13. Structures algébriques usuelles, corrigé

Exercice 1. (m) Soit $E = [0,1]$. On définit la loi $*$ sur E par $\forall x, y \in E,\ x * y = x + y - xy$.

1) $*$ est clairement commutative ($\forall x, y \in E,\ x * y = y * x$). Pour l'associativité, si on prend $x, y, z \in E$:

$$\begin{aligned} x * (y * z) &= x * (y + z - yz) \\ &= x + y + z - yz - x(y + z - yz) \\ &= x + y + z - yz - xy - xz + zyz. \end{aligned}$$

Un calcul similaire montre que $(x*y)*z = x+y+z-xy-yz-xz+xyz$ ce qui prouve l'associativité.

Il ne reste plus qu'à montrer que E est stable par $*$ (pour avoir une lci). Si on prend $x, y \in [0,1]$, alors on a tout d'abord :

$$x * y = x(1 - y) + y.$$

Puisque $1 - y \geq 0$, $x \geq 0$ et $y \geq 0$, on a bien $x * y \geq 0$. De plus, on a aussi :

$$x * y = x(1 - y) + y = x(1 - y) + y - 1 + 1 = (x - 1)(1 - y) + 1.$$

Puisque $x - 1 \leq 0$ et $1 - y \geq 0$, on a donc $x * y \leq 1$. On a donc bien $x * y \in [0,1]$ ce qui prouve que E est stable par $*$.

2) On cherche $e \in E$ tel que $\forall x \in E,\ x * e = e * x = x$. On remarque que $e = 0 \in E$ convient. Pour trouver les éléments inversibles, si on fixe $x \in E$, on cherche $y \in E$ tel que $x * y = y * x = 0$. On étudie donc l'équation :

$$x + y - xy = 0 \Leftrightarrow y(1 - x) = -x.$$

On remarque que $x = 1$ n'est pas inversible (on obtient une absurdité). Pour $x \in [0,1[$, on trouve comme inverse potentiel $y = \dfrac{x}{x-1}$. Or, pour $x \in]0,1[$, on a $x > 0$ et $x - 1 < 0$. On a donc $y < 0$, ce qui entraine que $y \notin E$. On en déduit donc finalement que 0 est le seul élément inversible pour $*$ dans E.

Montrer que $*$ possède un élément neutre. Quels sont les éléments de E inversibles pour $*$?

Exercice 2.

1) Puisque x et y commutent et que $*$ est associtative, on a $(x*y)*(x*y) = (x*x)*(y*y) = x*y$. On a donc bien $x * y$ idempotent.

2) On suppose que x est idempotent et inversible. On a donc $x * x = x$ et puisque x^{-1} existe, en multipliant par x^{-1} à droite, on obtient $x * x * x^{-1} = x * x^{-1}$, ce qui entraine que $x * e = e$ (on note e l'élément neutre). On a donc $x = e$, ce qui entraine $x^{-1} = e$. Puisque $e * e = e$, on a bien x^{-1} est idempotent.

Exercice 3. On a clairement $Z(G) \subset G$. On a $e \in Z(G)$ car $\forall x \in G,\ x * e = x$ et $e * x = x$ donc $e*x = x*e$. Supposons à présent que $x_1, x_2 \in G$. On a alors pour tout $y \in G$ en utilisant l'associativité de $*$ et le fait que x_1 et x_2 commutent avec tous les éléments de G :

$$\begin{aligned}(x_1 * x_2) * y &= x_1 * (x_2 * y)\\ &= x_1 * (y * x_2)\\ &= (x_1 * y) * x_2\\ &= (y * x_1) * x_2\\ &= y * (x_1 * x_2).\end{aligned}$$

On a donc $x_1 * x_2 \in Z(G)$.

Enfin, si $x \in Z(G)$, alors, pour tout $y \in G$, on a $x * y = y * x$. En multipliant par x^{-1} à gauche, on obtient $y = x^{-1} * y * x$. En multipliant par x^{-1} à droite, on obtient à présent $y * x^{-1} = x^{-1} * y$. On en déduit que $x^{-1} \in Z(G)$.

On a donc bien que $Z(G)$ est un sous-groupe de G.

