a vu ainsi, au chapitre précédent, certains exemples de calculs valables dans tous les espaces vectoriels (par exemple le fait que $0.\mathbf{v}$ est le «vecteur nul»); et le fait que tous les espaces vectoriels ayant la même dimension se «ressemblent» est un exemple de résultat de classification, qui sera énoncé précisément (et démontré) au chapitre 19.

2. 2 Structure de groupe.

Soit E un ensemble muni d'une loi de composition interne $\perp$ On dit que $(E, \perp)$ est un *groupe* si cette loi est associative, possède un élément neutre, et si tout élément de E admet un symétrique, c'est-à-dire qu'on a (pour tout x, y et z de E)

$$x \perp (y \perp z) = (x \perp y) \perp z \text{ (associativité de la loi } \perp),$$

qu'il existe un élément (noté e) de E tel que pour tout x de E

$$x \perp e = e \perp x = x$$

et que pour tout x de E il existe un élément x' de E (le symétrique de x pour $\perp$) tel que

$$x \perp x' = x' \perp x = e.$$

Si de plus la loi $\perp$ vérifie (pour tout x et y de E)

$$x \perp y = y \perp x \qquad \text{(commutativité de } \perp)$$

on dit que $(E, \perp)$ est un groupe *commutatif*, ou *abélien* (dans ce cas, on utilise souvent une notation «additive», et le symétrique de x s'appelle souvent l'*opposé* de x, et est noté $-x$).

$(\mathbf{Z}, +)$ ou $(\mathbf{R}, +)$, $(\mathbf{C}^*, \times)$ sont des exemples «évidents» de groupes (abéliens); l'exercice-type n° 33 indique les moyens de démontrer qu'une loi telle que $x * y = (x + y)/(1 + xy)$ donne à l'ensemble $]-1, 1[$ une structure de groupe. Mais il existe des groupes de types très variés : on rencontrera ainsi en Géométrie (au chapitre 22), des exemples «naturels» de groupes finis; une source importante d'exercices-types consiste à étudier les propriétés d'un ensemble (fini ou infini) de matrices, et à montrer qu'il forme un groupe (pour la multiplication).

2. 3 Anneaux et corps.

Si un groupe abélien $(E, \perp)$ est muni d'une seconde loi de composition interne (notée $\star$), on dit que $(E, \perp, \star)$ est un *anneau* si cette loi est associative, distributive (à

droite et à gauche) sur la loi $\perp$, et s'il existe un élément neutre u pour la loi $\star$ (appelé *élément unité*) *.

Ainsi, $(A, \perp, \star)$ est un anneau si $\forall (x,y,z) \in A^3$,

$$x \perp (y \perp z) = (x \perp y) \perp z$$
$$x \star (y \star z) = (x \star y) \star z$$
$$x \perp y = y \perp x$$
$$x \star (y \perp z) = (x \star y) \perp (x \star z)$$
$$(x \perp y) \star z = (x \star z) \perp (y \star z)$$

(Règles de «calcul»)

et

$$\exists e \in A,\ \forall x \in A,\ x \perp e = e \perp x = x$$
$$\forall x \in A,\ \exists y \in A, x \perp y = y \perp x = e$$
$$\exists u \in A,\ \forall x \in A,\ x \star u = u \star x = x$$

On note souvent 0_A l'élément neutre e de l'anneau $(A, \perp, \star)$ pour la loi $\perp$, et 1_A l'élément unité. Les éléments de A admettant un symétrique (pour la loi $\star$) sont dits *inversibles*, et le symétrique de x s'appelle alors l'*inverse*, et est noté (le plus souvent) x^{-1} (la notation $1/x$ est à proscrire, et x/y doit être remplacé par $x \star y^{-1}$ ou $y^{-1} \star x$, suivant les cas).

Si de plus la loi $\star$ est commutative, l'anneau est dit *commutatif*. Dans ce dernier type d'anneau, les «identités remarquables» sont valables (avec des notations convenables) : si on pose $2_A = 1_A \perp 1_A$ et $x^2 = x \star x$, on a par exemple $(x \perp y)^2 = x^2 \perp y^2 \perp 2_A \star x \star y$ (toutefois, bien des surprises restent possibles; ainsi, il existe des anneaux où $2_A = 0_A$!).

Les situations usuelles de calcul correspondent à des anneaux : c'est le cas de $(\mathbf{Z}, +, \times)$ (mais pas de $(\mathbf{N}, +, \times)$, car $(\mathbf{N}, +)$ n'est pas un groupe), ou de l'anneau des polynômes $\mathbf{R}[X]$ (cette dernière phrase est un grave abus de langage : il faut en fait préciser les deux lois de composition utilisées).

