

**Corrigé partiel du T. D. B6**  
**Structures algébriques**

**3** Soit  $E$  un ensemble.

Les couples  $(\mathcal{P}(E), \cap)$  et  $(\mathcal{P}(E), \cup)$  sont-ils des groupes ?

Non, l'élément neutre de  $\cap$  est  $E$  et l'élément neutre de  $\cup$  est  $\emptyset$ , mais aucun élément non trivial n'admet d'inverse (dès que  $E$  est non-vide).

**4** Soit  $M$  une matrice de taille  $(n, n)$  où  $n \in \mathbb{N}^*$ , à coefficient dans  $\mathbb{K} = \mathbb{R}$  ou  $\mathbb{C}$ . Soit :

$$Z(M) = \{ A \in \text{GL}_n(\mathbb{K}) \mid AM = MA \}.$$

Démontrer que  $Z(M)$  est un sous-groupe de  $(\text{GL}_n(\mathbb{K}), \times)$ .

On vérifie les axiomes de la définition d'un sous-groupe.

(i)  $Z(M) \subseteq \text{GL}_n(\mathbb{K})$  : c'est évident d'après la définition de  $Z(M)$ .

(ii)  $Z(M)$  est non-vide : en effet il contient la matrice identité  $I_n$  car celle-ci commute avec  $M$ , *i.e.*,  $I_n M = M I_n$ .

(iii)  $Z(M)$  est stable par  $\times$  :

Soit  $A$  et  $B$  deux éléments de  $G$ . Alors  $AM = MA$  et  $BM = MB$ .

Donc  $(AB)M = A(BM) = A(MB) = (AM)B = (MA)B = M(AB)$ , par associativité de la loi  $\times$ .

Donc  $AB \in Z(M)$ . Ceci étant vrai pour toutes matrices  $A$  et  $B$  de  $Z(M)$ , on a démontré que  $Z(M)$  est stable par multiplication.

(iv)  $Z(M)$  est stable par passage à l'inverse.

Soit  $A \in Z(M)$ . Alors  $A \in \text{GL}_n(\mathbb{K})$  donc  $A$  est inversible, et  $AM = MA$ .

En multipliant à gauche et à droite par  $A^{-1}$  cette égalité on obtient  $A^{-1}AMA^{-1} = A^{-1}MAA^{-1}$ , donc  $MA^{-1} = A^{-1}M$ . Ceci montre que  $A^{-1} \in Z(M)$ .

On a démontré que  $Z(M)$  est stable par passage à l'opposé.

Les quatre points ci-dessus montrent que  $Z(M)$  est un sous-groupe de  $(\text{GL}_n(\mathbb{K}), \times)$ .

**5** Soit  $(G, *)$  un groupe d'élément neutre  $e$ .

On suppose que pour tout  $x \in G$  :  $x^2 = e$

Démontrer que  $G$  est abélien.

Soit  $x$  et  $y$  deux éléments de  $G$ .

Alors  $x^2 = y^2 = e$ , ce qui montre que  $x^{-1} = x$  et  $y^{-1} = y$ .

De plus  $xy$  appartient à  $G$  donc  $(xy)^2 = e$ , i.e.,  $xyxy = e$ .

En multipliant à gauche par  $x^{-1}$  puis par  $y^{-1}$  on obtient  $yx = x^{-1}y^{-1}$  et donc  $yx = xy$ .

Ceci étant valable pour tout  $(x, y) \in G^2$ , le groupe  $G$  est abélien.

**6** Soit  $(G, *)$  un groupe d'élément neutre  $e$ .

Soit  $x$  et  $y$  deux éléments de  $G$  tels que :

$$xyx = y \quad \text{et} \quad yxy = x$$

Démontrer que  $x^2y^2 = e$  puis que  $x^4 = y^4 = e$ .

Comme  $xyx = y$  alors par multiplication à droite par  $x^{-1}$  on obtient  $xy = yx^{-1}$ .

Comme  $yxy = x$  alors par multiplication à gauche par  $y^{-1}$  on obtient  $xy = y^{-1}x$ .

Ainsi  $yx^{-1} = y^{-1}x$  et donc  $x^2 = y^2$ .

Puis  $x^2y^2 = x(xy)y = x(yx^{-1})y = (xy)x^{-1}y = (y^{-1}x)x^{-1}y = y^{-1}(xx^{-1})y = e$ .

Enfin  $x^4 = x^2y^2 = e$  et de même  $y^4 = e$ .

**7** Soit  $(G, *)$  un groupe fini.

a. Démontrer que dans la table de multiplication de  $G$ , chaque élément de  $G$  apparaît au plus une fois dans chaque colonne et dans chaque ligne.

b. En déduire que chaque élément de  $G$  apparaît une et une seule fois dans chaque colonne et dans chaque ligne de la table de multiplication.

a. Notons  $a_1, \dots, a_n$  les éléments de  $G$ , où  $n \in \mathbb{N}^*$ . On suppose que l'élément neutre est  $e = a_1$ . La table de multiplication de  $G$  est alors :

*	$e$	$a_2$	$\cdots$	$a_j$	$\cdots$	$a_n$
$e$				$\vdots$		
$a_2$				$\vdots$		
$\vdots$				$\vdots$		
$a_i$	$\cdots$	$\cdots$	$\cdots$	$a_i a_j$	$\cdots$	
$\vdots$						
$a_n$						

Supposons qu'un élément  $x$  apparaît deux fois sur une colonne, par exemple sur les lignes  $i$  et  $j$  de la colonne  $k$ . Alors  $x = a_i a_k$  et  $x = a_j a_k$ .

Comme  $G$  est un groupe alors  $a_k$  est inversible, et donc  $a_i = a_j$ . Ceci montre que  $x$  ne peut apparaître que sur une seule ligne de la colonne  $k$ .

De même chaque élément du groupe ne peut apparaître qu'une seule fois sur chaque ligne de la table de multiplication.

- b. Chaque colonne de la table de multiplication contient  $n$  éléments de  $G$ , et ne peut contenir deux fois le même élément, donc elle contient une et une seule fois chaque élément de  $G$ .

De même pour chaque ligne de la table.

Ce résultat peut s'exprimer de la façon suivante :

$$\forall x \in G \quad \forall j \in \{1, \dots, n\} \quad \exists ! i \in \{1, \dots, n\} \quad x = a_i a_j.$$

(Tout élément  $x$  de  $G$  apparaît une et une seule fois sur la colonne  $j$ .)

De façon équivalente :

$$\forall x \in G \quad \forall y \in G \quad \exists ! z \in G \quad x = zy.$$

Ce dernier résultat est effectivement clair car :

$$x = zy \iff z = xy^{-1}.$$

**8** Soit  $(G, *)$  un groupe à trois éléments.  
 Soit  $e, a, b$  ses trois éléments,  $e$  étant le neutre.  
 Donner la table de multiplication de  $G$ .  
 Donner ensuite un exemple de tel groupe.

On note  $e, a, b$  les trois éléments de  $G$ ,  $e$  étant élément neutre. Ainsi  $e, a$  et  $b$  sont distincts. On ne peut avoir  $ab = a$  car sinon on aurait  $b = e$ . On ne peut avoir  $ab = b$  sinon on aurait  $a = e$ , donc  $ab = e$ .

On peut démontrer de même que  $ba = e, a^2 = b^2 = e$ , mais on peut aussi compléter la table de multiplication de  $G$  en jouant au sudoku, d'après les résultats de l'exercice 7.

