STRUCTURES ALGÉBRIQUES

A. Lois de composition interne

♦ ***Exercice 1.*** [○]
Étudier les propriétés de la loi $*$ définie sur $\underline{\mathbb{R}} = \mathbb{R} \cup \{-\infty\}$ par

$$\forall x, y \in \underline{\mathbb{R}}, \qquad x * y = \max(x, y).$$

La loi $*$ est clairement interne sur $\underline{\mathbb{R}}$.
Pour tous $x, y, z \in \underline{\mathbb{R}}$, on a

$$(x * y) * z = \max(\max(x, y), z) = \max(x, y, z) = \max(x, \max(y, z)) = x * (y * z),$$

donc $*$ est associative.
Pour tous $x, y \in \underline{\mathbb{R}}$, on a

$$x * y = \max(x, y) = \max(y, x) = y * x,$$

donc $*$ est commutative.
Posons $e = -\infty$. Pour tout $x \in \underline{\mathbb{R}}$, on a

$$e * x = \max(-\infty, x) = x,$$

donc $-\infty$ est l'élément neutre de $*$ dans $\underline{\mathbb{R}}$.
On en conclut que

$$\boxed{(\underline{\mathbb{R}}, *) \text{ est un monoïde commutatif.}}$$

Remarque : Ce monoïde est à la base d'une branche de l'algèbre appelée « algèbre tropicale ».

♦ ***Exercice 2.*** [⋆]
Soit $(E, *)$ un magma associatif. Un élément a de E est dit *idempotent* lorsque $a^2 = a$.

1. On suppose que tout élément de E est simplifiable. Démontrer que E possède au plus un idempotent.
2. Démontrer que si E est fini, alors E possède au moins un idempotent. *Indication : Prendre un élément quelconque de E et étudier ses puissances.*

1. Supposons l'existence de $a_1, a_2 \in E$ tels que ${a_1}^2 = a_1$ et ${a_2}^2 = a_2$. En effectuant un « produit croisé » de ces égalités (le membre de gauche de la première égalité est multiplié par le membre de droite de la seconde et vice-versa), on obtient

$${a_1}^2 * a_2 = a_1 * {a_2}^2.$$

En simplifiant par a_1 à gauche et par a_2 à droite, il vient alors

$$a_1 = a_2.$$

Donc

$$\boxed{E \text{ possède au plus un idempotent.}}$$

2. Soit $a \in E$. Les éléments $a, a^2, a^3, \ldots, a^n, \ldots$ sont en nombre fini (puisque E est fini), ce qui démontre qu'il existe $p, k \in \mathbb{N}^*$ tels que $a^{p+k} = a^p$. Mézalors, on a $a^{p+\ell k} = a^p$ pour tout $\ell \in \mathbb{N}$. On prend alors assez grand pour que $\ell k > p$ et on écrit que

$$(a^{\ell k})^2 = a^{2\ell k} = a^{p+\ell k} a^{\ell k - p} = a^p a^{\ell k - p} = a^{\ell k},$$

ce qui prouve que $a^{\ell k}$ est un idempotent. Donc

$$\boxed{E \text{ possède au moins un idempotent.}}$$

♦ ***Exercice 3.*** [⋆]
Soit $(E,*)$ un magma associatif non vide tel que $\forall a,b\in E,\ \exists x\in E,\ b=a*x*a$. Démontrer que $(E,*)$ est un monoïde.

On nous demande de démontrer que E contient un élément neutre pour $*$.

Soit $a\in E$. Par hypothèse, il existe x tel que $a=a*x*a$. S'il nous était autorisé de simplifier par a et si nous disposions déjà d'un élément neutre, nous en déduirions tout de suite que $a*x=x*a=e$. Nous n'avons pas le droit de procéder ainsi mais tout de même $a*x$ et $x*a$ sont de bons candidats pour être le neutre recherché…

Posons $e_g=a*x$ et $e_d=x*a$.

Soit $b\in E$. L'hypothèse nous dit qu'il existe $y\in E$ tel que $b=a*y*a$. Alors

$$e_g*b=a*x*(a*y*a)=(a*x*a)*y*a=a*y*a=b$$

et

$$b*e_d=(a*x*a)*x*a=a*x*(a*x*a)=a*x*a=b,$$

ce qui démontre que e_g est neutre à gauche et e_d est neutre à droite.

Il ne reste plus qu'à démontrer que $e_g=e_d$. Pour cela, on écrit que

$$e_g*e_d=\begin{cases}e_g & \text{car } e_d \text{ est neutre à droite}\\ e_d & \text{car } e_g \text{ est neutre à droite}\end{cases}$$

donc

$$e_g=e_d,$$

ce qui démontre que E contient un élément neutre pour $*$.

En conclusion,

$\boxed{(E,*) \text{ est un monoïde.}}$

B. Groupes

♦ ***Exercice 4.*** [○]
Dresser les tables de tous les groupes de cardinal 1, 2, 3 et 4. Lorsque plusieurs tables sont isomorphes (c'est-à-dire identiques au nom et à l'ordre près des éléments), on ne gardera qu'une seule table.

Avec quel jeu classique cet exercice a-t-il un lien ?

Les propriétés définissant les groupes imposent que dans chaque ligne et dans chaque colonne, on trouve une fois et une seule chaque élément du groupe. On a donc l'impression de jouer au sudoku !

Pour les groupes de cardinal 1, il n'y a guère le choix :

↱	e
e	e

Pour les groupes de cardinal 2, on trouve également une seule table possible

↱	a	e
a	e	a
e	a	e

Pour les groupes de cardinal 3, on trouve également une seule table possible

↱	a	b	e
a	b	e	a
b	e	a	b
e	a	b	e

Pour les groupes de cardinal 4, on trouve 4 tables possibles mais trois d'entre-elles sont isomorphes. Il y a donc (à isomorphisme près) deux groupes de cardinal 4.