Dans un anneau (ayant au moins deux éléments), on montre aisément que $0_A \neq 1_A$, et que 0_A n'a pas de symétrique (pour la loi $\star$). Si tous les autres éléments de A sont inversibles, on montrera en classe que l'ensemble des éléments non nuls $A^* = A - \{0_A\}$ forme un groupe (pour la loi $\star$). On dit alors que $(A, \perp, \star)$ est un *corps*. Les règles de calcul dans un corps ressemblent suffisamment aux règles de calcul dans $\mathbf{R}$ ou $\mathbf{C}$ pour qu'on note alors les lois $\perp$ et $\star$ par les symboles d'addition et de multiplication ordinaire (ou par des symboles y ressemblant beaucoup); e se note alors 0 (ou un symbole analogue : O, $\mathbf{0}$ ...) et u, l'élément neutre pour $\star$ se note 1 (ou I ...). Il y a cependant encore une propriété élémentaire de la multiplication que ces définitions n'entraînent pas : il existe des corps non commutatifs (mais leur étude est rigoureusement hors-programme).

---

* Il s'agit en fait de ce qu'on appelait autrefois des anneaux *unitaires* : la définition «officielle» ayant changé, le lecteur se méfiera d'énoncés de concours datant d'avant 1990 : les anneaux, jusqu'à cette date, ne comportait pas nécessairement d'éléments unités, et les algèbres étaient donc toutes des anneaux !

2. 4 Espaces vectoriels, algèbres.

La définition des espaces vectoriels donnée au précédent chapitre se généralise en fait ainsi : soit $(E,+)$ un groupe abélien; K un corps commutatif. Si on a une loi «externe» (notée .), application de $K \times E$ dans E ($(x,\mathbf{y}) \mapsto x.\mathbf{y} \in E$), on dit que $(E,+,.)$ est un *K-espace vectoriel* si on a

$$\begin{array}{ll}(\forall a \in K)(\forall \mathbf{x},\mathbf{y} \in E)(a.(\mathbf{x}+\mathbf{y}) = a.\mathbf{x} + a.\mathbf{y}) & \text{(distributivité à droite)}\\ (\forall a,b \in K)(\forall \mathbf{x} \in E)((a+b).\mathbf{x} = a.\mathbf{x} + b.\mathbf{x}) & \text{(distributivité à gauche)}\\ (\forall a,b \in K)(\forall \mathbf{x} \in E)(a(b.\mathbf{x}) = (ab).\mathbf{x}) & \text{(pseudo-associativité)}\\ (\forall \mathbf{x} \in E)(1_K.\mathbf{x} = \mathbf{x}) & (1_K \text{ est élément «unité»})\end{array}$$

Dans le cadre du programme, on prend en général K égal à $\mathbf{R}$ ou $\mathbf{C}$; mais tous les résultats du chapitre précédent sont en fait vrais pour un espace vectoriel sur un corps K commutatif quelconque.

Soit $(E,+,*,.)$ un ensemble muni de deux lois internes $+$ et $*$ et d'une loi externe . telle que $(E,+,.)$ soit un K-espace vectoriel. Si la loi $*$ vérifie (avec la loi $+$) toutes les propriétés de la structure d'anneau, sauf l'existence d'un élément unité (voir note précédente), on dit que E est une *K-algèbre* si les lois vérifient de plus :

$$(\forall a \in K)(\forall \mathbf{x},\mathbf{y} \in E)(a.(\mathbf{x}*\mathbf{y}) = (a.\mathbf{x})*\mathbf{y} = \mathbf{x}*(a.\mathbf{y}))\text{(compatibilité des produits)}$$

Si de plus, $(E,+,*)$ est un anneau, on dit que l'algèbre est *unitaire*. On a vu au précédent chapitre que $\mathcal{M}_n(\mathbf{K},+,.,\times)$ étrait une $\mathbf{K}$-algèbre unitaire; un autre important exemples d'algèbre (l'algèbre des endomorphismes) sera donné dans le prochain chapitre.

2. 5 Sous-structures.

Un sous-ensemble F d'un ensemble E muni d'une structure algébrique est une *sous-structure* (de E) s'il est non vide et stable pour les opérations de E (y compris celles concernant l'existence d'opposés ou d'inverses), c'est-à-dire que la restriction des lois à F est encore «interne», et que F, muni des lois «restreintes», est une structure du même type que E.