On obtient la table de multiplication de  $G$  :

*	$e$	$a$	$b$
$e$	$e$	$a$	$b$
$a$	$a$	$b$	$e$
$b$	$b$	$e$	$a$

Deux exemples de tels groupes :  $\mathbb{Z}/3\mathbb{Z}$ , l'ensemble des entiers modulo 3, muni de l'addition, et  $\mathbb{U}_3$  muni de la multiplication.

+	0	1	2		×	1	$j$	$j^2$
0	0	1	2		1	1	$j$	$j^2$
1	1	2	0		$j$	$j$	$j^2$	1
2	2	0	1		$j^2$	$j^2$	1	$j$

**9** Soit  $(G, *)$  un groupe à quatre éléments, et soit  $e$  son élément neutre.

a. On suppose que tout élément  $x$  de  $G$  vérifie  $x^2 = e$ . En notant  $e, a, b, c$  les éléments de  $G$  donner sa table de multiplication.

Le groupe  $G$  est-il commutatif ?

b. On suppose qu'il existe  $a \in G$  tel que  $a^2 \neq e$ .

Donner la table de multiplication de  $G$ .

a. On suppose que  $a^2 = b^2 = c^2 = e$ , donc en utilisant les résultats de l'exercice 7 on peut compléter la table de multiplication de  $G$  :

*	$e$	$a$	$b$	$c$
$e$	$e$	$a$	$b$	$c$
$a$	$a$	$e$	$c$	$b$
$b$	$b$	$c$	$e$	$a$
$c$	$c$	$b$	$a$	$e$

Exemples de tels groupes :  $G = \{\pm 1\}^2$  muni de la multiplication.

Ou l'ensemble des matrices :

$$e = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \quad a = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \quad b = \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix} \quad c = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}$$

muni de la multiplication matricielle.

Ou le sous-groupe des bijections de  $\mathbb{C}$  contenant :

$$e : z \mapsto z \quad a : z \mapsto \bar{z} \quad b : z \mapsto -z \quad c : z \mapsto -\bar{z}$$

muni de la composition des fonctions.

b. Comme  $a^2 \neq a$  et  $a^2 \neq e$  alors on suppose que  $a^2 = b$ , quitte à intervertir  $b$  et  $c$ .

En utilisant les résultats de l'exercice 7 on peut compléter la table de multiplication de  $G$  :

*	$e$	$a$	$b$	$c$
$e$	$e$	$a$	$b$	$c$
$a$	$a$	$b$	$c$	$e$
$b$	$b$	$c$	$e$	$a$
$c$	$c$	$e$	$a$	$b$

On constate que  $c = a^3$ , donc  $G = \{e, a, a^2, a^3\}$  avec  $a^4 = e$ .

Exemples de tels groupes :  $\mathbb{Z}/4\mathbb{Z}$ , l'ensemble des entiers modulo 4, muni de l'addition, et  $\mathbb{U}_4$  muni de la multiplication.

+	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

×	1	$i$	-1	$-i$
1	1	$i$	-1	$-i$
$i$	$i$	-1	$-i$	1
-1	-1	$-i$	1	$i$
$-i$	$-i$	1	$i$	-1

**10** Soit  $(G, *)$  un groupe.

- Démontrer que les applications  $g \mapsto ag$  et  $g \mapsto ga$  sont des bijections de  $G$ .  
Sont-elles des endomorphismes ?
- Démontrer que l'application  $g \mapsto aga^{-1}$  est un automorphisme de  $G$ .
- Donner une condition nécessaire et suffisante pour que l'application  $g \mapsto g^{-1}$  soit un automorphisme de groupe.

- a. Pour tout  $a \in G$  on note  $\varphi_a : G \rightarrow G$   
 $g \mapsto ag$ .

Cette application est bien définie, car si  $a$  et  $g$  appartiennent à  $G$  alors  $ag$  appartient à  $G$ , ceci car la loi de  $G$  est interne.

On remarque que :

$$\forall g \in G \quad \varphi_{a^{-1}} \circ \varphi_a(g) = a^{-1}ag = g.$$

Ainsi  $\varphi_{a^{-1}} \circ \varphi_a = \text{Id}_G$ .

De même  $\varphi_a \circ \varphi_{a^{-1}} = \text{Id}_G$ , donc  $\varphi_a$  est bijective, et de plus sa réciproque est  $\varphi_{a^{-1}}$ .

On démontre de même que  $\psi_a : G \rightarrow G$  est bijective, de réciproque  $\psi_{a^{-1}}$ .

$$g \mapsto ga$$

Soit  $e$  l'élément neutre de  $G$ . Si  $a \neq e$  alors  $\varphi_a(e) = a \neq e$ , donc  $\varphi_a$  n'est pas un morphisme de groupes.

En effet l'image par un morphisme de groupes de l'élément neutre du groupe de départ est l'élément neutre du groupe d'arrivée, et ici  $\varphi_a(e) \neq e$ .

De même  $\psi_a$  n'est pas un morphisme de groupes si  $a \neq e$ .

Si  $a = e$  alors  $\varphi_a = \psi_a = \text{Id}_G$ , il s'agit d'un automorphisme de groupes.

- b. Pour tout  $a \in G$ , soit  $\sigma_a : G \rightarrow G$   
 $g \mapsto aga^{-1}$ .

On peut démontrer directement que  $\sigma_a$  est une bijection de  $G$ , mais on peut aussi remarquer que  $\sigma_a = \varphi_a \circ \psi_{a^{-1}}$  (en utilisant les notations de la question précédente), et donc  $\sigma_a$  est une bijection de  $G$ .

On calcule :

$$\begin{aligned} \forall (x, y) \in G^2 \quad \sigma_a(g)\sigma_a(h) &= (aga^{-1})(aha^{-1}) \\ &= ag(a^{-1}a)ha^{-1} = ageha^{-1} = agha^{-1} = \sigma_a(gh) \end{aligned}$$

Ceci montre que  $\sigma_a$  est un morphisme de groupes.

Celui-ci étant bijectif de  $G$  dans lui-même, c'est un automorphisme de  $G$ .

- c. Notons  $\tau : G \rightarrow G$   
 $g \mapsto g^{-1}$ .

Comme  $G$  est un groupe alors il est stable par passage à l'inverse, *i.e.*, pour tout  $g \in G$  on a  $g^{-1} \in G$ . Ceci montre que l'application  $\tau$  est bien définie.

Supposons que  $\tau$  est un morphisme de groupes. Ceci signifie :

$$\forall (g, h) \in G^2 \quad \tau(gh) = \tau(g)\tau(h).$$

Par équivalences :

$$\begin{aligned}\tau(gh) = \tau(g)\tau(h) &\iff (gh)^{-1} = g^{-1}h^{-1} \\ &\iff gh = (g^{-1}h^{-1})^{-1} = hg\end{aligned}$$

Ainsi  $\tau$  est un morphisme de groupes si et seulement si  $G$  est commutatif.

De plus on remarque que  $\tau \circ \tau = \text{Id}_G$  donc  $\tau$  est bijectif, d'inverse lui-même.

Ainsi  $\tau$  est un automorphisme de groupe si et seulement si  $G$  est commutatif.

**11** Soit  $G$  l'ensemble des bijections de l'ensemble  $X = \{a, b, c\}$ .

a. Justifier que  $(G, \circ)$  est un groupe fini.

b. On note  $e$  l'élément neutre de  $G$ , et  $\tau$  et  $\sigma$  les applications :

$$\begin{array}{ll}\tau : & a \mapsto b \quad \text{et} \quad \sigma : a \mapsto b \\ & b \mapsto a \quad \quad \quad b \mapsto c \\ & c \mapsto c \quad \quad \quad c \mapsto a\end{array}$$

Démontrer que :

$$G = \{e, \sigma, \sigma^2, \tau, \tau\sigma, \tau\sigma^2\}$$

Identifier l'élément  $\sigma\tau$ .

a. Il existe six bijections de  $X$  dans  $X$ , donc le groupe  $G$  contient 6 éléments, et il est fini.