Exercice 4. On a $1 \in \mathbb{U}_1$ par exemple donc $1 \in \bigcup_{n\in\mathbb{N}^*} \mathbb{U}_n$. Soient $z_1, z_2 \in \bigcup_{n\in\mathbb{N}^*} \mathbb{U}_n$. Il existe alors n_1 et n_2 dans $\mathbb{N}^*$ tels que $z_1 \in \mathbb{U}_{n_1}$ et $z_2 \in \mathbb{U}_{n_2}$. On a donc $z_1^{n_1} = 1$ et $z_2^{n_2} = 1$. On en déduit alors que :

$$(z_1 z_2)^{n_1 n_2} = (z_1^{n_1})^{n_2}((z_2)^{n_2})^{n_1} = 1.$$

On a donc $z_1 z_2 \in \mathbb{U}_{n_1 n_2}$ d'où $z_1 z_2 \in \bigcup_{n\in\mathbb{N}^*} \mathbb{U}_n$.

Si $z \in \bigcup_{n\in\mathbb{N}^*} \mathbb{U}_n$, alors il existe $n \in \mathbb{N}^*$ tel que $z \in \mathbb{U}_n$ et puisque $\mathbb{U}_n$ est un groupe pour la loi $\times$, on a $z^{-1} \in \mathbb{U}_n$ et donc $z^{-1} \in \bigcup_{n\in\mathbb{N}^*} \mathbb{U}_n$.

On en déduit que $\bigcup_{n\in\mathbb{N}^*} \mathbb{U}_n$ est un groupe. Ce n'est par contre pas égal à $\mathbb{U}$. En effet, posons $z = e^{2i\pi\sqrt{2}}$. Supposons par l'absurde que $z \in \bigcup_{n\in\mathbb{N}^*} \mathbb{U}_n$. Il existe alors $n \in \mathbb{N}^*$ tel que $z \in \mathbb{U}_n$ et donc tel que $z^n = 1$. Or, on a :

$$z^n = 1 \Leftrightarrow e^{2i\pi\sqrt{2}n} = 1 \Leftrightarrow 2\pi\sqrt{2}n \equiv 0\ [2\pi].$$

Ceci entraine que $\exists p \in \mathbb{Z}\ /\ 2\pi\sqrt{2}n = p2\pi$, soit que $\sqrt{2} = \dfrac{p}{n}$. On a alors $\sqrt{2} \in \mathbb{Q}$: absurde ! On a donc $z \notin \bigcup_{n\in\mathbb{N}^*} \mathbb{U}_n$ alors que $z \in \mathbb{U}$ (car $|z| = 1$ car pour tout $\theta \in \mathbb{R},\ |e^{i\theta}| = 1$).

Exercice 5.

1) Remarquons déjà que aHa^{-1} est bien défini car $a \in G$ est inversible et donc a^{-1} existe bien. On a de plus puisque G est stable par $*$ que pour tout $x \in H \subset G$, $a * x * a^{-1} \in G$. On a donc $aHa^{-1} \subset G$. On va alors utiliser la caractérisation des sous-groupes :
- aHa^{-1} est non vide (il contient par exemple le neutre e car $e \in H$ et $a * e * a^{-1} = a * a^{-1} = e$).
- Enfin, si $x, y \in aHa^{-1}$, alors par définition il existe $x_2, y_2 \in H$ tels que $x = a * x_2 * a^{-1}$ et $y = a * y_2 * a^{-1}$. y est alors dans G et est inversible. On a alors :

$$y^{-1} = (a * y_2 * a^{-1})^{-1} = (a^{-1})^{-1} * y_2^{-1} * a^{-1} = a * y_2 * a^{-1}.$$

On en déduit par associativité de $*$ que :

$$x * y^{-1} = a * x_2 * a^{-1} * a * y_2^{-1} * a^{-1} = a * x_2 * y_2^{-1} * a^{-1}.$$

Enfin, puisque $x_2 * y_2^{-1} \in H$ (car H est un groupe), on a bien $x * y^{-1} \in aHa^{-1}$.

Ces deux points entrainent que H est un sous groupe de G.

2) Montrons que $aH = H$ si et seulement si $a \in H$.

Supposons dans un premier temps que $aH = H$ soit un sous groupe de G. On a alors $e \in aH$ donc il existe $x \in H$ tel que $e = a * x$, ce qui entraine que $a = x^{-1}$. Puisque $x \in H$ et que H est un groupe, on en déduit que $x^{-1} \in H$, d'où $a \in H$.