Ainsi, par exemple, dans le cas d'une algèbre E, on montre facilement que cela revient à : $(\forall a \in K)(\forall \mathbf{x},\mathbf{y} \in F)(\mathbf{x}+\mathbf{y}, \mathbf{x}*\mathbf{y}, a.\mathbf{x} \in F)$ (car l'opposé de $\mathbf{x}$ est $(-1).\mathbf{x}$). On dira, suivant les cas, que F est un *sous-anneau*, un *sous-espace vectoriel*, une *sous-algèbre* ...

On dispose souvent de caractérisations plus rapides, comme on l'a vu au chapitre précédent : pour que S soit un sous-espace vectoriel de E, il suffit qu'il soit non vide, inclus dans E, et que pour tous $\mathbf{x}$ et $\mathbf{y}$ de S et tout λ de K, on ait $\mathbf{x}+\lambda\mathbf{y} \in S$. De même, pour que $(G',\star)$ soit un sous-groupe de $(G,\star)$, il suffit que G' soit non vide, inclus dans G, et que pour tous x et y de G', on ait $x \star y' \in G'$ (où y' désigne l'élément inverse de y pour la loi $\star$).

3 Morphismes.

3. 1 Définitions générales.

On s'intéresse souvent en algèbre à des applications allant d'une structure (groupe, anneau, algèbre ...) vers une autre de même type, et préservant les opérations. Plus précisément, soit $*$ une loi de composition interne sur E et $\bullet$ une loi de composition

interne sur F ; une application f de E vers F est appelée *morphisme* (de la structure $(E, *)$ vers la structure $(F, \bullet)$) si, pour tout $(x, y) \in E^2$, on a

$$f(x * y) = f(x) \bullet f(y)$$

(qu'on appelle parfois des formules de *transport de structure*). Un exemple typique est l'application $x \mapsto e^x$; on vérifiera que c'est un morphisme de $(\mathbf{R}, +)$ vers $(\mathbf{R}, \times)$.

Plus généralement, si plusieurs lois interviennent, des formules analogues doivent être vérifiées pour toutes les opérations. Ainsi, un morphisme de K-algèbres, allant de $(E, +, ., *)$ vers $(F, \perp, ., \star)$ (où, par commodité, on a noté identiquement la multiplication externe des deux algèbres) est une application f de E vers F telle que, pour tous $\mathbf{x}$ et $\mathbf{y}$ de E, et tout a de K,

$$\begin{aligned} f(\mathbf{x} + \mathbf{y}) &= f(\mathbf{x}) \perp f(\mathbf{y}), \\ f(a.\mathbf{x}) &= af(\mathbf{x}), \text{ et} \\ f(\mathbf{x} * \mathbf{y}) &= f(\mathbf{x}) \star f(\mathbf{y}). \end{aligned}$$

Le mot «morphisme» (qui signifie, à peu près, «qui respecte la forme») est souvent utilisé comme suffixe pour désigner des applications vérifiant certaines propriétés supplémentaires. Par exemple, on a vu que les bijections dérivables à dérivée non nulle s'appellaient des *difféomorphismes*. Dans ce cas, les morphismes qu'on vient de définir sont encore appelés des *homomorphismes*, pour éviter les confusions avec d'autres cas possibles.

Les morphismes «conservent les propriétés algébriques» : on peut montrer par exemple que si e est élément neutre pour $*$ dans E, et si f est un morphisme de $(E, *)$ vers $(F, \bullet)$, $f(e)$ est élément neutre de F (ou plus précisément de $f(E)$). En général, si E est une structure d'un certain type, et si f est un morphisme, $f(E)$ vérifie (par transport de structure) les mêmes axiomes que E ; c'est même un moyen de démontrer rapidement, dans certains cas, que ces axiomes sont effectivement vérifiés par une structure $f(E)$ (mais «deviner» f est alors souvent extrêmement difficile !). Le résultat le plus précis de ce type est la conservation des sous-structures, qui sera vue plus loin.

On appelle *isomorphisme* (de $(E, *)$ vers $(F, \bullet)$, par exemple) une bijection f de E vers F telle que f soit un morphisme (de $(E, *)$ vers $(F, \bullet)$) et que f^{-1} soit un morphisme (de $(F, \bullet)$ vers $(E, *)$) (en pratique, on verra que cette deuxième condition est vérifiée pour les structures usuelles, dès lors que f est bijective).