En effet si  $f$  est une bijection de  $X$  alors  $f(a)$  peut prendre l'une des trois valeurs  $a, b, c$ , puis  $f(b)$  prend l'une des deux valeurs restantes, et enfin  $f(c)$  prend la dernière valeur.

Ceci donne donc  $3 \times 2 \times 1 = 6$  possibilités.

b. Plus précisément les six bijections sont les suivantes.

$$\begin{array}{llllll}f_1 : & a \mapsto a & f_2 : & a \mapsto a & f_3 : & a \mapsto b & f_4 : & a \mapsto b & f_5 : & a \mapsto c & f_6 : & a \mapsto c \\ & b \mapsto b & & b \mapsto c & & b \mapsto a & & b \mapsto c & & b \mapsto a & & b \mapsto b \\ & c \mapsto c & & c \mapsto b & & c \mapsto c & & c \mapsto a & & c \mapsto b & & c \mapsto a\end{array}$$

On remarque que  $f_1$  est l'identité de  $X$ , donc l'élément neutre  $e$  de  $G$ .

Par définition  $f_3 = \tau$  et  $f_4 = \sigma$ .

On calcule les trois composées suivantes :

$$\begin{array}{lll}\sigma \circ \sigma : & a \mapsto c & \tau \circ \sigma : & a \mapsto a & \tau \circ \sigma \circ \sigma : & a \mapsto c \\ & b \mapsto a & & b \mapsto c & & b \mapsto b \\ & c \mapsto b & & c \mapsto b & & c \mapsto a\end{array}$$

On constate que  $f_2 = \tau \circ \sigma$ ,  $f_5 = \sigma \circ \sigma$  et  $f_6 = \tau \circ \sigma \circ \sigma$ . Ainsi, en omettant le signe  $\circ$  :

$$G = \{f_1, \dots, f_6\} = \{e, \sigma, \sigma^2, \tau, \tau\sigma, \tau\sigma^2\}$$

On calcule aussi que  $\sigma\tau = f_6 = \tau\sigma^2$ .

On peut aussi remarquer que  $\tau^2 = e$  et  $\sigma^3 = e$ , ce qui permet de calculer tous les produits possibles, et donne la table de multiplication suivante :

$\circ$	$e$	$\sigma$	$\sigma^2$	$\tau$	$\tau\sigma$	$\tau\sigma^2$
$e$	$e$	$\sigma$	$\sigma^2$	$\tau$	$\tau\sigma$	$\tau\sigma^2$
$\sigma$	$\sigma$	$\sigma^2$	$e$	$\tau\sigma^2$	$\tau$	$\tau\sigma$
$\sigma^2$	$\sigma^2$	$e$	$\sigma$	$\tau\sigma$	$\tau\sigma^2$	$\tau$
$\tau$	$\tau$	$\tau\sigma$	$\tau\sigma^2$	$e$	$\sigma$	$\sigma^2$
$\tau\sigma$	$\tau\sigma$	$\tau\sigma^2$	$\tau$	$\sigma^2$	$e$	$\sigma$
$\tau\sigma^2$	$\tau\sigma^2$	$\tau$	$\tau\sigma$	$\sigma$	$\sigma^2$	$e$

On constate que  $G$  n'est pas un groupe commutatif, par exemple  $\tau\sigma \neq \sigma\tau$  puisque  $f_2 \neq f_6$ .

Il s'agit, à isomorphisme près, du plus petit groupe non commutatif.

**12** Le but de cet exercice est de décrire tous les sous-groupes de  $(\mathbb{Z}, +)$ .

a. Démontrer que pour tout  $m \in \mathbb{N}$ ,  $m\mathbb{Z}$  est un sous-groupe de  $\mathbb{Z}$ .

Soit  $H$  un sous-groupe de  $\mathbb{Z}$ .

b. Démontrer que si  $H \cap \mathbb{N}^*$  est non-vide alors il admet un minimum  $m$ , puis que  $H = m\mathbb{Z}$ .

c. Qu'en est-il si  $H \cap \mathbb{N}^*$  est vide ?

d. Conclure.

a. Par définition  $m\mathbb{Z}$  est l'ensemble des multiples de  $m$  :

$$m\mathbb{Z} = \{ma \mid a \in \mathbb{Z}\}$$

Il est inclus dans  $\mathbb{Z}$ , non-vide car il contient 0 par exemple, stable par addition et passage à l'opposé, donc c'est une sous-groupe de  $(\mathbb{Z}, +)$ .

On peut aussi remarquer que l'application

$$\begin{aligned} f : \mathbb{Z} &\longrightarrow \mathbb{Z} \\ a &\longmapsto ma \end{aligned}$$

est un morphisme de groupes, car :

$$\forall (a, b) \in \mathbb{Z}^2 \quad f(a + b) = m(a + b) = ma + mb = f(a) + f(b)$$

Alors l'image de  $f$  est  $\text{im } f = m\mathbb{Z}$ , par propriété c'est un sous-groupe de  $(\mathbb{Z}, +)$ .

b. Supposons que  $H \cap \mathbb{N}^*$  est non-vide. C'est alors une partie non-vide de  $\mathbb{N}$ , donc par propriété elle admet un minimum que l'on note  $m$ .

Démontrons que  $H = m\mathbb{Z}$ .

Tout d'abord  $H$  contient  $m$  car  $m \in H \cap \mathbb{N}^*$ . Comme  $H$  est un sous-groupe de  $(\mathbb{Z}, +)$  alors il contient tous les itérés  $am$  de  $m$  avec  $a \in \mathbb{N}^*$ .

Ensuite, comme  $H$  est un sous-groupe de  $(\mathbb{Z}, +)$  alors il contient son élément neutre 0, donc il contient  $m \times 0$ .

Enfin, toujours comme  $H$  est un sous-groupe de  $(\mathbb{Z}, +)$  alors il est stable par passage à l'opposé, donc il contient tous les  $-ma$  pour  $a \in \mathbb{N}^*$ , et donc finalement  $H$  contient tous les  $ma$  pour  $a \in \mathbb{Z}$ .

On a donc prouvé que  $m\mathbb{Z} \subseteq H$ .

Démontrons l'inclusion inverse.

Soit  $h$  un élément de  $H$ . Comme  $m \in H \cap \mathbb{N}^*$  alors  $m$  est non-nul, donc on peut effectuer la division euclidienne de  $h$  par  $m$  : il existe  $(q, r) \in \mathbb{Z}^2$  tels que  $h = qm + r$  avec  $0 \leq r < m$ .

Alors  $r = h - qm$ . Comme  $h$  et  $qm$  appartiennent à  $H$  alors par stabilité de celui-ci,  $r$  appartient à  $H$ . Si  $r$  est non-nul alors  $r \in H \cap \mathbb{N}^*$ , mais ceci contredit la minimalité de  $m$  en tant qu'élément de  $H \cap \mathbb{N}^*$ . Donc  $r = 0$ , puis  $h = qm$ , et ainsi  $h \in m\mathbb{Z}$ .

On a prouvé que  $H \subset m\mathbb{Z}$ , puis par double inclusion  $H = m\mathbb{Z}$ .

- c. Supposons que  $H \cap \mathbb{N}^*$  est vide. Alors  $H$  ne contient aucun élément strictement positif. Donc il ne contient aucun élément strictement négatif. En effet,  $H$  est stable par passage à l'opposé, donc s'il contenait un élément  $h$  strictement négatif il contiendrait  $-h$  qui serait strictement positif.

