22

Structure de corps

22.1 Corps

Définition 22.1 *Soit $\mathbb{K}$ un ensemble non vide muni de deux lois de composition interne notées $+$ (une addition) et $\cdot$ (une multiplication). On dit que $(\mathbb{K}, +, \cdot)$ est un corps si :*
- *$(\mathbb{K}, +, \cdot)$ est un anneau unitaire (avec $1 \neq 0$) ;*
- *tous les éléments de $\mathbb{K} \setminus \{0\}$ sont inversibles pour la multiplication (ce qui revient à dire que $\mathbb{K}^\times = \mathbb{K} \setminus \{0\}$).*

Si de plus l'anneau $(\mathbb{K}, +, \cdot)$ est commutatif, on dit que le corps $(\mathbb{K}, +, \cdot)$ est commutatif.

Pour un corps on note aussi $\mathbb{K}^*$ l'ensemble $\mathbb{K}^\times = \mathbb{K} \setminus \{0\}$.

Dire que $(\mathbb{K}, +, \cdot)$ est un corps équivaut aussi à dire que :
- $(\mathbb{K}, +, \cdot)$ est un anneau unitaire ;
- $(\mathbb{K}^*, \cdot)$ est un groupe.

Dans un corps, on notera $-a$ l'opposé d'un élément a (i. e. le symétrique pour la loi $+$) et a^{-1} ou $\dfrac{1}{a}$ l'inverse d'un élément non nul a (i. e. le symétrique pour la loi $\cdot$).

Dans un corps tout élément non nul est simplifiable et il n'y a pas de diviseurs de 0. Un corps est donc en particulier un anneau intègre.

Les règles de calcul valables dans un anneau (exercice 21.1) le sont aussi dans un corps avec de plus l'équivalence :

$$ab = 0 \Leftrightarrow a = 0 \text{ ou } b = 0.$$

Dans un corps commutatif, pour $(a, b) \in \mathbb{K}^* \times \mathbb{K}$, on écrira $a^{-1} \cdot b = \dfrac{b}{a}$ (si le corps n'est pas commutatif on a, a priori, $a^{-1} \cdot b \neq b \cdot a^{-1}$ et l'écriture $\dfrac{b}{a}$ est ambiguë).

Exercice 22.1 *Montrer que si $\mathbb{K}$ est un corps, alors l'anneau produit $\mathbb{K}^2 = \mathbb{K} \times \mathbb{K}$ n'est pas un corps.*

Solution 22.1 *Pour $x \in \mathbb{K}^*$, on a $(x, 0) \cdot (0, x) = (0, 0)$, il existe donc des diviseurs de 0 dans l'anneau produit $\mathbb{K}^2$ et en conséquence ce n'est pas un corps.*

Exemple 22.1 *Les ensembles $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ muni des opérations usuelles sont des corps commutatifs. Mais $\mathbb{Z}$ n'est pas un corps.*

Exercice 22.2 *Montrer que l'ensemble :*

$$\mathbb{H} = \left\{ \begin{pmatrix} a & b \\ -\overline{b} & \overline{a} \end{pmatrix} \mid (a, b) \in \mathbb{C}^2 \right\}$$

(où $\overline{a}$ est le nombre complexe conjugué de a) est un corps non commutatif (corps des quaternions de Hamilton).

Solution 22.2 *On montre d'abord que $\mathbb{H}$ est un sous-anneau de $\mathcal{M}_2(\mathbb{C})$. On a $I_2 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \in \mathbb{H}$ et pour $A = \begin{pmatrix} a & b \\ -\overline{b} & \overline{a} \end{pmatrix}$, $B = \begin{pmatrix} a' & b' \\ -\overline{b'} & \overline{a'} \end{pmatrix}$ dans $\mathbb{H}$, on a :*

$$A - B = \begin{pmatrix} a - a' & b - b' \\ -\left(\overline{b - b'}\right) & \overline{a - a'} \end{pmatrix} \in \mathbb{H}$$

et :

$$AB = \begin{pmatrix} aa' - b\overline{b'} & ab' + \overline{a'}b \\ -\left(\overline{ab'} + a'\overline{b}\right) & \overline{aa'} - \overline{b}b' \end{pmatrix} \in \mathbb{H}.$$

Donc $\mathbb{H}$ est un sous-anneau de $\mathcal{M}_2(\mathbb{C})$.
Pour $A = \begin{pmatrix} a & b \\ -\overline{b} & \overline{a} \end{pmatrix} \in \mathbb{H}$ on a $\det(A) = |a|^2 + |b|^2$, de sorte que $\det(A) \neq 0$ pour $A \neq 0$ et A est inversible dans $\mathcal{M}_2(\mathbb{C})$ d'inverse :

$$A^{-1} = \frac{1}{|a|^2 + |b|^2} \begin{pmatrix} \overline{a} & -b \\ \overline{b} & a \end{pmatrix} \in \mathbb{H}$$

Il en résulte que $\mathbb{H}$ est un corps.
Au vu de la formule donnant le produit AB de deux matrices dans $\mathbb{H}$, on voit que ce corps n'est pas commutatif. Par exemple, pour $A = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$, $B = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}$, on a :

$$AB = \begin{pmatrix} -i & 0 \\ 0 & -i \end{pmatrix} \neq BA = \begin{pmatrix} i & 0 \\ 0 & i \end{pmatrix}.$$

Dans un corps on a en général plus de facilités à résoudre certaines équations que dans un anneau.