S'il existe f isomorphisme (de $(E, \ldots)$ vers $(F, \ldots)$), on dit que E et F sont *isomorphes* ; tout se passe alors comme si on pouvait (au moins pour les lois concernées) «identifier» E et F ; c'est ce genre d'argument qui justifie les «analogies» dont on a parlé au début ; on a vu par exemple au chapitre précédent l'existence d'une bijection entre $\mathbf{C}$ et un certain ensemble de matrices (l'application qui envoie $a + ib$ sur la matrice $\begin{pmatrix} a & -b \\ b & a \end{pmatrix}$) ; il est aisé de montrer qu'il s'agit en fait d'un isomorphisme, et il a pu être utilisé pour donner une «définition» des complexes.

Les morphismes entre espaces vectoriels ont reçu un vocabulaire particulier, qui sera détaillé au prochain chapitre : une *application linéaire* est un homomorphisme de K-espaces vectoriels, c'est-à-dire une application f d'un espace vectoriel E dans un espace vectoriel F telle que

$$(\forall k \in K)(\forall \mathbf{x}, \mathbf{y} \in E)(f(\mathbf{x} + k\mathbf{y}) = f(\mathbf{x}) + kf(\mathbf{y}))$$

(on démontre que cette unique formule équivaut aux deux relations de transport de structure vues plus haut). Si $E = F$, on parle d'*endomorphisme* (de E), les bijections linéaires sont appelées des *isomorphismes* (et alors on montre que toutes les propriétés algébriques (telles que la dimension) de E et F sont les mêmes), et les endomorphismes bijectifs sont des *automorphismes*; enfin les applications linéaires de E dans K sont appelées des *formes linéaires*.

3. 2 Morphismes et sous-structures.

Pour les structures usuelles (groupes, anneaux, algèbres, etc.), on a le théorème de transport suivant :

> *L'image et l'image réciproque d'une sous-structure par un morphisme sont des sous-structures.*

(en réalité, cet énoncé n'est pas tout à fait rigoureux : il faudrait plutôt dire, dans chaque cas particulier, que si par exemple $(E, \ldots)$ et $(F, \ldots)$ sont deux algèbres, E_1 et F_1 deux sous-algèbres (respectivement de E et F) et f un morphisme d'algèbres entre E et F, alors $f(E_1)$ est une sous-algèbre de F et $f^{-1}(F_1)$ est une sous-algèbre de E).

Montrons-le par exemple pour la structure de groupe : si $f : G \to H$ est un morphisme (de groupes, où $(G, \star)$ et $(H, \bullet)$ sont des groupes d'éléments neutres respectifs e_1 et e_2) et si G_1 est un sous-groupe de G, $f(G_1) = \{y \in H | \exists x \in G_1,\ y = f(x)\}$ est non vide (il contient $f(e_1) = e_2$) et stable, car $f(x)f(x')^{-1} = f(xx'^{-1})$, f étant un morphisme. On raisonnerait de même (et plus simplement) pour l'image réciproque $f^{-1}(H_2)$ d'un sous-groupe de H.

Il est en particulier souvent commode, pour montrer qu'un ensemble E est un sous-groupe de G, par exemple, de déterminer un morphisme f de G vers un groupe bien connu (comme $(\mathbf{R}, +)$ ou $(\mathbf{C}^*, \times)$), tel que $E = f^{-1}(0)$; on reverra cette idée lors de l'étude des solutions des systèmes linéaires homogènes.

L'image et l'image réciproque d'un sous-espace vectoriel par une application linéaire sont des sous-espaces vectoriels; en particulier on note $\mathrm{Im}(f) = f(E)$ (*image* de f) et $\mathrm{Ker}\,(f) = f^{-1}\{\mathbf{0}\}$ (*noyau* de f). Une étude plus précise de ces notions sera faite au prochain chapitre.

Exercices

1 (R) Dans $\mathbf{N}$, la soustraction est-elle une loi de composition interne? Dans $\mathbf{R}$, la division est-elle une loi de composition interne? Et dans $\mathbf{R}^*$?

2 ($\star\star\star$) Soit $*$ une loi de composition interne sur G, associative, telle qu'il existe un élément $e \in G$ vérifiant $\forall x \in G,\ x * e = x$ et $\forall x \in G,\ \exists x' \in G,\ x * x' = e$. Montrer que $(G, *)$ est un groupe (on commencera par montrer qu'en posant $y = e * x$, on a $y * x' = e$; on utilisera alors $z = (x')'$ pour montrer que $x = y$; on emploiera enfin un argument analogue pour prouver que $x' * x = e$).