Réciproquement, supposons que $a \in H$. On remarque alors que $aH \subset H$ (car H est stable par $*$). Réciproquement, si $x \in H$, on a $x = a*(a^{-1})*x$, ce qui entraine que $x \in aH$ (car $a^{-1}*x \in H$ puisque a et x sont dans H).

Exercice 6. Soient $x, y \in G$. On remarque que $x * x = e$ donc $x^{-1} = x$ et de meme $y^{-1} = y$. On a alors :

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

G est donc un groupe commutatif.

Exercice 7. (m) Soit $G = \mathbb{R}^* \times \mathbb{R}$ et $*$ la loi définie par :

$$\forall (x,y),(x',y') \in G,\ (x,y) * (x',y') = (xx', xy' + y).$$

1) On trouve comme élément neutre $(1,0)$ (fonctionne des deux côtés). La stabilité par $*$ ne pose aucun problème. L'associativité est un peu pénible à écrire mais ne pose pas de souci. En résolvant $(x,y) * (x',y') = (1,0)$, on trouve que $(x,y)^{-1} = \left(\frac{1}{x}, -\frac{y}{x}\right)$ qui est bien dans G (on vérifie que cette formule fonctionne également à gauche). Enfin, pour la non commutativité, on a par exemple $(1,2) * (2,1) = (2,3)$ et $(2,1) * (1,2) = (2,5)$ donc G n'est pas un groupe commutatif.

2) On a clairement $\mathbb{R}_+^* \times \mathbb{R} \subset \mathbb{R}^* \times \mathbb{R}$. L'élément neutre $(1,0)$ est également dans $\mathbb{R}_+^* \times \mathbb{R}$ et $\mathbb{R}_+^* \times \mathbb{R}$ est stable pour la loi $*$ (en effet, si x et x' sont strictements positifs, alors xx' aussi et donc $(x,y) * (x',y') \in \mathbb{R}_+^* \times \mathbb{R}$. Enfin, on avait trouvé comme inverse de (x,y) le couple $(\frac{1}{x}, -\frac{y}{x})$ et si $x > 0$, alors $\frac{1}{x} > 0$ donc l'inverse est également dans $\mathbb{R}_+^* \times \mathbb{R}$. On a donc bien un sous-groupe de $(G, *)$.

Exercice 8. La commutativité de $*$ ne pose pas de problème. Pour l'associativité, on calcule :

$$\begin{aligned}
(x_1 * x_2) * x_3 &= \left(\frac{x_1 + x_2}{1 + x_1 x_2}\right) * x_3 \\
&= \frac{\frac{x_1+x_2}{1+x_1x_2} + x_3}{1 + \frac{x_1x_3 + x_2x_3}{1+x_1x_2}} \\
&= \frac{x_1 + x_2 + x_3 + x_1x_2x_3}{1 + x_1x_2 + x_1x_3 + x_2x_3}.
\end{aligned}$$

On trouve exactement le même résultat pour $x_1 * (x_2 * x_3)$ donc la loi est associative. On vérifie sans difficulté que 0 est élément neutre pour la loi $*$. Il reste à vérifier la stabilité de G par $*$ et l'existence d'un inverse à tout élément de G.

Pour la stabilité, fixons $y \in]-1,1[$ et étudions la fonction $f : x \mapsto \frac{x+y}{1+xy}$ sur $]-1,1[$. Cette fonction est bien définie et dérivable sur cet intervalle. On a pour tout $x \in]-1,1[$:

$$f'(x) = \frac{1 - y^2}{(1+xy)^2} > 0.$$

Ceci entraine que f est strictement croissante. Or, on a $\lim_{x\to -1} f(x) = -1$ et $\lim_{x\to 1} f(x) = 1$. On a donc bien f à valeurs dans $]-1,1[$, ce qui entraine que G est stable pour la loi $*$.

On remarque enfin que si $x \in]-1,1[$, alors on a $x*(-x) = (-x)*x = 0$ et que $-x \in]-1,1[$. Tous les éléments de G sont donc inversibles pour $*$. On a donc bien $(G,*)$ qui est un groupe commutatif.