Ainsi  $H$  ne peut contenir que l'élément neutre 0. Il le contient bien car c'est un sous-groupe de  $(\mathbb{Z}, +)$ .

Donc dans le cas où  $H \cap \mathbb{N}^*$  est vide on a  $H = \{0\}$ .

On remarque que  $H = m\mathbb{Z}$  avec  $m = 0$ .

- d. Nous avons démontré que les sous-groupes de  $\mathbb{Z}$  sont les  $m\mathbb{Z}$  avec  $m \in \mathbb{Z}$ .

**13** Soit  $\mathbb{K} = \mathbb{R}$  ou  $\mathbb{C}$ , et  $n$  un entier naturel non-nul. On définit l'application :

$$\begin{aligned} f : \mathcal{M}_n(\mathbb{K}) &\longrightarrow \mathcal{M}_n(\mathbb{K}) \\ M &\longmapsto \frac{1}{2}(M + {}^tM) \end{aligned}$$

- a. Justifier que  $f$  est un endomorphisme du groupe  $(\mathcal{M}_n(\mathbb{K}), +)$ .  
b. Déterminer le noyau et l'image de  $f$ .

- a. Soit  $M$  et  $N$  deux matrices de  $\mathcal{M}_n(\mathbb{K})$ . Alors :

$$\begin{aligned} f(M + N) &= \frac{1}{2}((M + N) + {}^t(M + N)) = \frac{1}{2}(M + {}^tM + N + {}^tN) \\ &= \frac{1}{2}(M + {}^tM) + \frac{1}{2}(N + {}^tN) = f(M) + f(N). \end{aligned}$$

Ceci montre que  $f$  est un morphisme du groupe  $(\mathcal{M}_n(\mathbb{K}), +)$  vers lui-même, donc un endomorphisme de groupe de  $(\mathcal{M}_n(\mathbb{K}), +)$ .

- b. L'élément neutre du groupe  $(\mathcal{M}_n(\mathbb{K}), +)$  est la matrice nulle  $0_n$ . Donc :

$$\ker f = \{M \in \mathcal{M}_n(\mathbb{K}) \mid f(M) = 0_n\}.$$

Par équivalence :

$$\forall M \in \mathcal{M}_n(\mathbb{K}) \quad f(M) = 0_n \iff {}^tM = -M.$$



Ceci montre que le noyau de  $f$  est l'ensemble des matrices antisymétriques de taille  $(n, n)$  :  $\ker f = \mathcal{A}_n(\mathbb{K})$ .

On démontre par double inclusion que l'image de  $f$  est l'ensemble des matrices symétriques de taille  $(n, n)$  :  $\text{im } f = \mathcal{S}_n(\mathbb{K})$ .

L'image de  $f$  contient toutes les matrices  $f(M)$  pour  $M \in \mathcal{M}_n(\mathbb{K})$ . Or :

$${}^t(f(M))r = {}^t\left(\frac{1}{2}(M + {}^tM)\right) = \frac{1}{2}({}^tM + M) = f(M).$$

Ceci montre que  $f(M)$  est symétrique, ceci pour tout  $M \in \mathcal{M}_n(\mathbb{K})$ , donc  $\text{im } f \subseteq \mathcal{S}_n(\mathbb{K})$ .

Réciproquement, soit  $M \in \mathcal{S}_n(\mathbb{K})$ , *i.e.*,  $M$  est une matrice symétrique.

Alors  $f(M) = \frac{1}{2}(M + M) = M$ , donc  $M \in \text{im } f$ . Ceci montre que  $\mathcal{S}_n(\mathbb{K}) \subseteq \text{im } f$ .

Par double inclusion :  $\text{im } f = \mathcal{S}_n(\mathbb{K})$ .

**14** Soit  $G = \mathbb{R}^* \times \mathbb{R}$  muni de la loi  $*$  définie par :

$$\forall ((x, y), (x', y')) \in G^2 \quad (x, y) * (x', y') = (xx', yx' + y')$$

a. Démontrer que  $(G, *)$  est un groupe.

Est-il abélien ?

b. Démontrer  $H = \{(x, 0) \mid x \in \mathbb{R}^*\}$  et  $K = \{(1, y) \mid y \in \mathbb{R}\}$  sont deux sous-groupes abéliens de  $(G, *)$ .

c. Démontrer que les applications :

$$\begin{array}{ccc} \varphi : (\mathbb{R}^*, \times) & \longrightarrow & G \\ x & \longmapsto & (x, 0) \end{array} \quad \text{et} \quad \begin{array}{ccc} \psi : (\mathbb{R}, +) & \longrightarrow & G \\ y & \longmapsto & (1, y) \end{array}$$

sont des morphismes de groupes.

d. Donner les noyaux et les images de ces morphismes. Que retrouve-t-on ?

a. Vérifions les axiomes de définition d'un groupe.

(i) La loi  $*$  est une loi de composition interne de  $G$ .

Soit  $(x, y)$  et  $(x', y')$  deux éléments de  $G$ , c'est-à-dire que  $x, y, x', y'$  sont quatre réels avec  $x$  et  $x'$  non-nuls.

Alors  $(x, y) * (x', y') = (xx', yx' + y')$ . Comme  $x$  et  $x'$  sont non-nuls alors  $xx'$  est non-nul, et donc  $(x, y) * (x', y')$  appartient bien à  $\mathbb{R}^* \times \mathbb{R}$ , c'est-à-dire à  $G$ .

Ceci montre que  $*$  est une loi de composition interne de  $G$ .

(ii) La loi  $*$  est associative.

Soit  $(x, y)$ ,  $(x', y')$ , et  $(x'', y'')$  trois éléments de  $G$ . Alors :

$$\begin{aligned} [(x, y) * (x', y')] * (x'', y'') &= (xx', yx' + y') * (x'', y'') \\ &= (xx'x'', (yx' + y')x'' + y'') \\ &= (xx'x'', yx'x'' + y'x'' + y'') \\ \text{et } (x, y) * [(x', y') * (x'', y'')] &= (x, y) * (x'x'', y'x'' + y'') \\ &= (xx'x'', y(x'x'') + y'x'' + y'') \\ &= (xx'x'', yx'x'' + y'x'' + y'') \end{aligned}$$

On a bien égalité :  $[(x, y) * (x', y')] * (x'', y'') = (x, y) * [(x', y') * (x'', y'')]$ .

Ceci montre que la loi  $*$  est associative.

(iii)  $G$  contient un élément neutre pour  $*$ .

Soit  $e = (1, 0)$ . Alors  $e$  appartient à  $G$  car  $(1, 0) \in \mathbb{R}^* \times \mathbb{R}$ , et :

$$\begin{aligned} \forall (x, y) \in \mathbb{R}^* \times \mathbb{R} \quad (x, y) * e &= (x, y) * (1, 0) = (x \times 1, y \times 1 + 0) = (x, y) \\ \text{et} \quad e * (x, y) &= (1, 0) * (x, y) = (1 \times x, 0 \times x + y) = (x, y) \end{aligned}$$

Ceci montre que  $e$  est élément neutre de  $G$  pour la loi  $*$ .

(iv) Tout élément de  $G$  possède un symétrique dans  $G$ .