3 ($\star\star$) Soit $(A, +, \star)$ un anneau tel que, pour tout $x \in A$, on ait $x \star x = x$ (on dit que A est un anneau *booléen*). Montrer que dans A, seul 1_A est inversible. En calculant de deux manières $(x + x) \star (x + x)$, en déduire que pour tout x de A, $x + x = 0_A$; calculant alors $(x + y) \star (x + y)$, montrer que A est commutatif.

4 ($\star$) Soit $(K,+,\star)$ un corps ; résoudre dans K l'équation $a\star x+b=0_K$, avec x inconnue, a et b constantes de K, et $a\neq 0_K$.

5 ($\star\star$) Montrer que l'ensemble D des nombres divisibles par 5 dans $\mathbf{Z}$ (c'est-à-dire que $D=\{y\in\mathbf{Z}\mid \exists x\in\mathbf{Z},\ y=5x\}$) est un sous-groupe de $(\mathbf{Z},+)$. Pourquoi n'est-ce pas un sous-anneau de $(\mathbf{Z},+,\times)$?

T 33 Soit $\star$ la loi de composition définie sur $E=]-1,1[$ par $x\star y=\dfrac{x+y}{1+xy}$. Montrer que $\star$ est une loi interne sur E, associative. Montrer que l'application $f:x\mapsto \operatorname{th}x$ est un morphisme de $(\mathbf{R},+)$ vers $(E,\star)$, et en déduire que $(E,\star)$ est un groupe abélien.

6 ($\star\star\star$) On pose $x\star y=x\sqrt{y^2+1}+y\sqrt{x^2+1}$; montrer que l'application $x\mapsto \operatorname{sh}x$ est un isomorphisme de $(\mathbf{R},+)$ vers $(\mathbf{R},\star)$ et que $(\mathbf{R},\star)$ est un groupe abélien.

7 ($\star\star\star$) On pose $x\star y=x^{\ln y}$, montrer que la loi $\star$ est une loi de composition interne sur $I=]0,+\infty[$, associative et commutative ; montrer que l'application $x\mapsto e^x$ est un isomorphisme de $(\mathbf{R},+,\times)$ vers $(I,\times,\star)$, et en déduire que $(I,\times,\star)$ est un corps (commutatif).

8 ($\star$) Montrer que l'ensemble des matrices triangulaires supérieures d'ordre n est une sous-algèbre de $\mathcal{M}_n(\mathbf{K})$.

9 ($\star\star\star$), ou peut-être ($\star\star\star\star$) Soit $\mathcal{H}$ l'ensemble des matrices de $\mathcal{M}_2(\mathbf{C})$ de la forme $\begin{pmatrix} z_1 & -\overline{z_2}\\ z_2 & \overline{z_1}\end{pmatrix}$ (on rappelle que $\overline{z}$ est le conjugué de z). Montrer que $(\mathcal{H},+,\times)$ est un corps non commutatif, qu'on appelle le corps des quaternions (on pourra penser à exprimer les matrices de $\mathcal{H}$ à l'aide des matrices $I_2=\begin{pmatrix}1&0\\0&1\end{pmatrix}$, $I=\begin{pmatrix}i&0\\0&-i\end{pmatrix}$, $J=\begin{pmatrix}0&1\\-1&0\end{pmatrix}$ et $K=\begin{pmatrix}0&i\\i&0\end{pmatrix}$).

18. STRUCTURES ALGÉBRIQUES

Plan

1 Lois de composition internes. ..... p. 1

1.1 Introduction : le rôle des définitions «axiomatiques».

1.2 Lois de composition.

1.3 Propriétés des lois de composition.

2 Structures algébriques usuelles. ..... p. 3

2.1 Structures algébriques.

2.2 Structure de groupe.

2.3 Anneaux et corps.

2.4 Espaces vectoriels, algèbres.

2.5 Sous-structures.

3 Morphismes. ..... p. 5

3.1 Définitions générales.

3.2 Morphismes et sous-structures.

Exercices ..... p. 7

18. STRUCTURES ALGÉBRIQUES

(Formulaire)

1 Lois de composition.

Définition 1.1. *On appelle* **loi de composition** *la donnée d'une application f allant d'un produit $E \times F$ dans G (on a donc $f : (x, y) \mapsto z = f((x, y))$), notée sous forme infixée : $(x, y) \mapsto x\, f\, y$.*

Définition 1.2. *Soit E un ensemble, f une application de E^2 dans E, qui à tout couple (x, y) de E^2 associe $f(x, y)$, qu'on notera $x \star y$. On dit alors que $\star$ est une* **loi de composition interne** *(sur E)*

Définition 1.3. *La liste formée d'un ou plusieurs ensembles, et d'une (ou de plusieurs) loi de composition dans ces ensembles (c'est-à-dire, par exemple, le triplet $(E, \perp, \star)$) s'appelle une* **structure**.