$\mathbin{↱}$	a	b	c	e
a	e	c	b	a
b	c	e	a	b
c	b	a	e	c
e	a	b	c	e

groupe de Klein

et

$\mathbin{↱}$	a	b	c	e
a	b	c	e	a
b	c	e	a	b
c	e	a	b	c
e	a	b	c	e

$\mathbin{↱}$	a	b	c	e
a	e	c	b	a
b	c	a	e	b
c	b	e	a	c
e	a	b	c	e

$\mathbin{↱}$	a	b	c	e
a	c	e	b	a
b	e	c	a	b
c	b	a	e	c
e	a	b	c	e

isomorphes

♦ ***Exercice 5.*** [○]
Sur $]-1;1[$, on considère la loi $\oplus$ définie par

$$\forall a,b\in\,]-1;1[\,,\qquad a\oplus b=\frac{a+b}{1+ab}\cdot$$

1. Démontrer que $(]-1;1[\,,\oplus)$ est un groupe abélien.
2. Justifier que $(]-1;1[\,,\oplus)$ et $(\mathbb{R},+)$ sont isomorphes. *Indication : Connaissez-vous une bijection usuelle de $\mathbb{R}$ vers $]-1;1[$?*

1. Pour tous $a,b\in\,]-1;1[$, on a

$$\begin{aligned}
&-1<\frac{a+b}{1+ab}<1\\
\iff\quad &-(1+ab)<a+b<1+ab \qquad \text{car } 1+ab>0\\
\iff\quad &1+ab+a+b>0 \quad\text{et}\quad 1+ab-a-b>0\\
\iff\quad &(1+a)(1+b)>0 \quad\text{et}\quad (1-a)(1-b)>0.
\end{aligned}$$

Comme les deux inégalités finales sont clairement vraies (un produit de nombres strictement positifs étant évidemment strictement positif), on en déduit que $\oplus$ est interne sur $]-1;1[$.

Pour tous $a,b\in\,]-1;1[$, on a

$$a\oplus b=\frac{a+b}{1+ab}=\frac{b+a}{1+ba}=b\oplus a,$$

donc $\oplus$ est commutative. Dans la suite, il est donc inutile de démontrer les propriétés « dans les deux sens ».

Pour tout $a\in\,]-1;1[$, on a

$$a\oplus 0=\frac{a+0}{1+a.0}=a,$$

donc 0 est élément neutre dans $]-1;1[$ pour $\oplus$.

Pour tous $a,b,c\in\,]-1;1[$, on a

$$(a\oplus b)\oplus c=\frac{a+b}{1+ab}\oplus c=\frac{\dfrac{a+b}{1+ab}+c}{1+\dfrac{a+b}{1+ab}c}=\frac{a+b+c+abc}{1+ab+bc+ca}=\frac{a+\dfrac{b+c}{1+bc}}{1+a\dfrac{b+c}{1+bc}}=a\oplus(b\oplus c),$$

donc $\oplus$ est associative.

Pour tout $a \in]-1;1[$, on a $-a \in]-1;1[$ et

$$a \oplus (-a) = \frac{a+(-a)}{1+a(-a)} = 0,$$

donc a est symétrisable pour $\oplus$ de symétrique $-a$.

On en conclut que

$$\boxed{(]-1;1[\,,\oplus) \text{ est un groupe abélien.}}$$

2. Considérons

$$\mathrm{th}\left\{\begin{array}{ccc}(\mathbb{R},+) & \longrightarrow & (]-1;1[\,,\oplus)\\ x & \longmapsto & \mathrm{th}(x)\end{array}\right.$$

Pour tout $x, y \in \mathbb{R}$, on a

$$\mathrm{th}(x+y) = \frac{\mathrm{th}(x)+\mathrm{th}(y)}{1+\mathrm{th}(x)\,\mathrm{th}(y)} = \mathrm{th}(x) \oplus \mathrm{th}(y),$$

donc th est un morphisme de groupes de $(\mathbb{R},+)$ vers $(]-1;1[\,,\oplus)$. Comme th est en outre une bijection entre $\mathbb{R}$ et $]-1;1[$ (c'est le théorème de la bijection qui le dit puisque th une fonction continue et strictement croissante de $\mathbb{R}$ vers $]-1;1[$), on en déduit que th est un isomorphisme entre $(\mathbb{R},+)$ et $(]-1;1[\,,\oplus)$. Par conséquent,

$$\boxed{(]-1;1[\,,\oplus) \text{ et } (\mathbb{R},+) \text{ sont isomorphes.}}$$

♦ ***Exercice 6.*** [○]
Soit $(G,*)$ un groupe d'élément neutre e. On suppose que, pour tout $g \in G$, on a $g^2 = e$. Démontrer que G est abélien.

La condition $\forall g \in G,\ g^2 = e$ implique que $\forall g \in G,\ g = g^{-1}$.
Pour tous $x, y \in G$, on a

$$x * y = (x * y)^{-1} = y^{-1} * x^{-1} = y * x.$$

Donc

$$\boxed{G \text{ est abélien.}}$$

♦ ***Exercice 7.*** [○]
Soient $(G,*)$ un groupe et $g_1, g_2 \in G$. On suppose que $g_1 g_2$ commute avec tout autre élément de G. Démontrer que g_1 et g_2 commutent.

On a

$$\begin{array}{rcll} g_1 g_2 & = & (g_2 {g_2}^{-1})(g_1 g_2) & \text{Binet !}\\ & = & (g_2)({g_2}^{-1})(g_1 g_2) & \\ & = & (g_2)(g_1 g_2)({g_2}^{-1}) & g_1 g_2 \text{ commute avec } {g_2}^{-1}\\ & = & (g_2 g_1)(g_2 {g_2}^{-1}) & \\ & = & g_2 g_1, & \end{array}$$

donc

$$\boxed{g_1 \text{ et } g_2 \text{ commutent.}}$$

♦ ***Exercice 8.*** [⋆]
Soit $(G,.)$ un groupe. Soient $a,b \in G$ vérifiant $aba = b^3$ et $b^5 = e$. Démontrer que a et b commutent.