Soit  $(x, y) \in G$ . Alors  $x$  est non-nul donc  $\frac{1}{x}$  est défini et appartient à  $\mathbb{R}^*$ , puis  $(\frac{1}{x}, -\frac{y}{x}) \in G$ . De plus :

$$\begin{aligned} (x, y) * (\frac{1}{x}, -\frac{y}{x}) &= (x \times \frac{1}{x}, y \times \frac{1}{x} - \frac{y}{x}) = (1, 0) = e \\ \text{et} \quad (\frac{1}{x}, -\frac{y}{x}) * (x, y) &= (\frac{1}{x} \times x, -\frac{y}{x} \times x + y) = (1, 0) = e \end{aligned}$$

Ceci montre que  $(x, y)$  est symétrisable, de symétrique  $(\frac{1}{x}, -\frac{y}{x})$ , lequel est bien dans  $G$ .

Ainsi tout élément de  $G$  possède un symétrique dans  $G$ .

Les quatre points ci-dessus montrent que  $(G, *)$  est un groupe.

On calcule :

$$(1, 1) * (2, 3) = (2, 5) \quad \text{et} \quad (2, 3) * (1, 1) = (2, 4)$$

Ceci montre que la loi  $*$  n'est pas commutative, *i.e.*,  $(G, *)$  n'est pas un groupe abélien.

b. Soit  $H = \{(x, 0) \mid x \in \mathbb{R}^*\}$ . On vérifie les axiomes de définition d'un sous-groupe.

(i)  $H$  est inclus dans  $G$  : ceci est immédiat.

(ii)  $H$  est non-vide : également, par exemple  $(1, 0) \in H$ .

(iii)  $H$  est stable par  $*$  :

Soit  $(x, 0)$  et  $(x', 0)$  deux éléments de  $H$ , c'est-à-dire que  $x$  et  $x'$  sont deux réels non-nuls. Alors  $(x, 0) * (x', 0) = (xx', 0)$  : cet élément appartient bien à  $H$ .

Donc  $H$  est stable par  $*$ .

(iv)  $H$  est stable par passage au symétrique :

Soit  $(x, 0) \in H$ . La formule  $(x, y)^{-1} = (\frac{1}{x}, -\frac{y}{x})$  obtenue dans la question précédente montre que  $(x, 0)^{-1} = (\frac{1}{x}, 0)$ , cet élément appartient bien à  $H$ .

Donc  $H$  est stable par passage au symétrique.

Ces quatre points montrent que  $H$  est un sous-groupe de  $(G, *)$ .

Soit  $K = \{(1, y) \mid y \in \mathbb{R}\}$ . Alors :

(i)  $K$  est inclus dans  $G$  : c'est immédiat, car  $1 \in \mathbb{R}^*$ .

(ii)  $K$  est non-vide : également, par exemple  $(1, 0) \in K$ .

(iii)  $K$  est stable par  $*$  :

Soit  $(1, y)$  et  $(1, y')$  deux éléments de  $K$ , c'est-à-dire que  $y$  et  $y'$  sont deux réels. Alors  $(1, y) * (1, y') = (1, y + y')$  : cet élément appartient bien à  $K$ .

Donc  $K$  est stable par  $*$ .

(iv)  $K$  est stable par passage au symétrique :

Soit  $(1, y) \in K$ . La formule  $(x, y)^{-1} = \left(\frac{1}{x}, -\frac{y}{x}\right)$  montre que  $(1, y)^{-1} = (1, -y)$ , cet élément appartient bien à  $K$ .

Donc  $K$  est stable par passage au symétrique.

Ces quatre points montrent que  $K$  est un sous-groupe de  $(G, *)$ .

- c. On vérifie que  $\varphi : (\mathbb{R}^*, \times) \longrightarrow (G, *)$  et  $\psi : (\mathbb{R}, +) \longrightarrow (G, *)$  sont des morphismes.
- $$x \longmapsto (x, 0) \qquad y \longmapsto (1, y)$$

Pour le premier :

$$\forall (x, x') \in (\mathbb{R}^*)^2 \quad \varphi(x \times x') = (xx', 0) = (x, 0) * (x', 0) = \varphi(x) * \varphi(x').$$

Donc  $\varphi$  est un morphisme de  $(\mathbb{R}^*, \times)$  dans  $(G, *)$ .

Ensuite :

$$\forall (y, y') \in \mathbb{R}^2 \quad \psi(y + y') = (1, y + y') = (1, y) * (1, y') = \psi(y) * \psi(y').$$

Donc  $\psi$  est un morphisme de  $(\mathbb{R}, +)$  dans  $(G, *)$ .

- d. Par définition le noyau de  $\varphi$  est  $\ker \varphi = \{x \in \mathbb{R}^* \mid \varphi(x) = e\}$  où  $e$  est l'élément neutre de  $G$ , c'est-à-dire  $e = (1, 0)$ .

Ainsi  $\ker \varphi = \{1\}$ .

De même  $\ker \psi = \{y \in \mathbb{R} \mid \psi(y) = (1, 0)\}$  donc  $\ker \psi = \{0\}$ .

Ces deux noyaux sont réduits à l'élément neutre de  $(\mathbb{R}^*, \times)$  et  $(\mathbb{R}, +)$  respectivement, ce qui justifie que  $\varphi$  et  $\psi$  sont injectifs.

Par définition :  $\text{im } \varphi = \{\varphi(x) \mid x \in \mathbb{R}^*\}$ .

Donc  $\text{im } \varphi = \{(x, 0) \mid x \in \mathbb{R}^*\}$ , et ainsi  $\text{im } \varphi = H$ .

Ensuite  $\text{im } \psi = \{\psi(y) \mid y \in \mathbb{R}\}$ , donc  $\text{im } \psi = \{(1, y) \mid y \in \mathbb{R}\}$ , et ainsi  $\text{im } \psi = K$ .

L'image d'un morphisme de groupes est un sous-groupe du groupe d'arrivée, donc on a démontré de nouveau que  $H$  et  $K$  sont des sous-groupes de  $(G, *)$ .

Soit  $\text{Aff}(\mathbb{R})$  l'ensemble des applications affines bijectives de  $\mathbb{R}$  dans  $\mathbb{R}$ .

Alors  $(\text{Aff}(\mathbb{R}), \circ)$  est un groupe, et on peut démontrer que  $(G, *)$  est isomorphe à ce groupe via l'application  $f : G \longrightarrow \text{Aff}(\mathbb{R})$ .

$$(a, b) \longmapsto (x \mapsto ax + b)$$

**15** Soit  $(G, *)$  un groupe,  $H$  un sous-groupe de  $G$ .

On définit la relation  $\sim$  sur  $G$  par :

$$x \sim y \iff x^{-1}y \in H$$

a. Démontrer que la relation  $\sim$  est une relation d'équivalence.

b. Soit  $x \in G$  et  $\text{Cl}(x)$  sa classe d'équivalence.

Démontrer que  $\text{Cl}(x) = xH$ .

c. Démontrer pour tout  $x \in G$  l'application

$$\begin{aligned} m_x : H &\longrightarrow xH \\ h &\longmapsto xh \end{aligned}$$

est bijective.

d. On suppose que  $G$  est un groupe fini. Démontrer que le cardinal de  $H$  divise celui de  $G$ .

a. On vérifie que la relation  $\sim$  est une relation d'équivalence.

- La relation  $\sim$  est réflexive :

$$\forall x \in G \quad x \sim x$$

En effet  $x^{-1}x = e$ , où  $e$  est l'élément neutre de  $G$ , lequel appartient bien à  $H$  car  $H$  est un sous-groupe de  $G$ .

- La relation  $\sim$  est symétrique :

$$\forall (x, y) \in G^2 \quad x \sim y \implies y \sim x$$

En effet, si  $x \sim y$  alors  $x^{-1}y \in H$ . Comme  $H$  est un sous-groupe de  $H$  alors il est stable par passage à l'inverse, donc  $(x^{-1}y)^{-1} \in H$ , ce qui donne  $y^{-1}x \in H$ , et donc  $y \sim x$ .