Définition 1.4. *On dit qu'une loi de composition interne $\star$ sur E est* **associative** *(ou qu'elle possède la propriété d'***associativité***) si*

$$\forall (x, y, z) \in E^3,\ x \star (y \star z) = (x \star y) \star z$$

Définition 1.5. *On dit qu'une loi de composition interne $\star$ sur E est* **commutative** *(ou qu'elle possède la propriété de* **commutativité***) si*

$$\forall (x, y) \in E^2,\ x \star y = y \star x$$

Définition 1.6. *On dit qu'une loi $\star$ est* **distributive** *sur une loi $\perp$ (à droite et à gauche) si*

$$\forall (x, y, z) \in E^3,\ x \star (y \perp z) = (x \star y) \perp (x \star z)$$

et

$$\forall (x, y, z) \in E^3, (\ x \perp y) \star z = (x \star z) \perp (y \star z)$$

Définition 1.7. *On dit que $e \in E$ est* **élément neutre** *pour la loi de composition interne $\star$ sur E si*

$$\forall x \in E,\ x \star e = e \star x = x.$$

(avec cette définition, il ne peut exister au plus qu'un élément neutre)

Définition 1.8. *Si e est élément neutre pour la loi de composition interne $\star$ sur E, on dit que $x \in E$ a pour* **symétrique** *y (pour la loi $\star$) si $x \star y = y \star x = e$ (on emploie aussi le terme d'***opposé** *(pour les lois associatives et commutatives) et d'***inverse***).*

2 Structures et sous-structures usuelles.

Groupes, anneaux, corps.

Définition 2.1. *On dit que la loi $\star$ munit E d'une* **structure de groupe** *(ou que $(E,\star)$ est un* **groupe***) si $\star$ est une loi de composition interne sur E, associative, possédant un élément neutre, et telle que tout élément possède un symétrique (on note souvent x^{-1} le symétrique de x dans ce cas).*

$(G,\star)$ est donc un groupe si $\forall (x,y)\in G^2,\ x\star y\in G$ et si

$$\begin{aligned}\forall (x,y,z)\in G^3,\ x\star(y\star z)&=(x\star y)\star z,\\ \exists e\in G,\ \forall x\in G,\ x\star e&=e\star x=x \text{ et}\\ \forall x\in G,\ \exists x'\in G,\ x\star x'&=x'\star x=e.\end{aligned}$$

Définition 2.2. *Si, de plus, la loi $\star$ est commutative, on dit que $(G,\star)$ est un* **groupe abélien** *(ou* **commutatif***). Dans ce cas, on note fréquemment l'élément neutre par 0_G, et le symétrique de x par $-x$.*

Définition 2.3. *On appelle* **sous-groupe** *d'un groupe $(G,\star)$ un sous-ensemble G' de G ($G'\subset G$) qui soit un groupe pour la restriction de $\star$ à G'.*

Cela équivaut en fait à : G' est non vide, et «stable» pour les opérations $\star$ et $x\mapsto x^{-1}$ (l'inverse de x), et on a même l'importante caractérisation suivante :

$$(G',\star)\text{ sous-groupe de }(G,\star)\iff\begin{cases}G'\subset G\\ G'\neq\emptyset\text{ (ce qui équivaut à }e\in G')\\ \forall (x,y)\in G'^{\,2},\ x\star y^{-1}\in G'\end{cases}$$

Quelques exemples de groupes usuels : $(\mathbf{Z},+)$, $(\mathbf{C},+)$, $(\mathbf{R}[X],+)$, etc. ; $(\mathbf{R}^*,\times)$, $(\mathbf{R}_+^*,\times)$, $(\{z\in\mathbf{C}\,/\,|z|=1\},\times)$; $(\{f\,/\,f\text{ est une bijection de }E\text{ vers }E\},\circ)$.