En mutipliant l'égalité $aba = b^3$ par b à gauche, on obtient

$$baba = b^4. \qquad (*)$$

En multipliant cette égalité par bab à droite et en tenant compte du fait que $b^5 = e$, on obtient

$$bababab = ab. \qquad (**)$$

En remplaçant le $baba$ qui est au milieu du membre de gauche de $(**)$ par l'expression donnée par $(*)$, on a

$$ba(b^4)b = ab,$$

ce qui donne, compte tenu du fait que $b^5 = e$,

$$ba = ab.$$

Donc

$\boxed{a \text{ et } b \text{ commutent.}}$

♦ ***Exercice 9.*** [⋆] (Caractérisation régulière des groupes finis)
Soit $(E,*)$ un monoïde fini dans lequel tout élément est simplifiable. Soient $a \in E$ et

$$\gamma \left\{ \begin{array}{ccc} E & \longrightarrow & E \\ x & \longmapsto & a*x \end{array} \right.$$

1. Démontrer que l'application γ est injective puis qu'elle est surjective.
   En déduire que $(E,*)$ est un groupe.
2. Ce résultat subsiste-t-il si E est infini ?

1. Vérifions que γ est injective. Soient $x_1, x_2 \in E$ tels que $\gamma(x_1) = \gamma(x_2)$, c'est-à-dire $a*x_1 = a*x_2$, ce qui donne $x_1 = x_2$ en simplifiant a. Donc

   $\boxed{\gamma \text{ est injective.}}$

   Comme E est fini, γ est donc une application injective entre deux ensembles finis de même cardinal. Cela permet d'affirmer, selon le cours, que

   $\boxed{\gamma \text{ est surjective.}}$

   Notons e l'antécédent de a par γ de sorte que $a*e = a$.
   Soit $x \in E$.
   Alors $a*e*x = a*x$ et comme a est simplifiable, on a $e*x = x$ donc e est neutre à gauche.
   On a aussi $x*e*x = x*x$, d'où, puisque x est simplifiable, $x*e = x$, donc e est aussi neutre à droite.
   Donc e est neutre.

   On note b l'antécédent de e par γ de sorte que $a*b = e$, ce qui signifie que b est un symétrique à droite de a.
   On a aussi $b*a*b = b$, et comme b est simplifiable, $b*a = e$, donc b est aussi un symétrique à gauche de a.
   Donc b est le symétrique de a.

   Tout ceci implique que

   $\boxed{(E,*) \text{ est un groupe.}}$

2. Lorsque E est infini, $(\mathbb{N},+)$ est un contre-exemple. Donc

   $\boxed{\text{le résultat est faux si } E \text{ est infini.}}$

♦ ***Exercice 10.*** [○]

On considère les applications suivantes de $\mathbb{R}\setminus\{0;1\}$ dans lui même :

$$a : x \longmapsto x\,; \qquad b : x \longmapsto \frac{1}{1-x}\,; \qquad c : x \longmapsto \frac{x-1}{x}\,;$$

$$d : x \longmapsto \frac{1}{x}\,; \qquad e : x \longmapsto 1-x\,; \qquad f : x \longmapsto \frac{x}{x-1}\cdot$$

Démontrer que $G = \{a, b, c, d, e, f\}$ est un groupe pour la loi $\circ$ dont on dressera la table.

Il est clair que chacune des applications est une bijection de $\mathbb{R}\setminus\{0,1\}$ sur lui-même.

On forme la table de G :

$\circ \curvearrowright$	a	b	c	d	e	f
a	a	b	c	d	e	f
b	b	c	a	f	d	e
c	c	a	b	e	f	d
d	d	e	f	a	b	c
e	e	f	d	c	a	b
f	f	d	e	b	c	a

On constate que G est stable pour la loi $\circ$.

Tout élément de G a un symétrique dans G. Plus précisément, les applications a, d, e, f sont involutives (i.e. sont leur propre inverse), alors que les applications b et c sont inverses l'une de l'autre.

Donc

G est donc un sous-groupe du groupe des bijections de $\mathbb{R}\setminus\{0,1\}$ dans lui-même.

♦ ***Exercice 11.*** [○]

Démontrer que $\left(\bigcup_{n=1}^{+\infty} \mathbb{U}_n, \times\right)$ est un groupe abélien.

Démontrons que $G = \bigcup_{n=1}^{+\infty} \mathbb{U}_n$ est un sous-groupe de $(\mathbb{U}, \times)$.

On sait que 1 appartient à tous les $\mathbb{U}_n$ donc $1 \in G$.

Soit $u, v \in G$. Il existe alors $n, m \in \mathbb{N}^*$ tels que $u \in \mathbb{U}_n$ et $v \in \mathbb{U}_m$. Mézalors, $(uv)^{nm} = (u^n)^m (u^m)^n = 1^m 1^n = 1$ donc $uv \in \mathbb{U}_{nm}$ et par conséquent $uv \in G$.

Enfin, si $u \in G$, alors il existe alors $n \in \mathbb{N}^*$ tels que $u \in \mathbb{U}_n$ et l'on a aussi $u^{-1} \in \mathbb{U}_n$, d'où $u^{-1} \in G$.

Donc

$\left(\bigcup_{n=1}^{+\infty} \mathbb{U}_n, \times\right)$ est un groupe abélien en tant que sous-groupe de $(\mathbb{U}, \times)$.

♦ ***Exercice 12.*** [○]

Démontrer qu'une partie stable, finie, non vide d'un groupe en est un sous-groupe. *Indication : Pour la symétrisabilité, on prendra un élément de la partie et on étudiera ses itérés.*

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

Soit A une partie finie de G qui est non vide et stable par $*$.

La stabilité de A fait donc partie des hypothèses.

Soit $a \in A$ (qui existe puisque A n'est pas vide). On veut démontrer que $a^{-1} \in A$. Considérons la suite $(a^n)_{n\geqslant 0}$ des itérés de a. C'est une suite d'éléments de A puisque A est stable. Comme A est finie, cette suite ne peut contenir qu'un nombre fini de termes. En particulier, il existe $p, k \in \mathbb{N}^*$ tel que $a^p = a^{p+k}$. En multipliant cette égalité par a^{-p-1},il vient $a^{-1} = a^{k-1}$. Or $a^{k-1} \in A$, donc $a^{-1} \in A$.