Par exemple dans un anneau une équation de la forme $ax + b = 0$ n'a pas nécessairement de solution. On peut considérer le cas d'un anneau de matrices. Si A, B sont des matrices réelles d'ordre n, l'équation $AX + B = 0$ équivaut à $AX = -B$ qui donne $\det(A)\det(X) = (-1)^n \det(B)$ et pour A non inversible, B inversible, on aboutit à une impossibilité puisque $\det(A) = 0$ et $\det(B) \neq 0$.

Exercice 22.3 *Soit $(\mathbb{K}, +, \cdot)$ un corps commutatif.*

1. *Montrer que pour tout $(a, b) \in \mathbb{K}^* \times \mathbb{K}$ l'équation $ax + b = 0$ a un unique solution.*
2. *Soit $\lambda \in \mathbb{K}$. Montrer que s'il existe $\alpha \in \mathbb{K}$ tel que $\alpha^2 = \lambda$, alors l'équation $x^2 = \lambda$ a deux solutions exactement dans $\mathbb{K}$, à savoir α et $-\alpha$.*
3. *Soit $(a, b,) \in \mathbb{K}^* \times \mathbb{K}^2$. Montrer que si l'équation $ax^2 + bx + c = 0$ a une solution x_1 dans $\mathbb{K}$, elle en alors une seconde x_2. Dans ce cas, on a $x_1 + x_2 = -\dfrac{b}{a}$, $x_1 x_2 = \dfrac{c}{a}$ et pour tout $x \in \mathbb{K}$, $ax^2 + bx + c = a(x - x_1)(x - x_2)$ (forme factorisée de $ax^2 + bx + c$). Dans un corps commutatif, une équation de degré 2 a donc 0 ou 2 solutions.*

Solution 22.3

1. *Dans le groupe* $(\mathbb{K},+)$, *l'équation* $ax+b=0$ *équivaut à* $ax=-b$ *(unicité de l'opposé) et comme* $a\in\mathbb{K}^*$ *est inversible, l'équation* $ax=-b$ *équivaut à* $a^{-1}ax=a^{-1}(-b)$, *encore équivalent à* $x=-a^{-1}b$. *D'où l'existence et l'unicité dans* $\mathbb{K}$ *de la solution de l'équation* $ax+b=0$.
2. *L'équation* $x^2=\lambda=\alpha^2$ *équivaut à* $x^2-\alpha^2=(x-\alpha)(x+\alpha)=0$ *encore équivalente à* $x=\alpha$ *ou* $x=-\alpha$.
3. *De* $ax_1^2+bx_1+c=0$, *on déduit que pour tout* $x\in\mathbb{K}$, *on a :*

$$\begin{aligned}ax^2+bx+c&=ax^2+bx+c-\left(ax_1^2+bx_1+c\right)\\&=a\left(x^2-x_1^2\right)+b(x-x_1)\\&=(x-x_1)(a(x+x_1)+b)\end{aligned}$$

de sorte que l'équation $ax^2+bx+c=0$ *est équivalente à* $(x-x_1)(a(x+x_1)+b)=0$ *encore équivalent à* $x-x_1=0$ *ou* $a(x+x_1)+b=0$, *la dernière équation ayant pour unique solution* $x_2=-a^{-1}b-x_1$. *Notre équation a donc exactement deux solutions, à savoir* x_1 *et* $x_2=-\dfrac{b}{a}-x_1$. *On a donc* $x_1+x_2=-\dfrac{b}{a}$ *et :*

$$x_1x_2=-\frac{1}{a}\left(bx_1+ax_1^2\right)=-\frac{1}{a}(-c)=\frac{c}{a}.$$

Pour tout $x\in\mathbb{K}$, *on a :*

$$\begin{aligned}ax^2+bx+c&=(x-x_1)(a(x+x_1)+b)\\&=a(x-x_1)\left(x+x_1+\frac{b}{a}\right)\\&=a(x-x_1)(x-x_2).\end{aligned}$$

On a donc montré que ax^2+bx+c *est factorisable dans* K, *si, et seulement si, l'équation* $ax^2+bx+c=0$ *a des solutions dans* $\mathbb{K}$.
Par exemple sur $\mathbb{R}$, *l'équation* x^2+1 *n'est pas factorisable.*