Exercice 9. Union de groupes. Si $G_1 \subset G_2$, on a $G_1 \cup G_2 = G_2$ qui est donc bien un groupe. On raisonne de même si $G_2 \subset G_1$. Le seul sens qui pose problème est la réciproque.

Supposons par la contraposée que G_1 n'est pas inclus dans G_2 et que G_2 n'est pas inclus dans G_1 et montrons que $G_1 \cup G_2$ n'est pas un groupe. Soit $a \in G_1$ tel que $a \notin G_2$ et $b \in G_2$ tel que $b \notin G_1$. Considérons $c = a*b$.

On a $c \notin G_1$. En effet, par l'absurde, si $c \in G_1$, alors puisque $a \in G_1$, on a $a^{-1} \in G_1$ (car G_1 est un groupe) et donc $a^{-1}*c \in G_1$ (car G_1 est un groupe). On a donc $b \in G_1$: absurde !

De même, on a $c \notin G_2$ (on multiplie par b^{-1} à droite pour avoir une absurdité).

On a donc a et b dans $G_1 \cup G_2$ et $a*b \notin G_1 \cup G_2$. $G_1 \cup G_2$ n'est donc pas un groupe.

Exercice 10. Soit $(G,*)$ un groupe non commutatif dont l'élément neutre est noté e. Soit $n \in \mathbb{N}^*$ tel que $(a*b)^n = e$.

On peut réécrire cette égalité comme $(a*b)*(a*b)*\ldots*(a*b) = e$, ou en utilisant l'associativité, on a alors $a*(b*a)*(b*a)*\ldots*(b*a)*b = e$, c'est à dire $a*(b*a)^{n-1}*b = e$. On peut alors multiplier cette égalité par a^{-1} à gauche. On obtient $(b*a)^{n-1}*b = a^{-1}$. On multiplie ensuite par a à droite, ce qui donne $(b*a)^n = e$.

Exercice 11.
Tout d'abord $(\mathbb{R}^*,\times)$ est bien un groupe (de neutre 1). On a $\varphi(1) = 1^2 = 1$ et pour $x,y \in \mathbb{R}^*$, $\varphi(x\times y) = (xy)^2 = x^2y^2 = \varphi(x)\times\varphi(y)$. On en déduit que φ est un morphisme de groupe.

On a alors $\ker(\varphi) = \{x \in \mathbb{R}^* \ / \ \varphi(x) = 1\} = \{-1,\}$ et $\mathrm{Im}(\varphi) = \{x^2,\ x \in \mathbb{R}^*\} = R_+^*$.

Exercice 12. Puisque φ est un morphisme de groupe, on a $\forall x,y \in \mathbb{R},\ \varphi(x+y) = \varphi(x)\varphi(y)$. Fixons $y \in \mathbb{R}$. Puisque φ est dérivable, on en déduit en dérivant par rapport Ã x que :

$$\forall x \in \mathbb{R},\ 1\times\varphi'(x+y) = \varphi'(x)\varphi(y).$$

En $x = 0$, on obtient alors que pour tout $y \in \mathbb{R}$, $\varphi'(y) = \varphi'(0)\varphi(y)$. En posant $\alpha = \varphi'(0) \in \mathbb{R}$, on en déduit que φ est solution de l'équation différentielle homogène :

$$\varphi' - \alpha\varphi = 0.$$

On en déduit qu'il existe $\lambda \in \mathbb{R}$ tel que $\forall x \in \mathbb{R},\ \varphi(x) = ke^{\alpha x}$. Or, puisque φ est un morphisme de groupe, on a $\varphi(0) = 1$ (φ envoie le neutre de $(\mathbb{R},+)$ sur le neutre de $(\mathbb{R}^*,\times)$). On a donc $k = 1$.

On en déduit finalement qu'il existe $\alpha \in \mathbb{R}$ tel que $\forall x \in \mathbb{R},\ \varphi(x) = e^{\alpha x}$. On peut alors vérifier réciproquement que pour tout $\alpha \in \mathbb{R}$, $x \mapsto e^{\alpha x}$ est bien un morphisme de groupe de $(\mathbb{R},+)$ dans $(\mathbb{R}_+^*,\times)$.