Soit $a \in A$ (qui existe puisque A n'est pas vide). Comme $a^{-1} \in A$ (on veint de le voir) et comme A est stable par $*$, on a $a * a^{-1} \in A$, c'est-à-dire $e \in A$.

En conclusion,

une partie stable, finie, non vide d'un groupe en est un sous-groupe.

♦ ***Exercice 13.*** [○] (Centre d'un groupe)
Soit $(G, *)$ un groupe. On définit le *centre* de G comme le sous-ensemble $Z(G)$ de G constitué des éléments de G qui commutent avec tous les autres. Démontrer que $Z(G)$ est un sous-groupe de G.

A faire.

♦ ***Exercice 14.*** [○] (Sous-groupes distingués)
Soit $(G, *)$ un groupe d'élément neutre e. Un sous-groupe H de G est *distingué* dans G lorsque

$$\forall a \in G, \quad \forall x \in H, \qquad a * x * a^{-1} \in H.$$

1. Démontrer que $\{e\}$ et G sont distingués dans G.
2. Que dire lorsque G est abélien ?
3. Démontrer que le noyau d'un morphisme de groupes $f : G \longrightarrow G'$ est distingué dans G.

1. AQT
2. Tous les sous groupes sont distingués.
3. Pour tout $a \in G$ et tout $x \in \operatorname{Ker} f$, on a

$$f(a * x * a^{-1}) = f(a) * f(x) * f(a)^{-1} = f(a) * e * f(a)^{-1} = e,$$

donc $a * x * a^{-1} \in \operatorname{Ker} f$. On a bien démontré que

le noyau d'un morphisme de groupes $f : G \longrightarrow G'$ est distingué dans G.

♦ ***Exercice 15.*** [○] (Union de sous-groupes)
Soient $(G, .)$ un groupe et H, K deux sous-groupes de G tels que $G = H \cup K$. Démontrer que $G = H$ ou $G = K$. *Indication : On pourra raisonner par l'absurde et trouver $x \in K \setminus H$ et $y \in H \setminus K$ puis examiner la position de xy.*

Supposons que $G \neq H$ et $G \neq K$. On sait alors qu'il existe $x \in K \setminus H$ et $y \in H \setminus K$. On considèr alors l'élément $xy \in G$. Ou $xy \in H$ et $x = (xy)y^{-1} \in H$, ou $xy \in K$ et $y = x^{-1}(xy) \in H$. Dans les deux cas, c'est absurde !

♦ ***Exercice 16.*** [⋆]
Soit $(G, *)$ un groupe, E un ensemble et $f : G \longrightarrow E$ une bijection. Sur E, on définit la loi $\star$ par

$$\forall x, y \in E, \qquad x \star y = f\big(f^{-1}(x) * f^{-1}(y)\big).$$

Démontrer que $(E, \star)$ est un groupe isomorphe à $(G, *)$.

A faire.

♦ ***Exercice 17.*** [∘] (Automorphismes intérieurs)
Soit $(G,*)$ un groupe. Pour tout $a \in G$, on note

$$\tau_a \left\{ \begin{array}{ccc} G & \longrightarrow & G \\ x & \longmapsto & a*x*a^{-1} \end{array} \right.$$

1. Soit $a \in G$. Démontrer que τ_a est un endomorphisme de G.
2. Démontrer que $\forall a,b \in G,\ \tau_a \circ \tau_b = \tau_{a*b}$ et en déduire que τ_a est un automorphisme de G. Préciser ${\tau_a}^{-1}$.

▶ On dit que τ_a est un automorphisme intérieur de G.

1. Pour tout $x,y \in G$, on a

$$\tau_a(x*y) = a*x*y*a^{-1} = a*x*a^{-1}*a*y*a^{-1} = \tau_a(x)*\tau_a(y),$$

donc

$$\boxed{\tau_a \text{ est un endomorphisme de } G.}$$

2. Pour $a,b \in G$, on a

$$\forall x \in G, \qquad (\tau_a \circ \tau_b)(x) = \tau_a\big(\tau_b(x)\big) = \tau_a(b*x*b^{-1}) = a*b*x*b^{-1}*a^{-1} = a*b*x*(a*b)^{-1} = \tau_{a*b}(x),$$

donc

$$\boxed{\forall a,b \in G, \qquad \tau_a \circ \tau_b = \tau_{a*b}.}$$

Soit $a \in G$. Remarquons que

$$\tau_a \circ \tau_{a^{-1}} = \tau_{a*a^{-1}} = \tau_e = \mathrm{Id}_G \qquad \text{et} \qquad \tau_{a^{-1}} \circ \tau_a = \tau_{a^{-1}*a} = \tau_e = \mathrm{Id}_G$$

donc

$$\boxed{\tau_a \text{ est un automorphisme de } G \text{ tel que } {\tau_a}^{-1} = \tau_{a^{-1}}.}$$

♦ ***Exercice 18.*** [⋆]
Démontrer que les groupes $(\mathbb{Q}_+^*,\times)$ et $(\mathbb{Q},+)$ ne sont pas isomorphes. *Indication :* $\sqrt{2}$.

Raisonnons par l'absurde en supposant qu'il existe un isomorphisme $\varphi : (\mathbb{Q},+) \longrightarrow (\mathbb{Q}_+^*,\times)$.
On sait que $\varphi(0) = 1$ et $\forall x,y \in \mathbb{Q}_+^*,\ \varphi(x+y) = \varphi(x)\varphi(y)$.
Comme $2 \in \mathbb{Q}_+^*$, il possède un antécédent a dans $\mathbb{Q}$ par φ. Le nombre $a/2$ est encore un rationnel, ce qui autorise le calcul de $\varphi(a/2)$. Or

$$\varphi\Big(\frac{a}{2}\Big)^2 = \varphi(a) = 2,$$

donc

$$\varphi\Big(\frac{a}{2}\Big) = \pm\sqrt{2},$$

ce qui est absurde puisque $\varphi(a/2)$ devrait appartenir à $\mathbb{Q}$.
Donc

$$\boxed{\text{les groupes } (\mathbb{Q}_+^*,\times) \text{ et } (\mathbb{Q},+) \text{ ne sont pas isomorphes.}}$$

♦ ***Exercice 19.*** [⋆]
Démontrer que les groupes $(\mathbb{R}^*,\times)$ et $(\mathbb{C}^*,\times)$ ne sont pas isomorphes.