Définition 2.4. *On dit que les lois $\perp$ et $\star$ munissent A d'une* **structure d'anneau** *(ou que $(A,\perp,\star)$ est un* **anneau***) si $(A,\perp)$ est un groupe abélien (dont l'élément neutre s'appelle l'***élément nul** *(ou le* **zéro***) de A, et se note souvent 0_A), et si $\star$ est une loi de composition interne sur A, associative, distributive à droite et à gauche sur la loi $\perp$, et possédant un élément neutre (appelé* **élément unité** *de l'anneau, et souvent noté 1_A). Si de plus la loi $\star$ est commutative, on dit que $(A,\perp,\star)$ est un* **anneau commutatif**.

Définition 2.5. *On appelle* **sous-anneau** *d'un anneau $(A,\perp,\star)$ un sous-ensemble A' de A qui soit un anneau pour les restrictions de $\perp$ et $\star$ à A' (avec le même élément unité).*

Cela équivaut à : $1_A\in A'$, et A' «stable» pour les opérations $\perp$, $\star$ et $x\mapsto -x$ (le symétrique de x pour la loi $\perp$), d'o- la caractérisation suivante :

$$(A',\perp,\star)\text{ sous-anneau de }(A,\perp,\star)\iff\begin{cases}A'\subset A\\ 1_A\in A'\\ \forall (x,y)\in A'^{\,2},\ x\perp(-y)\in A'\\ \forall (x,y)\in A'^{\,2},\ x\star y\in A'\end{cases}$$

Quelques exemples d'anneaux usuels : $(\mathbf{Z},+,\times)$, $(\mathbf{C},+,\times)$, $(\mathbf{R}[X],+,\times)$, tous les anneaux d'applications tels que $(\mathcal{C}^\infty(\mathbf{R}),+,\times)$, etc. D'autres exemples sont fournis aux chapitres 17 et 19 (anneaux de matrices et d'applications linéaires).

Définition 2. 6. *On dit que $(K, \perp, \star)$ est un* **corps** *si $(K, \perp, \star)$ est un anneau et si tous les éléments non nuls de K ont un symétrique pour la loi $\star$, c'est-à-dire si $(K - \{0_K\}, \star)$ est un groupe.*

Définition 2. 7. *Si $(K', \perp, \star)$ est un sous-anneau d'un corps $(K, \perp, \star)$, stable pour l'opération de symétrie (pour la seconde loi), on dit que $(K', \perp, \star)$ est un* **sous-corps** *de K.*

Cela équivaut à : $1_K \in K'$, et K' «stable» pour les opérations $\perp$, $\star$, $x \mapsto -x$ et $x \mapsto x^{-1}$ (le symétrique de x pour la loi $\star$), d'o- la caractérisation suivante :

$$(K', \perp, \star) \text{ sous-corps de } (K, \perp, \star) \iff \begin{cases} K' \subset K \\ 1_K \in K' \\ \forall (x, y) \in {K'}^2,\ x \perp (-y) \in K' \\ \forall (x, y) \in K' \times {K'}^*,\ x \star y^{-1} \in K' \\ (\text{o- } {K'}^* = K' - \{0_K\}) \end{cases}$$

Corps usuels : $(\mathbf{Q}, +, \times)$, $(\mathbf{R}, +, \times)$, $(\mathbf{C}, +, \times)$, $(\mathbf{R}(X), +, \times)$.

Espaces vectoriels, algèbres.

Définition 2. 8. *Soit $(E, +)$ un groupe abélien, K un corps, . une loi de composition externe : $(\lambda, x) \in K \times E \mapsto \lambda.x \in E$. On dit que $(E, +, .)$ est un K-* **espace vectoriel** *si*

$$\begin{array}{ll} \forall (a, \mathbf{x}, \mathbf{y}) \in K \times E^2,\ a.(\mathbf{x} + \mathbf{y}) = a.\mathbf{x} + a.\mathbf{y} & \textit{(distributivité à droite)} \\ \forall (a, b, \mathbf{x}) \in K^2 \times E,\ (a + b).\mathbf{x} = a.\mathbf{x} + b.\mathbf{x} & \textit{(distributivité à gauche)} \\ \forall (a, b, \mathbf{x}) \in K^2 \times E,\ a(b.\mathbf{x}) = (ab).\mathbf{x} & \textit{(pseudo-associativité)} \\ \forall \mathbf{x} \in E,\ 1_K.\mathbf{x} = \mathbf{x} & \textit{(1_K est élément «unité»)} \end{array}$$

Définition 2. 9. *On appelle* **sous-espace** *(vectoriel) de $(E, +, .)$, o- $(E, +, .)$ est un K-espace vectoriel, un sous-ensemble non vide de E, stable pour les deux lois.*

