Corrigé partiel du T. D. B6
Structures algébriques

③ Soit $(G, *)$ un groupe à quatre éléments, d'élément neutre e.

a. On suppose qu'il existe un élément a de G tel que $a^2 \neq e$. On note $b = a^2$. Justifier que $a \neq b$ et construire la table de composition de G.

b. 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 composition.

a. Si $a = b$ alors $a^2 = a$, ce qui donne $a = e$ en simplifiant par a. Or $a^2 \neq e$ donc $a \neq e$, et cette contradiction montre que $a \neq b$.

On note c le quatrième élément de G. Comme chaque colonne et chaque ligne de la table de composition de G contient une seule fois chaque élément, on obtient :

$*$	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

$\times$	1	i	-1	$-i$
1	1	i	-1	$-i$
i	i	-1	$-i$	1
-1	-1	$-i$	1	i
$-i$	$-i$	1	i	-1

b. On suppose que $a^2 = b^2 = c^2 = e$, donc la table de composition de G est :

$*$	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 :

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

muni de la multiplication matricielle.

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

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

muni de la composition des fonctions.

2 Soit E un ensemble.

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

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

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

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

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

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

(SG_1) $Z(M) \subseteq \mathrm{GL}_n(\mathbb{K})$: c'est évident d'après la définition de $Z(M)$.

(SG_2) $Z(M)$ est non-vide : en effet il contient la matrice identité I_n car celle-ci commute avec M, *i.e.*, $I_n M = M I_n$.

(SG_3) $Z(M)$ 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.

(SG_4) $Z(M)$ est stable par passage à l'inverse.

Soit $A \in Z(M)$. Alors $A \in \mathrm{GL}_n(\mathbb{K})$ 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 $(\mathrm{GL}_n(\mathbb{K}), \times)$.

4 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.

5 Soit $(G, *)$ un groupe d'élément neutre e.
Soit x et y deux éléments de G tels que :

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

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 $y^4 = e$.

6 Soit $(G, *)$ un groupe et a un de ses éléments.

a. Démontrer que les applications $g \mapsto ag$ et $g \mapsto ga$ sont des bijections de G.
Sont-elles des endomorphismes ?
b. Démontrer que l'application $g \mapsto aga^{-1}$ est un automorphisme de G.
c. 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 $\varphi_a : \begin{array}{ccc} G & \longrightarrow & G \\ g & \longmapsto & ag. \end{array}$
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 :

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

Ainsi $\varphi_{a^{-1}} \circ \varphi_a = \mathrm{Id}_G$.
De même $\varphi_a \circ \varphi_{a^{-1}} = \mathrm{Id}_G$, donc φ_a est bijective, et de plus sa réciproque est $\varphi_{a^{-1}}$.
On démontre de même que $\psi_a : \begin{array}{ccc} G & \longrightarrow & G \\ g & \longmapsto & ga \end{array}$ est bijective, de réciproque $\psi_{a^{-1}}$.

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

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

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

On peut démontrer directement que σ_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 σ_a est une bijection de G.

On calcule :

$$\forall (x,y) \in G^2 \qquad \sigma_a(g)\sigma_a(h) = \left(aga^{-1}\right)\left(aha^{-1}\right)$$
$$= ag(a^{-1}a)ha^{-1} = ageha^{-1} = agha^{-1} = \sigma_a(gh)$$

Ceci montre que σ_a est un morphisme de groupes.

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

c. Notons $\tau : G \longrightarrow G$
$g \longmapsto g^{-1}$.

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 τ est bien définie.

Supposons que τ est un morphisme de groupes. Ceci signifie :

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

Par équivalences :

$$\tau(gh) = \tau(g)\tau(h) \iff (gh)^{-1} = g^{-1}h^{-1}$$
$$\iff gh = \left(g^{-1}h^{-1}\right)^{-1} = hg$$

Ainsi τ est un morphisme de groupes si et seulement si G est commutatif.

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

Ainsi τ est un automophisme de groupe si et seulement si G est commutatif.

7 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 τ et σ les applications :

$$\tau : \begin{array}{l} a \mapsto b \\ b \mapsto a \\ c \mapsto c \end{array} \qquad \text{et} \qquad \sigma : \begin{array}{l} a \mapsto b \\ b \mapsto c \\ c \mapsto a \end{array}$$

Démontrer que :

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

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.