Raisonnons par l'absurde en supposant qu'il existe un isomorphisme $\varphi : (\mathbb{C}^*,\times) \longrightarrow (\mathbb{R}^*,\times)$.
On sait que $\varphi(1) = 1$ et $\forall x,y \in \mathbb{C}^*,\ \varphi(xy) = \varphi(x)\varphi(y)$.
On a

$$\varphi(-1)^2 = \varphi(1) = 1$$

donc

$$\varphi(-1) = \pm 1.$$

Or

$$\varphi(-1) = \varphi(i^2) = \varphi(i)^2 \geqslant 0,$$

donc

$$\varphi(-1) = 1,$$

c'est-à-dire

$$\varphi(-1) = \varphi(1).$$

C'est absurde puisque φ est injective.

Donc

les groupes $(\mathbb{R}^*, \times)$ et $(\mathbb{C}^*, \times)$ ne sont pas isomorphes.

C. Anneaux

♦ ***Exercice 20.*** [○]
Soit $(A, +, \times)$ un anneau. Quel est le nom de la propriété « $A \setminus \{0\}$ est stable par $\times$ » ?

La stabilité de $A \setminus \{0\}$ par $\times$ dit que $\forall a, b \in A \setminus \{0\},\ ab \in A \setminus \{0\}$ ou encore $\forall a, b \in A,\ (a \neq 0 \text{ et } b \neq 0) \Longrightarrow (ab \neq 0)$. En contraposant, on obtient $\forall a, b \in A,\ (ab = 0) \Longrightarrow (a = 0 \text{ ou } b = 0)$. On voit donc que

la propriété « $A \setminus \{0\}$ est stable par $\times$ » est l'intégrité.

♦ ***Exercice 21.*** [⋆] (Nilpotence)
Soit $(A, +, \times)$ un anneau. Un élément de A est dit *nilpotent* lorsque $\exists n \in \mathbb{N},\ x^n = 0$.

1. Soit $x, y \in A$. Démontrer que si xy est nilpotent, alors yx l'est aussi.
2. Soit x un élément nilpotent. Démontrer que $1 - x$ est inversible et calculer son inverse.
3. Dans cette question, on suppose que A est commutatif.
   a) Démontrer que, si x et y sont deux éléments nilpotents, alors $-x$, xy et $x + y$ sont nilpotents.
   b) Démontrer que l'ensemble $G = \{1 - x : x \text{ nilpotent}\}$ est un groupe pour la loi $\times$.

1. On a $(yx)^{n+1} = y(xy)^n x = y0x = 0$, donc

   si xy est nilpotent, yx l'est aussi.

2. On a

   $$(1-x)(1+x+x^2+\cdots+x^{n-1}) = 1+x+x^2+\cdots+x^{n-1}-x-x^2-\cdots-x^{n-1}-x^n = 1-x^n = 1$$

   et, de même,

   $$(1+x+x^2+\cdots+x^{n-1})(1-x) = 1.$$

   Donc

   $1 - x$ est inversible d'inverse $1 + x + x^2 + \cdots + x^{n-1}$.

3. a) Soient x et y deux éléments nilpotents d'indices de nilpotence n_1 et n_2. D'une part, on a

   $$(-x)^{n_1} = (-1)^{n_1} x^{n_1} = (-1)^{n_1}.0 = 0,$$

   et, comme la loi est commutative, on a d'autre part

   $$(xy)^{n_1} = x^{n_1} y^{n_1} = 0.y^{n_1} = 0$$

   et

   $$(x+y)^{n_1+n_2} = \sum_{k=0}^{n_1+n_2} \binom{n_1+n_2}{k} x^k y^{n_1+n_2-k} = \sum_{k=0}^{n_1+n_2} \binom{n_1+n_2}{k} 0 = 0.$$

   Donc

   si x et y sont deux éléments nilpotents d'un anneau commutatif, alors $-x$, xy et $x + y$ sont aussi nilpotents.

b) Démontrons que G est un sous-groupe de $\big(U(A),\times\big)$.
On sait que $G \subset U(A)$ d'après la question 2.
Comme 0 est nilpotent, on a $1-0 \in G$, c'est-à-dire $1 \in G$.
Soient $1-x$ et $1-y$ deux éléments de G, ce qui singifie que x et y sont nilpotents. Alors $(1-x)(1-y) = 1-(x+y-xy)$. Comme x et y sont nilpotents, les résultats de la question a) disent que $x+y-xy$ est nilotente. Cela signifie que $(1-x)(1-y) \in G$.
Soit $1-x \in G$ un élément de G. Alors $(1-x)^{-1} = 1+x+x^2+\cdots+x^{n-1} = 1-(-x-x^2-\cdots-x^{n-1})$ d'après 2. Comme x est nilpotent, les résultats de la question a) disent que $-x-x^2-\cdots-x^{n-1}$ l'est aussi. Donc $(1-x)^{-1} \in G$.
En conclusion,

$\boxed{G \text{ est un sous-groupe de } \big(U(A),\times\big).}$

♦ ***Exercice 22.*** [⋆]
Soient $(A,+,\times)$ un anneau et $a \in A$. On suppose que a admet un unique inverse à droite (c'est-à-dire $\exists! b \in A,\ ab=1$). Démontrer que a est simplifiable et en déduire que a est inversible.

