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 $\varnothing$, mais aucun élément non trivial n'admet d'inverse (dès que E est non-vide).

5 Soit G un groupe d'élément neutre e.
On suppose que pour tout $x \in G$: $\quad x^2 = e$
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 :

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

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 $y^4 = e$.

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

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 on a $\varphi_a(e) \neq e$.

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'un automorphisme de groupes.

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

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 :

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

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 $\tau : \begin{array}{ccc} G & \longrightarrow & G \\ g & \longmapsto & g^{-1}. \end{array}$

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 :

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

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.

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 τ et σ les applications :

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

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 la notation $\circ$:

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

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.

14 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 $m\in\mathbb{Z}$.

15 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 $(z,z')\in\mathbb{U}_n^2$:

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

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

16 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.

17 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.

19 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 $\mathbb{D}$.

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

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

c. Déterminer 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 $\mathbb{Z}[i]$ est un anneau.

b. Comme :

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

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

c. On sait que tout complexe non-nul est inversible, car $\mathbb{C}$ est un corps.

Un élément non-nul de $\mathbb{Z}[i]$ est inversible dans $\mathbb{Z}[i]$ si et seulement si son inverse appartient à $\mathbb{Z}[i]$.

Soit $z = a+ib$ un élément non-nul de $\mathbb{Z}[i]$. Alors son module est $|z| = \sqrt{a^2 + b^2}$. Comme z est non-nul alors a ou b est non-nul, donc a^2 ou b^2 est supérieur ou égal à 1, et donc le module de z est supérieur ou égal à 1.

Si $|z| > 1$ alors $|z^{-1}| = \frac{1}{|z|} < 1$, donc z^{-1} n'appartient pas à $\mathbb{Z}[i]$.

Si $|z| = 1$ alors $a^2 + b^2 = 1$, et comme a et b sont entiers alors on a juste quatre possibilités : $(a, b) = (1, 0)$, $(-1, 0)$, $(0, 1)$ 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 $\mathbb{U}_4$.

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

22 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 $\left\{ x^k \;\middle|\; k \in \mathbb{N} \right\}$ 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 $x^k = x^\ell$.

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 $\ell - k \geqslant 1$, 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.

23 Soit K un corps et A un anneau.
Démontrer que tout morphisme d'anneaux $f : K \to A$ 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 $f : K \to A$ 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 propriété f est injectif.

24 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 $f : \mathbb{C} \longrightarrow C$
$a + ib \longmapsto \left(\begin{smallmatrix} a & b \\ -b & a \end{smallmatrix}\right)$.
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 isomorpisme d'anneaux (donc de corps).