Remarque 22.1 *Dans un corps non commutatif une équation de degré* 2 *peut avoir plus de deux racines, elle peut même en avoir une infinité. Par exemple dans le corps* $\mathbb{H}$ *des quaternions (exercice 22.2) une matrice* $A\in\mathbb{H}$ *est annulée par son polynôme caractéristique* $P(X)=X^2-\operatorname{tr}(A)X+\det(A)$ *(théorème de Cayley-Hamilton) et on peut trouver une infinité de matrices dans* $\mathbb{H}$ *de trace et déterminant donné. Par exemple, pour tout réel* θ, *on a* $A=\begin{pmatrix}1 & e^{it}\\ -e^{-it} & 1\end{pmatrix}\in\mathbb{H}$ *avec* $\operatorname{tr}(A)=\det(A)=2$. *Toutes ces matrices sont solutions de* $X^2-2X+2=0$.

Exercice 22.4 *Montrer qu'un anneau unitaire intègre et fini est un corps.*

Solution 22.4 *Soit* A *un anneau unitaire intègre. Pour tout* $a\neq 0$ *dans* A, *l'application* $x\mapsto ax$ *est injective. En effet si* $ax=a=y$, *alors* $a(x-y)=0$ *et* $x-y=0$ *puisque* A *est intègre et* $a\neq 0$. *Si de plus* A *est fini, alors cette application est bijective et en particulier il existe* $b\in A$ *tel que* $ab=1$, *ce qui prouve que* a *est inversible à droite. On montre de même que* a *est inversible à gauche. On a donc montré que tout élément non nul de* a *est inversible, ce qui revient à dire que* A *est un corps.*

Définition 22.2 *Soit* $(\mathbb{K},+,\cdot)$ *un corps. On dit qu'une partie* $\mathbb{L}$ *de* $\mathbb{K}$ *est un sous-corps de* $\mathbb{K}$ *si :*

- $\mathbb{L}$ *est un sous-anneau de* $\mathbb{K}$ *;*
- $\mathbb{L}^* = \mathbb{L} \setminus \{0\}$ *est stable par passage à l'inverse, c'est-à-dire que pour tout* $x \in \mathbb{L}^*$, x^{-1} *est dans* $\mathbb{L}^*$.

On vérifie facilement qu'un sous-corps d'un corps est lui même un corps.

Théorème 22.1 *Soit* $(\mathbb{K}, +, \cdot)$ *un corps et* $\mathbb{L}$ *une partie non vide de* $\mathbb{K}$. $\mathbb{L}$ *est un sous-corps de* $\mathbb{K}$ *si, et seulement si :*

- $1 \in \mathbb{L}$ *:*
- $\forall (x, y) \in \mathbb{L}^2$, $x - y \in \mathbb{L}$ *;*
- $\forall (x, y) \in \mathbb{L} \times \mathbb{L}^*$, $xy^{-1} \in \mathbb{L}$.

Démonstration. Laissée au lecteur. ∎

Si $\mathbb{L}$ est un sous-corps d'un corps $\mathbb{K}$, on dit alors que $\mathbb{K}$ est une extension de $\mathbb{L}$.

Exemple 22.2 *Les ensembles* $\mathbb{Q}, \mathbb{R}$ *muni des opérations usuelles sont des sous-corps de* $\mathbb{C}$.

Exercice 22.5 *Montrer que le seul sous-corps de* $\mathbb{Q}$ *est lui même.*

Solution 22.5 *Laissée au lecteur.*

Exercice 22.6 *Soit* p *un entier sans facteurs carrés dans sa décomposition en produit de nombres premiers. Montrer que l'ensemble :*

$$\mathbb{Q}\left[\sqrt{p}\right] = \left\{r + s\sqrt{p} \mid (r, s) \in \mathbb{Q}^2\right\}$$

est un sous-corps de $\mathbb{R}$.

Solution 22.6 *On vérifie facilement que* $\mathbb{Q}\left[\sqrt{p}\right]$ *est un sous-anneau de* $\mathbb{R}$ *(même démonstration que pour* $\mathbb{Z}\left[\sqrt{p}\right]$ *déjà rencontré). Comme* $\sqrt{p}$ *est irrationnel, on a* $a = r + s\sqrt{p} = 0$ *si, et seulement si,* $r = s = 0$. *Pour* $a \neq 0$ *dans* $\mathbb{Q}\left[\sqrt{p}\right]$, *on a ;*

$$a^{-1} = \frac{1}{r + s\sqrt{p}} = \frac{r - r\sqrt{p}}{r^2 - ps^2} \in \mathbb{Q}\left[\sqrt{p}\right].$$

En conclusion, $\mathbb{Q}\left[\sqrt{p}\right]$ *est un sous-corps de* $\mathbb{R}$.