On note b l'unique inverse à droite de a dans A de sorte que

$$ab = 1 \qquad (*).$$

L'élément a ayant un inverse à droite, il est clairement simplifiable à droite. Démontrons qu'il est simplifiable à gauche. Pour cela, on considère $x, y \in A$ tels que

$$ax = ay.$$

On a alors

$$a(x-y) = 0 \qquad (**).$$

En ajoutant les égalités $(*)$ et $(**)$, il vient alors

$$a(x-y+b) = 1,$$

ce qui démontre que $x-y-b$ est un inverse à droite de a dans A. Comme le seul inverse à droite de a dans A est b, on en déduit que

$$x-y+b = b,$$

c'est-à-dire

$$x-y = 0$$

ou encore

$$x = y.$$

On ainsi démontré que a est simplifiable à gauche et donc que

$\boxed{a \text{ est simplifiable.}}$

En multipliant $(*)$ par a à droite, on obtient

$$aba = a,$$

ce qui permet de simplifier par a à gauche pour obtenir

$$ba = 1.$$

Par conséquent,

$\boxed{a \text{ est inversible, d'inverse } b.}$

♦ ***Exercice 23.*** [⋆]
Soient $(A,+,\times)$ un anneau et $a,b\in A$. On suppose que $1-ab$ est inversible Démontrez que $1-ba$ est inversible.

Indication : Pour deviner l'inverse de $(1-ba)$, on utilisera (au brouillon et sans le dire à personne) la formule $(1-x)^{-1}=\sum_{k=0}^{+\infty}x^k$ en précisant d'où elle peut bien sortir.

Pour résoudre cet exercice, autorisons-nous tout d'abord à écrire quelques horreurs, inspirées de ce qui pourrait se faire dans les réels. On a

$$(1-ba)^{-1}=\sum_{k=0}^{+\infty}(ba)^k=1+\sum_{k=1}^{+\infty}(ba)^k=1+\sum_{k=1}^{+\infty}b(ab)^{k-1}a=1+b\Big(\sum_{k=1}^{+\infty}(ab)^{k-1}\Big)a=1+b(1-ab)^{-1}a.$$

Tout cela n'était certes pas bien joli mais cela nous a permis de deviner qui est l'inverse de $1-ba$. Du coup, il ne reste plus qu'à vérifier que cela marche ! Pas très moral mais très efficace !

On a

$$\begin{aligned}(1-ba)\big(1+b(1-ab)^{-1}a\big) &= (1-ba)+(1-ba)b(1-ab)^{-1}a\\ &= (1-ba)+(b-bab)(1-ab)^{-1}a\\ &= (1-ba)+b(1-ab)(1-ab)^{-1}a\\ &= (1-ba)+ba\\ &= 1\end{aligned}$$

et

$$\begin{aligned}(1-ba)\big(1+b(1-ab)^{-1}a\big)(1-ba) &= (1-ba)+b(1-ab)^{-1}a(1-ba)\\ &= (1-ba)+b(1-ab)^{-1}(a-aba)\\ &= (1-ba)+b(1-ab)^{-1}(1-ab)a\\ &= (1-ba)+ba\\ &= 1,\end{aligned}$$

donc

$$\boxed{1-ba \text{ est inversible d'inverse } 1+b(1-ab)^{-1}a.}$$

♦ ***Exercice 24.*** [⋆]
On pose $\mathbb{Z}[i]=\{a+ib : a,b\in\mathbb{Z}\}$ l'ensemble des *entiers de Gauß*.

1. Démontrer que $\mathbb{Z}[i]$ est un sous-anneau de $(\mathbb{C},+,\times)$.
2. Déterminer les éléments inversibles de $\mathbb{Z}[i]$.
3. Démontrer que $\forall(u,v)\in\mathbb{Z}[i]\times(\mathbb{Z}[i]\setminus\{0\}),\ \exists(q,r)\in\mathbb{Z}[i]^2,\ u=vq+r$ avec $|r|<|v|$. On dit que $\mathbb{Z}[i]$ est *euclidien*.

1. Les nombres 0 et 1 appartiennent bien à $\mathbb{Z}[i]$ car $0=0+i0$ et $1=1+i0$.
   Si $a+ib$ et $c+id$ appartiennent à $\mathbb{Z}[i]$ alors
   $$-(a+ib)=(-a)+i(-b),(a+ib)+(c+id)=(a+c)+i(b+d)\in\mathbb{Z}[i]$$
   et
   $$(a+ib)(c+id)=(ac-bd)+i(ad+bc)\in\mathbb{Z}[i].$$
   Donc
   $$\boxed{\mathbb{Z}[i] \text{ est bien un sous-anneau de } \mathbb{C}.}$$
2. Deux solutions pour le prix d'une !

   Solution géométrique : Les unités sont sur le cercle unité sinon elles-mêmes ou leurs inverses sont strictement dans le disque unité où il n'y a que 0. Donc les seules unités possibles sont $1,i,-1,-i$ et ce sont bien des éléments inversibles.

   Solution arithmétique : Soit $a+ib\in U(\mathbb{Z}[i])$. Alors $1/(a+ib)\in\mathbb{Z}[i]$. Or $1/(a+ib)=a/(a^2+b^2)-ib/(a^2+b^2)$ donc $a^2+b^2\mid a$ et $a^2+b^2\mid b$. Cela n'est clairement possible que si $(a,b)=(0,\pm1)$ ou

$(a,b) = (\pm 1, 0)$, c'est-à-dire si $a + ib \in \{1, i, -1, -i\}$. On vérifie réciproquement que $\{1, i, -1, -i\} \subset U(\mathbb{Z}[i])$.
Conclusion : On a

$$\boxed{U(\mathbb{Z}[i]) = \{1, i, -1, -i\}.}$$

3. Soit $(u, v) \in \mathbb{Z}[i] \times (\mathbb{Z}[i] \setminus \{0\})$. Dans le plan complexe, les éléments de $\mathbb{Z}[i]$ sont tous les points à coordonnées entières ce qui forme un « quadrillage » du plan. Du coup, il est clair qu'il existe au moins un $q \in \mathbb{Z}[i]$ dont la distance à u/v est inférieur ou égale à $\sqrt{2}/2$, c'est-à-dire $|u/v - q| \leqslant \sqrt{2}/2 < 1$ ou encore $|u - vq| < |v|$. On pose $r = u - vq$ de sorte que $r \in \mathbb{Z}[i]$ puisque $\mathbb{Z}[i]$ est un anneau. On a donc $u = vq + r$ avec $q, r \in \mathbb{Z}[i]$ et $|r| < |v|$. En conclusion,

$$\boxed{\mathbb{Z}[i] \text{ est euclidien.}}$$

Remarque : Le caractère euclidien de cet anneau permet de démontrer que tous les entiers de Gauß se décompose, de manière unique, en un produit d'entiers irréductibles. On peut donc faire de l'arithmétique dans $\mathbb{Z}[i]$.