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

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 :

$$\sigma \circ \sigma : \begin{array}{l} a \mapsto c \\ b \mapsto a \\ c \mapsto b \end{array} \qquad \tau \circ \sigma : \begin{array}{l} a \mapsto a \\ b \mapsto c \\ c \mapsto b \end{array} \qquad \tau \circ \sigma \circ \sigma : \begin{array}{l} a \mapsto c \\ b \mapsto b \\ c \mapsto a \end{array}$$

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 $\circ$:

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

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	σ	σ^2	τ	$\tau\sigma$	$\tau\sigma^2$
e	e	σ	σ^2	τ	$\tau\sigma$	$\tau\sigma^2$
σ	σ	σ^2	e	$\tau\sigma^2$	τ	$\tau\sigma$
σ^2	σ^2	e	σ	$\tau\sigma$	$\tau\sigma^2$	τ
τ	τ	$\tau\sigma$	$\tau\sigma^2$	e	σ	σ^2
$\tau\sigma$	$\tau\sigma$	$\tau\sigma^2$	τ	σ^2	e	σ
$\tau\sigma^2$	$\tau\sigma^2$	τ	$\tau\sigma$	σ	σ^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.

8 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 :

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

Alors l'image de f est $\operatorname{im} f = m\mathbb{Z}$, 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 $0 \leqslant r < m$.

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 $m \in \mathbb{Z}$.

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

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

a. Justifier que f est un endomorphisme du groupe $(\mathscr{M}_n(\mathbb{K}), +)$.

b. Déterminer le noyau et l'image de f.

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

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

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

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

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

Par équivalence :

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

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

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

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

$${}^t(f(M)) = {}^t\Big(\tfrac{1}{2}(M + {}^tM)\Big) = \tfrac{1}{2}({}^tM + M) = f(M).$$

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

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

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

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

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

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

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 :

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

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.

(G_1) 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.

(G_2) La loi $*$ est associative.
Soit (x,y), (x',y'), et (x'',y'') trois éléments de G. Alors :

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

On a bien égalité : $[(x,y) * (x',y')] * (x'',y'') = (x,y) * [(x',y') * (x'',y'')]$.
Ceci montre que la loi $*$ est associative.

(G_3) 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 :

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

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

(G_4) 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 $\left(\frac{1}{x}, -\frac{y}{x}\right) \in G$. De plus :

$$(x,y) * \left(\tfrac{1}{x}, -\tfrac{y}{x}\right) = \left(x \times \tfrac{1}{x}, y \times \tfrac{1}{x} - \tfrac{y}{x}\right) = (1,0) = e$$
$$\text{et} \quad \left(\tfrac{1}{x}, -\tfrac{y}{x}\right) * (x,y) = \left(\tfrac{1}{x} \times x, -\tfrac{y}{x} \times x + y\right) = (1,0) = e$$

Ceci montre que (x,y) est symétrisable, de symétrique $\left(\frac{1}{x}, -\frac{y}{x}\right)$, 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 :

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

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.

(SG_1) H est inclus dans G : ceci est immédiat.

(SG_2) H est non-vide : également, par exemple $(1,0) \in H$.

(SG_3) 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 $*$.

(SG_4) H est stable par passage au symétrique :

Soit $(x,0) \in H$. La formule $(x,y)^{-1} = \left(\frac{1}{x}, -\frac{y}{x}\right)$ obtenue dans la question précédente montre que $(x,0)^{-1} = \left(\frac{1}{x}, 0\right)$, 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 :

(SG_1) K est inclus dans G : c'est immédiat, car $1 \in \mathbb{R}^*$.

(SG_2) K est non-vide : également, par exemple $(1,0) \in K$.

(SG_3) 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 $*$.

(SG_4) 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.
$x \longmapsto (x, 0)$ $y \longmapsto (1, y)$

Pour le premier :

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

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

Ensuite :

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

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

d. Par définition le noyau de φ 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 φ et ψ sont injectifs.

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

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

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

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

Alors $(\mathrm{Aff}(\mathbb{R}), \circ)$ est un groupe, et on peut démontrer que $(G, *)$ est isomorphe à ce groupe via l'application $f : \begin{array}{ccc} G & \longrightarrow & \mathrm{Aff}(\mathbb{R}) \\ (a, b) & \longmapsto & (x \mapsto ax + b) \end{array}$.

11 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 $\mathrm{Cl}(x)$ sa classe d'équivalence.
Démontrer que $\mathrm{Cl}(x) = xH$.

c. Démontrer pour tout $x \in G$ l'application $\begin{array}{ccc} m_x : H & \longrightarrow & xH \\ h & \longmapsto & xh \end{array}$ 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 :
$$\forall x \in G \qquad x \sim x$$
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 :
$$\forall (x, y) \in G^2 \qquad x \sim y \implies y \sim x$$
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 :
$$\forall (x, y, z) \in G^3 \qquad (x \sim y \quad \text{et} \quad y \sim z) \implies x \sim z$$
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 :
$$\mathrm{Cl}(x) = \{y \in G \mid x \sim y\}$$
On démontre par double inclusion que $\mathrm{Cl}(x) = xH$ où $xH = \{xh \mid h \in H\}$.

Soit $y \in \mathrm{Cl}(x)$. 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 $y \in \mathrm{Cl}(x)$.

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

c. L'application $\begin{array}{ccc} m_x : H & \longrightarrow & xH \\ h & \longmapsto & xh \end{array}$ est bien définie.