- La relation  $\sim$  est transitive :

$$\forall (x, y, z) \in G^3 \quad (x \sim y \text{ et } y \sim z) \implies x \sim z$$

En effet, si  $x \sim y$  et  $y \sim z$  alors  $x^{-1}y \in H$  et  $y^{-1}z \in H$ . Comme  $H$  est stable par produit alors  $x^{-1}yy^{-1}z \in H$ , ce qui donne  $x^{-1}z \in H$ , et donc  $x \sim z$ .

Ainsi la relation  $\sim$  est une relation d'équivalence.

b. Par définition la classe d'équivalence de  $x$  est :

$$\text{Cl}(x) = \{y \in G \mid x \sim y\}$$

On démontre par double inclusion que  $\text{Cl}(x) = xH$  où  $xH = \{xh \mid h \in H\}$ .

Soit  $y \in \text{Cl}(x)$ . Alors  $x^{-1}y \in H$  donc il existe  $h \in H$  tel que  $x^{-1}y = h$ . Alors  $y = xh$  et donc  $y \in xH$ .

Soit  $y \in xH$ , *i.e.*,  $y = xh$  où  $h$  est un élément de  $H$ . Alors  $x^{-1}y = h$ , donc  $x^{-1}y \in H$ , puis  $x \sim y$  donc  $y \in \text{Cl}(x)$ .

On a démontré par double inclusion que la classe d'équivalence de  $x$  est  $xH$ .

c. L'application  $m_x : H \longrightarrow xH$  est bien définie.

$$h \longmapsto xh$$

On vérifie qu'elle est bijective de réciproque l'application  $n_x : xH \longrightarrow H$ .

$$y \longmapsto x^{-1}y$$

En effet cette dernière application est bien définie, et  $n_x \circ m_x = \text{Id}_H$ ,  $m_x \circ n_x = \text{Id}_{xH}$ .

d. Comme  $\sim$  est une relation d'équivalence sur  $G$  alors l'ensemble de ses classes d'équivalence est une partition de  $G$ .

Notons  $C_1, \dots, C_m$  l'ensemble des classes d'équivalences. Elles sont en nombre fini car leur union est  $G$ , qui est fini.

Comme elles sont toutes en bijection avec  $H$  d'après la question précédente alors elles sont toute même cardinal, et ce cardinal est celui de  $H$ .

Celui-ci est fini car  $H$  est inclus dans  $G$ .

Comme les classes d'équivalence forment une partition de  $G$  alors :

$$\text{Card } G = \sum_{k=1}^m \text{Card } C_k = m \times \text{Card } H$$

Ainsi le cardinal de  $H$  divise celui de  $G$ .

Il s'agit du théorème de Lagrange.

**16** Pour  $m$  et  $n$  entiers naturels non-nuls on pose :

$$\begin{aligned} f : \mathbb{U}_n &\longrightarrow \mathbb{U}_n \\ z &\longmapsto z^m. \end{aligned}$$

- a. Justifier que  $f$  est bien définie et que c'est un endomorphisme du groupe  $(\mathbb{U}_n, \times)$ .  
 b. Démontrer que le noyau de  $f$  est  $\mathbb{U}_{m \wedge n}$ .

a. Soit  $z \in \mathbb{U}_n$ . Alors  $z^m$  est défini, et  $(z^m)^n = (z^n)^m = 1^m = 1$  car  $z^n = 1$  puisque  $z \in \mathbb{U}_n$ . Ceci montre que  $z^m \in \mathbb{U}_n$ , donc  $f$  est bien définie.

De plus pour tout  $(z, z') \in \mathbb{U}_n^2$  :

$$f(zz') = (zz')^m = z^m z'^m = f(z)f(z')$$

Ceci montre que  $f$  est un endomorphisme du groupe  $(\mathbb{U}_n, \times)$ .

b. Soit  $d = m \wedge n$ . Il existe donc  $(a, b) \in \mathbb{N}^*$  tel que  $n = ad$  et  $m = bd$ .

Si  $z \in \mathbb{U}_d$  alors  $z^m = (z^d)^b = 1$  car  $z^d = 1$ , donc  $z \in \ker f$ .

Réciproquement si  $z \in \ker f$  alors  $z^m = 1$ , et  $z^n = 1$  car  $z \in \mathbb{U}_n$ .

D'après le théorème de Bézout il existe  $(u, v) \in \mathbb{Z}^2$  tel que  $mu + nv = d$ , donc  $z^d = z^{mu+nv} = (z^m)^u \times (z^n)^v = 1$  et  $z \in \mathbb{U}_d$ .

On a démontré par double inclusion que  $\ker f = \mathbb{U}_d$ .

**17** Soit  $A$  un anneau,  $a$  et  $b$  deux éléments de  $A$ .

a. Démontrer que :

$$aba = 1 \iff (a^2b = ba^2 = 1)$$

b. Démontrer que dans ce cas  $a$  et  $b$  sont inversibles et commutent.

a. Sens direct : Si  $aba = 1$  alors  $a^2ba = a$ . On multiplie à droite par  $ba$ , on obtient  $a^2bababa = aba$  donc  $a^2b = 1$ .

De même  $aba^2 = a$ , on multiplie à gauche par  $ab$ , ce qui donne  $abababa^2 = aba$ , donc  $ba^2 = 1$ .

Sens indirect : On suppose que  $a^2b = ba^2 = 1$ . Comme  $a^2b = 1$  alors  $a^2ba = a$ , on multiplie à gauche par  $ba$ , on obtient  $ba^3ba = ba^2$ , et comme  $ba^2 = 1$  alors  $aba = 1$ .

b. On suppose que  $aba = a^2b = ba^2 = 1$ .

Alors  $a^2b = 1$  et  $aba = 1$  donc  $a$  est inversible d'inverse  $ab$ .

Aussi  $ba^2 = 1$  et  $aba = 1$  donc  $a$  est inversible d'inverse  $ba$ .

Ainsi  $ab = ba$  par unicité de l'inverse.

Comme  $a^2b = ba^2 = 1$  alors  $b$  est inversible d'inverse  $a^2$ .

**18** Pour tout  $(x, y) \in \mathbb{R}$  on pose :

$$x \oplus y = x + y - 1 \quad x \otimes y = x + y - xy$$

a. Démontrer que  $(\mathbb{R}, \oplus)$  est un groupe abélien.

b. Démontrer que  $(\mathbb{R}, \oplus, \otimes)$  est un anneau commutatif.

c. Cet anneau est-il un corps ?

a. Il est clair que la loi  $\oplus$  est une loi de composition interne de  $\mathbb{R}$ .

Il faut démontrer qu'elle est associative et commutative, *i.e.*, vérifier que :

$$\forall (x, y, z) \in \mathbb{R}^3 \quad (x \oplus y) \oplus z = x \oplus (y \oplus z) \quad \text{et} \quad x \oplus y = y \oplus x$$

On démontre que 1 est élément neutre pour la loi  $\oplus$ , *i.e.*, que :

$$\forall x \in \mathbb{R} \quad x \oplus 1 = x$$

L'opposé d'un réel  $x$  pour la loi  $\oplus$  est  $2 - x$ , car :

$$\forall x \in \mathbb{R} \quad x \oplus (2 - x) = 1$$

Finalement  $(\mathbb{R}, \oplus)$  est un groupe abélien.

b. Il est clair que la loi  $\otimes$  est une loi de composition interne de  $\mathbb{R}$ .