Exercice 22.7 *Montrer que l'ensemble :*

$$\mathbb{Q}[i] = \left\{r + si \mid (r, s) \in \mathbb{Q}^2\right\}$$

est un sous-corps de $\mathbb{C}$.

Solution 22.7 *On vérifie facilement que* $\mathbb{Q}[i]$ *est un sous-anneau de* $\mathbb{C}$ *(même démonstration que pour* $\mathbb{Z}[i]$ *déjà rencontré). Pour* $z \neq 0$ *dans* $\mathbb{Q}[i]$, *on a ;*

$$a^{-1} = \frac{1}{r + si} = \frac{r - si}{r^2 + s^2} \in \mathbb{Q}[i].$$

En conclusion, $\mathbb{Q}[i]$ *est un sous-corps de* $\mathbb{C}$.

Exercice 22.8 *Montrer que l'ensemble* $\mathbb{A}$ *des réels algébriques est un corps.*

Solution 22.8 *On sait déjà que* $\mathbb{A}$ *est un sous-anneau de* $\mathbb{R}$.
Si $\alpha \in \mathbb{A}^*$ *est annulé par* $P \in \mathbb{Q}[X] \setminus \{0\}$ *de degré* $n \geq 1$, *alors* $\dfrac{1}{\alpha}$ *est annulé par* $X^n P\left(\dfrac{1}{X}\right) \in \mathbb{Q}[X] \setminus \{0\}$ *et en conséquence est algébrique. On en déduit que* $\mathbb{A}$ *est un sous-corps de* $\mathbb{R}$. *On a ainsi un exemple de corps strictement compris entre* $\mathbb{Q}$ *et* $\mathbb{R}$.

22.2 Morphismes de corps

On désigne par $(\mathbb{K},+,\cdot)$ et $(\mathbb{L},+,\cdot)$ deux corps. On note respectivement 0 et 1 les éléments neutres de ces corps pour l'addition et la multiplication (en cas d'ambiguïté, on les notera $0_{\mathbb{K}}$, $0_{\mathbb{L}}$, $1_{\mathbb{K}}$ et $1_{\mathbb{L}}$).

Définition 22.3 *On dit que φ est un morphisme de corps de $\mathbb{K}$ dans $\mathbb{L}$ si φ est une application de $\mathbb{K}$ dans $\mathbb{L}$ telle que :*

- $\varphi(1)=1$;
- $\forall (a,b)\in A^2,\ \varphi(a+b)=\varphi(a)+\varphi(b)$;
- $\forall (a,b)\in A^2,\ \varphi(a\cdot b)=\varphi(a)\cdot\varphi(b)$

Dans le cas où φ est de plus bijective, on dit que φ est un isomorphisme de corps de $\mathbb{K}$ sur L.
Dans le cas où $\mathbb{K}=\mathbb{L}$, on dit que φ est un endomorphisme du corps $\mathbb{K}$ et que c'est un automorphisme du corps $\mathbb{K}$ si φ est de plus bijective.

On peut remarquer qu'un morphisme de corps est en fait un morphisme d'anneaux unitaires.

On a, pour un tel morphisme, $\varphi(0)=0$, $\varphi(1)=1$, $\varphi(a)=-\varphi(a)$ pour tout $a\in\mathbb{K}$ et $\varphi(a^{-1})=\varphi(a)^{-1}$ pour tout $a\in\mathbb{K}^*$.

Exercice 22.9 *Montrer que l'identité est le seul endomorphisme de corps non identiquement nul de $\mathbb{R}$.*

Solution 22.9 *Si f est endomorphisme du corps $\mathbb{R}$, on a alors $f(x+y)=f(x)+f(y)$ et $f(xy)=f(x)f(y)$ pour tous x,y dans $\mathbb{R}$.*
Avec $f(1)=(f(1))^2$, on déduit que $f(1)=0$ ou $f(1)=1$. Si $f(1)=0$, alors pour tout $x\in\mathbb{R}$ on a $f(x)=f(x)f(1)=0$ et f est identiquement nulle. C'est une homothétie de rapport 0.
On suppose donc que f n'est pas identiquement nulle et on a alors $f(1)=1$.
Avec $f(x^2)=(f(x))^2\geq 0$, on déduit que $f(x)\geq 0$ pour tout $x\geq 0$ et pour $x\geq y$ dans $\mathbb{R}$, on a $f(x)-f(y)=f(x-y)\geq 0$, ce qui signifie que f est croissante. On déduit alors de l'exercice 20.26 que $f(x)=x$ pour tout $x\in\mathbb{R}$ ($\lambda=f(1)=1$). L'identité est donc le seul morphisme de corps non identiquement nul de $\mathbb{R}$ dans lui même.