On vérifie qu'elle est bijective de réciproque l'application $\begin{array}{ccc} n_x : xH & \longrightarrow & H \\ y & \longmapsto & x^{-1}y \end{array}$.

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

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 :

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

Ainsi le cardinal de H divise celui de G.

Il s'agit du théorème de Lagrange.

12 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 $\ker f = \mathbb{U}_d$.

13 Soit A un anneau, a et b deux éléments de A.

a. Démontrer que :
$$aba = 1 \iff \Big(a^2b = ba^2 = 1\Big)$$

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 $a^2baba = aba$ donc $a^2b = 1$.

De même $aba^2 = a$, on multiplie à gauche par ab, ce qui donne $ababa^2 = aba$, 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.

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

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

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 :

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

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

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

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

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

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 :

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

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

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

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

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

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 :

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

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

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

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.

15 On note $\mathbb{Q}[\sqrt{2}] = \left\{ a + b\sqrt{2} \;\middle|\; (a,b) \in \mathbb{Q}^2 \right\}$.

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 $\mathbb{R}$.

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

a. Démontrer que $\mathbb{D}$ est un sous-groupe de $(\mathbb{R}, +)$.
b. Démontrer que $(\mathbb{D}, +, \times)$ est un anneau. Est-il un corps ?
c. Décrire le groupe de inversibles de $\mathbb{D}$.
d. Donner un isomorphisme $f : (\mathbb{Z}^2, +) \to (\mathscr{D}^*, \times)$.

a. On justifie que $\mathbb{D}$ contient 0, qu'il est stable par addition et par passage à l'opposé.

b. 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.

c. On obtient $\mathbb{D}^* = \left\{ 2^a 5^b \;\middle|\; (a,b) \in \mathbb{Z}^2 \right\}$.

d. Par propriété $(\mathbb{D}^*, \times)$ est un groupe. On définit l'application

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

Cette application est bien définie et surjective d'après la question précédente.

On démontre que f est un morphisme de groupes :

$$\begin{aligned} \forall ((a,b),(c,d)) \in \left(\mathbb{Z}^2\right)^2 \qquad f((a,b)+(c,d)) &= f((a+c, b+d)) \\ &= 2^{a+c}5^{b+d} = 2^a 5^b \times 2^c 5^d \\ &= f(a,b) \times f(c,d) \end{aligned}$$

Ainsi f est un morphisme de groupes.

Pour démontrer qu'elle est injective on détermine son noyau.

Comme l'élément neutre du groupe $(\mathbb{D}^*, \times)$ est 1, par définition :

$$\ker f = \left\{ (a,b) \in \mathbb{Z}^2 \;\middle|\; f(a,b) = 1 \right\}.$$

Pour tout $(a,b) \in \mathbb{Z}^2$, l'égalité $2^a 5^b = 1$ a lieu si et seulement si $a = b = 0$.

Ainsi $\ker f = \{(0,0)\}$, il s'agit de l'élément neutre du groupe $(\mathbb{Z}^2, +)$, et donc par théorème f est injective.

Ainsi f est bijective, et comme c'est un morphisme de groupes alors f est un isomorphisme de groupes.

17 On note :

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

a. Démontrer que $\mathbb{Z}[i]$ muni de l'addition et de la multiplication des complexes est un anneau.

b. Justifier que l'application $N : z \mapsto |z|$ est un morphisme de groupes de $(\mathbb{C}^*, \times)$ dans $\left(\mathbb{R}_+^*, \times\right)$.

c. Vérifier que $N(\mathbb{Z}[i]) \subseteq \mathbb{N}$.

En déduire le groupe des inversibles de $\mathbb{Z}[i]$.

a. 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 :

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

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

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 $N(z)$ est $N(z^{-1})$ 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 $\mathbb{U}_4$.

18 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 $\mathbb{Q} \subseteq K$.

19 Démontrer que si un anneau intègre est fini alors c'est un corps.

On pourra considérer, pour un élément a, l'ensemble des a^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 a un élément non-nul de A.

L'ensemble $\left\{ a^k \;\middle|\; k \in \mathbb{N} \right\}$ 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 ℓ distincts tels que $a^k = a^\ell$.

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

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

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

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

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

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

20 Soit K un corps et A un anneau.

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

Soit $f : K \to A$ un morphisme d'anneaux.

Par théorème f est injectif si et seulement si $\ker f = \{0_K\}$.

D'une part $\{0_K\} \subseteq \ker f$ car $f(0_K) = 0_A$, car $f : K \to A$ 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 théorème f est injectif.

21 On définit l'ensemble :

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

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

b. Démontrer que C est un corps

c. 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-vide, 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 $f : \begin{array}{ccc} \mathbb{C} & \longrightarrow & C \\ a + ib & \longmapsto & \left(\begin{smallmatrix} a & b \\ -b & a \end{smallmatrix}\right). \end{array}$

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).