On démontre qu'elle est associative et commutative :

$$\forall (x, y, z) \in \mathbb{R}^3 \quad (x \otimes y) \otimes z = x \otimes (y \otimes z) \quad \text{et} \quad x \otimes y = y \otimes x$$

L'élément neutre pour la loi  $\otimes$  est 0 :

$$\forall x \in \mathbb{R} \quad x \otimes 0 = x$$

De plus la loi  $\otimes$  est distributive par rapport à la loi  $\oplus$  :

$$\forall (x, y, z) \in \mathbb{R}^3 \quad x \otimes (y \oplus z) = (x \otimes y) \oplus (x \otimes z)$$

Finalement  $(\mathbb{R}, \oplus, \otimes)$  est un anneau commutatif.

c. L'élément neutre pour la loi  $\oplus$  est 1.

On démontre que l'anneau commutatif  $(\mathbb{R}, \oplus, \otimes)$  est intègre :

$$\forall (x, y) \in \mathbb{R}^2 \quad x \otimes y = 1 \implies x = 1 \quad \text{ou} \quad y = 1$$

L'élément neutre pour la loi  $\otimes$  est 0. On vérifie que tout élément de  $\mathbb{R}$  différent de 1 est inversible, d'inverse  $\frac{x}{x-1}$  :

$$\forall x \in \mathbb{R} \setminus \{1\} \quad x \otimes \frac{x}{1-x} = 0$$

Ceci montre que  $(\mathbb{R}, \oplus, \otimes)$  est un corps.

On peut ajouter que l'application :

$$\begin{aligned} f : (\mathbb{R}, \oplus, \otimes) &\longrightarrow (\mathbb{R}, +, \times) \\ x &\longmapsto 1 - x \end{aligned}$$

est un isomorphisme de corps.

**19** On note  $\mathbb{Q}[\sqrt{2}] = \{a + b\sqrt{2} \mid (a, b) \in \mathbb{Q}^2\}$ .

a. Démontrer que  $\mathbb{Q}[\sqrt{2}]$  est un sous-anneau de  $\mathbb{R}$ .

b. Démontrer que  $\mathbb{Q}[\sqrt{2}]$  est un corps.

On dit alors que  $\mathbb{Q}[\sqrt{2}]$  est un sous-corps de  $\mathbb{R}$ .

a. On vérifie que  $\mathbb{Q}[\sqrt{2}]$  est inclus dans  $\mathbb{R}$ , stable par addition, passage à l'opposé, et stable par produit.

b. Soit  $x = a + b\sqrt{2} \in \mathbb{Q}[\sqrt{2}] \setminus \{0\}$ .

Alors  $x$  est inversible dans  $\mathbb{R}$ , d'inverse  $x^{-1} = \frac{1}{a+b\sqrt{2}}$ . Démontrons que  $x^{-1} \in \mathbb{Q}[\sqrt{2}]$ .

Si  $b = 0$  alors  $a \neq 0$  car  $x \neq 0$ , donc  $x^{-1} = \frac{1}{a}$ . Comme  $a$  est rationnel non-nul alors  $\frac{1}{a}$  est rationnel non-nul, et donc  $x^{-1} \in \mathbb{Q}[\sqrt{2}]$ .

Si  $b$  est non-nul alors  $a - b\sqrt{2} \neq 0$ , sinon on aurait  $\sqrt{2} = \frac{a}{b} \in \mathbb{Q}$ , ce qui est faux car  $\sqrt{2}$  est irrationnel.

Donc en multipliant par  $a - b\sqrt{2}$  on obtient  $x^{-1} = \frac{a-b\sqrt{2}}{a^2-2b^2}$  avec  $a^2 - 2b^2 = (a + b\sqrt{2})(a - b\sqrt{2}) \neq 0$ .

Comme  $\frac{a}{a^2-2b^2}$  et  $-\frac{b}{a^2-2b^2}$  sont rationnels alors  $x^{-1} \in \mathbb{Q}[\sqrt{2}]$ .

Tout élément non-nul de  $\mathbb{Q}[\sqrt{2}]$  admet un inverse dans  $\mathbb{Q}[\sqrt{2}]$ , donc  $\mathbb{Q}[\sqrt{2}]$  est un corps.

C'est un exemple de corps strictement compris entre  $\mathbb{Q}$  et  $\mathbb{R}$ .

**20** Soit  $\mathbb{D}$  l'ensemble des nombres décimaux.

- Démontrer que  $\mathbb{D}$  est un sous-groupe de  $(\mathbb{R}, +)$ .
- Démontrer que  $(\mathbb{D}, +, \times)$  est un anneau.  
Est-il un corps ?
- Décrire le groupe de inversibles de  $\mathbb{D}$ .

- On justifie que  $\mathbb{D}$  contient 0, qu'il est stable par addition et par passage à l'opposé.
- D'après la question précédente  $(\mathbb{D}, +)$  est un groupe. De plus  $\mathbb{D}$  est stable par produit. Les lois  $+$  et  $\times$  sont induites par celles de  $\mathbb{R}$  donc  $\times$  est associative et la distributivité est vérifiée.

De plus 1 est décimal donc  $1 \in \mathbb{D}$ .

Ainsi  $(\mathbb{D}, +, \times)$  est un anneau commutatif.

Comme  $\frac{1}{3}$  n'est pas décimal alors 3 n'est pas inversible dans  $\mathbb{D}$ , donc  $\mathbb{D}$  n'est pas un corps.

- On obtient  $\mathbb{D}^* = \{2^a 5^b \mid (a, b) \in \mathbb{Z}^2\}$ .

Par propriété  $(\mathbb{D}^*, \times)$  est un groupe, et on peut ajouter que l'application

$$\begin{aligned} (\mathbb{Z}^2, +) &\longrightarrow (\mathbb{D}^*, \times) \\ (a, b) &\longmapsto 2^a 5^b \end{aligned}$$

est un isomorphisme de groupes.

**21** On note :

$$\mathbb{Z}[i] = \{a + ib \mid (a, b) \in \mathbb{Z}^2\}$$

- Démontrer que  $\mathbb{Z}[i]$  muni de l'addition et de la multiplication des complexes est un anneau.
- Justifier que l'application  $z \mapsto |z|$  est un morphisme de groupes de  $(\mathbb{C}^*, \times)$  dans  $(\mathbb{R}_+^*, \times)$ .
- Vérifier que  $N(\mathbb{Z}[i]) \subseteq \mathbb{N}$ .  
En déduire le groupe des inversibles de  $\mathbb{Z}[i]$ .

- On vérifie que  $\mathbb{Z}[i]$  est un sous-anneau de  $\mathbb{C}$ . En effet :

- $\mathbb{Z}[i]$  est inclus dans  $\mathbb{C}$ .
- $\mathbb{Z}[i]$  contient 1 car  $1 = 1 + i \times 0$  et 1 et 0 sont des entiers.
- $\mathbb{Z}[i]$  est stable par addition, car la somme de deux entiers est un entier.
- $\mathbb{Z}[i]$  est stable par passage à l'opposé, car l'opposé d'un entier est un entier.
- $\mathbb{Z}[i]$  est stable par produit. En effet, si  $a + ib$  et  $c + id$  sont deux éléments de  $\mathbb{Z}[i]$ , alors leur produit est :

$$(a + ib) \times (c + id) = (ac - bd) + i(ad + bc)$$

Comme  $a, b, c, d$  sont des entiers alors  $ac - bd$  et  $ad + bc$  sont des entiers et donc  $(a + ib) \times (c + id)$  appartient à  $\mathbb{Z}[i]$ .