D. Corps

♦ ***Exercice 25.*** [○]
L'ensemble $\mathbb{D} = \bigcup_{k=0}^{+\infty} 10^{-k}\mathbb{Z}$ des décimaux est-il un corps pour l'addition et la multiplication usuelles ?

Ben non puisque 3 est dans $\mathbb{D}$ mais son inverse $1/3$ n'y est pas sinon il existerait $p \in \mathbb{Z}$ et $n \in \mathbb{N}$ tel que $1/3 = p/10^n$, c'est-à-dire $10^n = 3p$, ce qui obligerait 10^n à être divisible par 3 (alors que ses seuls facteurs premiers sont 2 et 5). Donc

$$\boxed{(\mathbb{D}, +, \times) \text{ n'est pas un corps.}}$$

♦ ***Exercice 26.*** [⋆]
Soit A un anneau commutatif, fini et intègre.
1. Soit $a \in A \setminus \{0\}$. Démontrer que l'application

$$\varphi \left\{ \begin{array}{ccc} A & \longrightarrow & A \\ b & \longmapsto & ab \end{array} \right.$$

est injective.
2. Démontrer que A est un corps.

1. Supposons que $\varphi(b) = \varphi(b')$. Alors $ab = ab'$, d'où $a(b - b') = 0$. Comme A est intègre et $a \neq 0$, on a donc $b - b' = 0$, c'est-à-dire $b = b'$ et

$$\boxed{\varphi \text{ est injective.}}$$

Comme φ est une injection entre deux ensembles finis de même cardinal, on peut affirmer que

$$\boxed{\varphi \text{ est bijective.}}$$

2. L'anneau A est déjà commutatif et intégre. Si $a \in A$ et $a \neq 0$, alors, d'après la question 1, il existe $b \in A$ tel que $ab = \varphi(b) = 1$ et $a \in A^*$, ce qui signifie que a est inversible. Ainsi $U(A) = A^*$ et

$$\boxed{A \text{ est un corps.}}$$

Note : l'hypothèse de commutativité n'est pas nécessaire...

♦ ***Exercice 27.*** [○]
Quels sont les sous-corps de $(\mathbb{Q}, +, \times)$?

Un sous-corps de $\mathbb{Q}$ doit contenir 1, donc tous les itérés additifs de 1, c'est-à-dire tous les entiers relatifs. Il doit alors contenir tous les inverses de ces entiers non nuls et aussi tous les itérés additifs de ces inverses, c'est-à-dire tous les rationnels. Par conséquent,

le seul sous-corps de $(\mathbb{Q}, +, \times)$ est $\mathbb{Q}$ lui-même.

♦ ***Exercice 28.*** [○]
On note $\mathbb{Q}(i) = \{a + bi : a, b \in \mathbb{Q}\}$. Démontrer que $\big(\mathbb{Q}(i), +, \times\big)$ est un corps, appelé corps des *nombres de Gauß*.

A faire.

♦ ***Exercice 29.*** [⋆]
Soit A un anneau commutatif non réduit à $\{0\}$.

1. On suppose que les seuls idéaux de A sont les idéaux triviaux ($\{0\}$ et A). Démontrer que A est un corps. *Indication : Si $x \in A \setminus \{0\}$, considérer l'idéal xA.*
2. Un idéal I de A est dit *premier* lorsque $I \neq A$ et $\forall x, y \in A,\ (xy \in I) \Longrightarrow (x \in I \text{ ou } y \in I)$.
   On suppose que tous les idéaux de A (sauf A) sont premiers. Démontrer que A est intègre, puis que $x \in x^2A$ pour tout x et enfin que A est un corps.

1. Soit $x \in A \setminus \{0\}$. Considérons l'idéal xA. Comme $x \neq 0$, on a $xA \neq \{0\}$ donc $xA = A$. Dès lors $1 \in xA$, ce qui démontre l'existence de $a \in A$ tel que $1 = xa$. Ainsi x est inversible. Cela prouve que $U(A) = A \setminus \{0\}$ et donc que

   A est un corps.

   Remarque : La réciproque est vraie. Nous l'avons démontré en cours.

2. Soient $x, y \in A$ tels que $xy = 0$. Alors xy appartient à l'idéal $\{0\}$. Comme c'est un idéal premier (comme tous les autres sauf A), cela implique que $x \in \{0\}$ ou $y \in \{0\}$, c'est-à-dire $x = 0$ ou $y = 0$. Donc

   A est intègre.

   Soit $x \in A$. L'élément $x^2 = xx$ appartient clairement à l'idéal x^2A. Comme cet idéal est premier, on en déduit que $x \in x^2A$ ou $x \in x^2A$. Donc

   $\forall x \in A, \qquad x \in x^2A.$

   Soit $x \in A \setminus \{0\}$. Comme $x \in x^2A$, on peut affirmer l'existence de $a \in A$ tel que $x = x^2a$, c'est-à-dire $x(1 - xa) = 0$. Comme A est intègre et $x \neq 0$, on a $1 - xa = 0$, c'est-à-dire $ax = 1$. Donc x est inversible. On en conclut que

   A est un corps.