On a l'importante caractérisation suivante :

$$S \text{ est un sous-espace vectoriel de } (E, +, .) \iff \begin{cases} S \subset E \\ S \neq \emptyset \text{ (ce qui équivaut à } \mathbf{0}_E \in S) \\ \forall (\lambda, \mathbf{x}, \mathbf{y}) \in K \times S^2,\ \mathbf{x} + \lambda.\mathbf{y} \in S \end{cases}$$

Définition 2. 10. *Soit $(A, +, .)$ un K-espace vectoriel, et $\star$ une loi de composition interne sur A. $(A, +, ., \star)$ est une K-* **algèbre** *si $\star$ est associative, distributive (à droite et à gauche) sur $+$, et si*

$\forall (\lambda, \mathbf{x}, \mathbf{y}) \in K \times A^2,\ \lambda.(\mathbf{x} \star \mathbf{y}) = (\lambda.\mathbf{x}) \star \mathbf{y} = \mathbf{x} \star (\lambda.\mathbf{y})$ *(compatibilité des produits).*

Si, de plus, $(A, +, \star)$ est un anneau, on dit que l'algèbre est **unitaire**

Définition 2. 11. *On appelle* **sous-algèbre** *d'une K-algèbre $(A, +, ., \star)$ un sous-ensemble non vide de A, stable pour les trois lois.*

On a la caractérisation suivante :

$$A' \text{ est une sous-algèbre de } (A, +, ., \star) \iff \begin{cases} A' \subset A \\ A' \neq \emptyset \text{ (ce qui équivaut à } \mathbf{0}_A \in A') \\ \forall (\lambda, \mathbf{x}, \mathbf{y}) \in K \times {A'}^2,\ \mathbf{x} + \lambda.\mathbf{y} \in A' \\ \forall (\mathbf{x}, \mathbf{y}) \in {A'}^2,\ \mathbf{x} \star \mathbf{y} \in A' \end{cases}$$

3 Morphismes.

Définition 3.1. *Soit $(G,*)$ et $(H,\star)$ deux groupes; f, application de G vers H, est un* **morphisme** *(de groupes) si*

$$\forall (x,y)\in G^2,\ f(x*y)=f(x)\star f(y);$$

on démontre (aisément) que cela implique que $f(e_G)=e_H$ et $f(x^{-1})=(f(x))^{-1}$

Si $f:G\to H$ est un morphisme de groupes, et G' et H' des sous-groupes (respectivement) de G et de H, $f(G')$ est un sous-groupe de H, et $f^{-1}(H')$ est un sous-groupe de G.

Définition 3.2. *Soit $(A,+,*)$ et $(B,\perp,\star)$ deux anneaux; f, application de A vers B, est un* **morphisme** *(d'anneaux) si*

$$\begin{aligned}\forall (x,y)\in A^2,\ f(x+y)&=f(x)\perp f(y)\\ \text{et } f(x*y)&=f(x)\star f(y)\end{aligned}$$

Si $f:A\to B$ est un morphisme d'anneaux, et A' et B' des sous-anneaux (respectivement) de A et de B, $f(A')$ est un sous-anneau de B, et $f^{-1}(B')$ est un sous-anneau de A.

Définition 3.3. *Si $(E,+,.)$ et $(F,+,.)$ sont deux K-espaces vectoriels, on dit que $f:E\to F$ est une* **application linéaire** *si*

$$\forall (\lambda,\mathbf{x},\mathbf{y})\in K\times E^2,\ f(\mathbf{x}+\lambda\mathbf{y})=f(\mathbf{x})+\lambda f(\mathbf{y}).$$

Si $f:E\to F$ est une application linéaire, et S et S' des sous-espaces (respectivement) de E et de F, $f(S)$ est un sous-espace de F, et $f^{-1}(S')$ est un sous-espace de E.

Définition 3.4. *Si $(E,+,.,*)$ et $(F,+,.,\star)$ sont deux K-algèbres, on dit que $f:E\to F$ est un* **morphisme d'algèbres** *si f est une application linéaire (de $(E,+,.)$ vers $(F,+,.)$ et si*

$$\forall (\mathbf{x},\mathbf{y})\in E^2,\ f(\mathbf{x}*\mathbf{y})=f(\mathbf{x})\star f(\mathbf{y}).$$

Définition 3.5. *Dans les quatre cas précédents, si f est de plus bijective, on dit que f est un* **isomorphisme**, *et on démontre alors que f^{-1} est aussi un isomorphisme.*