Ainsi  $\mathbb{Z}[i]$  est un sous-anneau de  $\mathbb{C}$  et donc  $(\mathbb{Z}[i], +, \times)$  est un anneau.

b. Pour tout  $z \in \mathbb{C}^*$  on a  $N(z) = |z|^2 \in \mathbb{R}_+^*$ , donc  $N$  est une application de  $\mathbb{C}^*$  dans  $\mathbb{R}_+^*$ .

De plus :

$$\forall (z, z') \in (\mathbb{C}^*)^2 \quad N(zz') = |zz'|^2 = (|z||z'|)^2 = |z|^2|z'|^2 = N(z)N(z').$$

Ainsi  $N$  est un morphisme de groupes de  $(\mathbb{C}^*, \times)$  dans  $(\mathbb{R}_+^*, \times)$ .

c. Soit  $z = a + ib \in \mathbb{Z}[i]$ . Alors  $a$  et  $b$  sont des entiers. Comme  $N(z) = a^2 + b^2$  alors  $N(z)$  est un entier positif.

Ceci montre que  $N(\mathbb{Z}[i]) \subseteq \mathbb{N}$ .

Supposons que  $z$  est inversible dans  $\mathbb{Z}[i]$ . Alors son inverse  $z^{-1}$  appartient à  $\mathbb{Z}[i]$ .

Comme  $zz^{-1} = 1$  alors  $N(zz^{-1}) = N(1) = 1$ .

Comme  $N$  est un morphisme de groupes alors  $N(zz^{-1}) = N(z)N(z^{-1})$ .

Ainsi  $N(z)$  et  $N(z^{-1})$  sont des entiers naturels vérifiant  $N(z)N(z^{-1}) = 1$ . Donc  $N(z) = N(z^{-1}) = 1$ .

Ceci donne  $a^2 + b^2 = 1$  alors  $a, b$  entiers. Donc  $(a, b) = (1, 0), (-1, 0), (0, 1)$  ou  $(0, -1)$ .

Effectivement  $1, -1, i$  et  $-i$  sont inversibles dans  $\mathbb{Z}[i]$ .

Ainsi  $\mathbb{Z}[i]^* = \{\pm 1, \pm i\}$ , il s'agit du groupe multiplicatif  $\mathbb{U}_4$ .

**22** Soit  $K$  un sous-corps de  $\mathbb{C}$ , c'est-à-dire un sous-anneau de  $\mathbb{C}$  qui est un corps. Démontrer que  $\mathbb{Q} \subseteq K$ .

Comme  $K$  est un corps alors il contient 0 et 1.

De plus  $(K, +)$  est un groupe, donc il est stable par addition. On démontre par récurrence que tout entier  $n$  est dans  $K$ , et ainsi  $\mathbb{N} \subseteq K$ .

Aussi  $K$  est stable par passage à l'opposé (toujours car  $(K, +)$  est un groupe), donc tous les entiers négatifs sont aussi dans  $K$ , et ainsi  $\mathbb{Z} \subseteq K$ .

Ensuite  $K$  est un corps, donc tout élément non-nul est inversible. Or tout entier  $q$  strictement positif est dans  $K$ , donc tout rationnel  $\frac{1}{q}$  est dans  $K$ .

Enfin  $K$  est un anneau donc il est stable par multiplication donc tout rationnel  $\frac{p}{q}$  est dans  $K$ , ce qui achève de démontrer que  $\mathbb{Q} \subseteq K$ .

**23** Démontrer que si un anneau intègre est fini alors c'est un corps. On pourra considérer l'ensemble des  $x^k$  où  $k \in \mathbb{N}$ .

Soit  $A$  un anneau intègre et fini.

Démontrons que  $A$  est un corps, donc que tout élément non-nul de  $A$  est inversible.

Soit  $x$  un élément non-nul de  $A$ .

L'ensemble  $\{x^k \mid k \in \mathbb{N}\}$  est inclus dans  $A$  car  $A$  est stable par produit.

Comme  $A$  est fini alors cet ensemble est fini, donc il existe deux entiers naturels  $k$  et  $\ell$  distincts tels que  $x^k = x^\ell$ .

Quitte à les inverser on suppose que  $k < \ell$ .

Comme  $x^k = x^\ell$  alors  $x^\ell - x^k = 0$ , donc  $x^k(x^{\ell-k} - 1) = 0$ .

Or l'anneau  $A$  est intègre donc  $x^k = 0$  ou  $x^{\ell-k} - 1 = 0$ .

Dans le premier cas on obtient, toujours par intégrité,  $x = 0$ . Ceci est supposé faux.

Donc  $x^{\ell-k} = 1$  avec  $\ell - k \geq 1$ , ce qui montre que  $x$  est inversible d'inverse  $x^{\ell-k-1}$ .

Ainsi tout élément non-nul de  $A$  est inversible, donc  $A$  est un corps.

**24** Soit  $K$  un corps et  $A$  un anneau.

Démontrer que tout morphisme d'anneaux  $f : K \rightarrow A$  est injectif.

Par propriété il faut démontrer que  $\ker f = \{0_K\}$ .

D'une part  $\{0_K\} \subseteq \ker f$  car  $f(0_K) = 0_A$ , car  $f : K \rightarrow A$  est une morphisme de groupes de  $(K, +)$  car  $(A, +)$ , puisque  $f$  est un morphisme d'anneaux.

Démontrons que  $\ker f \subseteq \{0_K\}$ .

Soit  $x \in \ker f$ . Alors  $f(x) = 0_A$ . Si  $x$  est inversible, alors  $f(xx^{-1}) = f(1_K) = 1_A$  car  $f$  est un morphisme d'anneaux. Or  $f(xx^{-1}) = f(x)f(x^{-1}) = 0_A$  car  $f(x) = 0_A$ , et donc on obtient la contradiction  $0_A = 1_A$ .

Ainsi  $x$  ne peut être inversible, donc  $x = 0_K$  puisque  $K$  est un corps.

On a démontré que  $\ker f \subseteq \{0_K\}$ , donc  $\ker f = \{0_K\}$  par double inclusion, et par propriété  $f$  est injectif.

**25** On définit l'ensemble :

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

- Démontrer que  $C$  est un sous-anneau de  $(\mathcal{M}_2(\mathbb{R}), +, \times)$ .
- Démontrer que  $C$  est un corps
- Démontrer que le corps  $C$  est isomorphe à  $\mathbb{C}$ , c'est-à-dire qu'il existe un isomorphisme d'anneaux de  $C$  dans  $\mathbb{C}$ .

a. On vérifie que  $C$  est inclus dans  $\mathcal{M}_2(\mathbb{R})$ , non-vidé, stable par addition et passage à l'opposé. Donc  $(C, +)$  est un sous-groupe de  $(\mathcal{M}_2(\mathbb{R}), +)$ .

Ensuite on vérifie que  $C$  contient  $I_2$  et est stable par  $\times$ .

Donc  $C$  est un sous-anneau de  $(\mathcal{M}_2(\mathbb{R}), +, \times)$ .

b. Tout élément non-nul est inversible dans  $\mathcal{M}_2(\mathbb{R})$  car son déterminant  $a^2 + b^2$  est non-nul.

On vérifie que son inverse appartient à  $C$ , donc  $C$  est stable par passage à l'inverse, et ainsi  $C$  est un corps.

c. Posons par exemple  $f : \mathbb{C} \rightarrow C$

$$a + ib \mapsto \begin{pmatrix} a & b \\ -b & a \end{pmatrix}.$$

On vérifie que  $f(1) = I_2$ , et que  $f$  est compatible avec l'addition et la multiplication. Donc  $f$  est un morphisme d'anneaux.

Il est clair que  $f$  est bijectif, donc  $f$  est un isomorphisme d'anneaux (donc de corps).