♦ ***Exercice 30.*** [⋆] (Endomorphismes de $\mathbb{Q}$, $\mathbb{R}$ et $\mathbb{C}$)
On rappelle un endomorphisme de corps de $\mathbb{K}$ est une application $f : \mathbb{K} \longrightarrow \mathbb{K}$ telle que $f(1) = 1$,

$$\forall x, y \in \mathbb{K}, \quad f(x + y) = f(x) + f(y) \qquad \text{et} \qquad \forall x, y \in \mathbb{K}, \quad f(xy) = f(x)f(y).$$

1. Soit f un endomorphisme de corps de $\mathbb{Q}$. Démontrer que f est l'identité de $\mathbb{Q}$.
2. Soit f un endomorphisme de corps de $\mathbb{R}$. Justifier que f est une fonction impaire vérifiant $\forall x \in \mathbb{Q},\ f(x) = x$. Démontrer ensuite que $\forall x \geqslant 0,\ f(x) \geqslant 0$ puis que f est croissant. En déduire que f est l'identité de $\mathbb{R}$.
3. Soit f un endomorphisme de corps de $\mathbb{C}$ tel que $f(\mathbb{R}) \subset \mathbb{R}$. Démontrer que f est ou bien l'identité de $\mathbb{C}$ ou bien la conjugaison complexe.

1. Démontrons la propriété $\mathscr{P}_n : \forall x \in \mathbb{R},\ f(nx) = n$ par récurrence sur $n \in \mathbb{N}^*$.

   Initialisation : On a $f(1) = 1$ par hypothèse donc $\mathscr{P}_1$ est vraie.

   Hérédité : Fixons $n \in \mathbb{N}^*$. Supposons que $\mathscr{P}_n$ soit vérifiée et démontrons $\mathscr{P}_{n+1}$. On a

   $$f(n+1) = f(n) + f(1) = n + 1,$$

   où l'on a utilisé l'hypothèse d'additivité de f et l'hypothèse de récurrence, ce qui établit $\mathscr{P}_{n+1}$.

   Conclusion : D'après le principe de récurrence, on a $\forall n \in \mathbb{N}^*,\ f(n) = n$.

   Reste à traiter le cas où $n = 0$, c'est-à-dire à démontrer que $f(0) = 0$. On utilise pour cela l'hypothèse d'additivité de f sous la forme : $f(0) = f(0+0) = f(0) + f(0)$, d'où $f(0) = 0$.

   Finalement, on a démontré que

   $$\boxed{\forall n \in \mathbb{N}, \qquad f(n) = n.}$$

   Soit $x \in \mathbb{R}$. La nullité de f en 0 et l'hypothèse d'additivité de f permettent d'écrire l'égalité $0 = f(0) = f(x - x) = f(x) + f(-x)$, d'où $f(x) = -f(-x)$. Cela traduit le fait que

   $$\boxed{f \text{ est impaire sur } \mathbb{R}.}$$

   Soit $m \in \mathbb{Z}$. Si $m \in \mathbb{N}$, on sait, d'après b), que $f(m) = m$. Si, au contraire, $m \in \mathbb{Z} \setminus \mathbb{N}$, on note que $-m \in \mathbb{N}^*$, d'où, d'après b), $f(-m) = -m$. De plus, l'imparité de f nous permet d'écrire $f(-m) = -f(m)$. En définitive, on a $f(m) = m$ également dans ce cas.
   Donc

   $$\boxed{\forall m \in \mathbb{Z}, \qquad f(m) = m.}$$

   Soit $r \in \mathbb{Q}$. On peut écrire r sous la forme p/q avec $(p, q) \in \mathbb{Z} \times \mathbb{N}^*$. Alors

   $$qf\big(r\big) = f(qr) = f(p) = p,$$

   où l'on a successivement utilisé la question 1, l'égalité $qr = p$ et la question c). Il s'ensuit, après division par q, que $f(r) = p/q = r$. Donc

   $$\boxed{\forall r \in \mathbb{Q}, \qquad f(r) = r.}$$

2. En raisonnant exactement comme à la question précédente, on démontre que

   $$\boxed{f \text{ est une fonction impaire vérifiant } \forall x \in \mathbb{Q},\ f(x) = x.}$$

   Soit $x \geqslant 0$. L'astuce consiste à écrire que $x = (\sqrt{x})^2$ puis à utiliser l'hypothèse de multiplicativité de f pour obtenir

   $$f(x) = f\big((\sqrt{x})^2\big) = f\big(\sqrt{x}\big)^2 \geqslant 0$$

   d'où

   $$\boxed{\forall x \geqslant 0, \qquad f(x) \geqslant 0.}$$

   Soient $x, y \in \mathbb{R}$ tel que $x < y$. On a $f(y - x) \geqslant 0$ car $y - x > 0$, ce qui donne $f(y) - f(x) \geqslant 0$ et donc $f(y) \geqslant f(x)$. Cela traduit bien que

   $$\boxed{f \text{ est croissante sur } \mathbb{R}.}$$

   Raisonnons par l'absurde en supposant l'existence de $a \in \mathbb{R}$ tel que $f(a) \neq a$. Supposons que $a < f(a)$ (l'autre cas est similaire). La densité de $\mathbb{Q}$ dans $\mathbb{R}$ assure l'existence de $r \in\ ]a; f(a)[$. Comme $a < r$, la croissance de f implique que $f(a) \leqslant f(r) = r$, ce qui contredit le fait que $r < f(a)$. Donc $\forall x \in \mathbb{R}, f(x) = x$, ce qui signifie que

   $$\boxed{\text{le seul endomorphisme de corps de } \mathbb{R} \text{ est l'identité.}}$$

3. Comme $f(\mathbb{R}) \subset \mathbb{R}$, les résultats de la question précécente nous dit que $\forall x \in \mathbb{R},\ f(x) = x$.
   Par ailleurs, on a

   $$f(i)^2 = f(i^2) = f(-1) = -1,$$

   donc

   $$f(i) = \pm i.$$

   Si $f(i) = i$, alors pour tout nombre complexe $a + ib$ avec $a, b \in \mathbb{R}$, on a

   $$f(a + ib) = f(a) + f(i)f(b) = a + ib,$$

donc f est l'identité.
Si $f(i) = -i$, alors pour tout nombre complexe $a + ib$ avec $a, b \in \mathbb{R}$, on a

$$f(a + ib) = f(a) + f(i)f(b) = a - ib,$$

donc f est la conjugaison.
En conclusion,

les seuls endomorphismes de corps de $\mathbb{C}$ qui laissent $\mathbb{R}$ stable sont l'identité et la conjugaison.