Exercice 13. On a tout d'abord $0 \in n\mathbb{Z}$ (car $0 = n\times 0$) donc $n\mathbb{Z} \neq \emptyset$. On a clairement $n\mathbb{Z} \subset \mathbb{Z}$. Enfin, si $x,y \in n\mathbb{Z}$, alors, il existe $k_1,k_2 \in \mathbb{Z}$ tels que $x = nk_1$ et $y = nk_2$. On a alors :

$$x - y = n(k_1 - k_2)$$

avec $k_1 - k_2 \in \mathbb{Z}$. On en déduit que $x - y \in n\mathbb{Z}$. Par caractérisation des sous-groupes, on en déduit que $n\mathbb{Z}$ est un sous-groupe de $\mathbb{Z}$ (et c'est donc un groupe).

Posons pour $x \in \mathbb{Z}$, $\varphi(x) = nx$. On a φ qui est bien définie de $\mathbb{Z}$ dans $n\mathbb{Z}$ et on a $\forall x, y \in \mathbb{Z}$, $\varphi(x+y) = n(x+y) = nx + ny = \varphi(x) + \varphi(y)$. φ est donc bien un morphisme de groupe. C'est de plus clairement un isomorphisme. En effet, elle est injective car si $nx_1 = nx_2$, alors $x_1 = x_2$ car $n \neq 0$ et si $y \in n\mathbb{Z}$, alors on a $x = \dfrac{y}{n} \in \mathbb{Z}$ et $\varphi(x) = y$ d'où la surjectivité. On a donc bien $\mathbb{Z}$ et $n\mathbb{Z}$ qui sont isomorphes.

Exercice 14. Supposons par l'absurde qu'il existe φ un morphisme de groupe bijectif de $(\mathbb{Z}, +)$ dans $(\mathbb{Z}^2, +)$. On a alors $\varphi(0) = (0,0)$. On a ensuite $\varphi(1) = (k_1, k_2)$ avec $k_1, k_2 \in \mathbb{Z}$. On montre alors par récurrence que pour $n \in \mathbb{N}$, $\varphi(n) = (nk_1, nk_2)$. Ensuite, on a que si $n < 0$:

$$\varphi(n) = \varphi(-(-n)) = -\varphi(-n) = -(-nk_1, -nk_2) = (nk_1, nk_2).$$

On en déduit finalement que pour $n \in \mathbb{Z}$, $\varphi(n) = (nk_1, nk_2)$. Ceci entraine que si $k_1 \neq 0$, le point $(0,1)$ n'est pas atteint par φ (car on a pour $n \neq 0$, $\varphi(n) = (nk_1, nk_2)$ et $nk_1 \neq 0$ et $\varphi(0) = (0,0) \neq (0,1)$. Si $k_1 = 0$, c'est cette fois le point $(1,0)$ qui n'est pas atteint (car pour $n \in \mathbb{Z}$, $\varphi(n) = (0, nk_2)$).

Ceci entraine qu'il n'y a pas d'isomorphisme de $(\mathbb{Z}, +)$ dans $(\mathbb{Z}^2, +)$.

Exercice 15.

1) On a $3 \in \mathbb{Z}$. Supposons qu'il existe $x \in \mathbb{Z}$ tel que $3 = x + x$. On a alors $x = \dfrac{3}{2} \notin \mathbb{Z}$: absurde ! On en déduit que $(\mathbb{Z}, +)$ ne vérifie pas (D).

Soit à présent $x \in \mathbb{Q}$. On a alors $\dfrac{x}{2} \in \mathbb{Q}$ et $x = \dfrac{x}{2} + \dfrac{x}{2}$. On en déduit que $\mathbb{Q}$ vérifie la propriété (D).

2) Soit φ un isomorphisme entre G_1 et G_2. Supposons que G_1 vérifie la propriété (D) et montrons que G_2 la vérifie. Soit $y_1 \in G_2$. Il existe alors (puisque φ est un isomorphisme) $x_1 \in G_1$ tel que $y_1 = \varphi(x_1)$. Puisque G_1 vérifie (D), il existe $x_2 \in G_1$ tel que $x_1 = x_2 *_1 x_2$. Puisque φ est un morphisme, on a alors :

$$y_1 = \varphi(x_1) = \varphi(x_2) *_2 \varphi(x_2).$$

En posant alors $y_2 = \varphi(x_2) \in G_2$, on a alors $y_1 = y_2 *_2 y_2$ ce qui entraine bien que G_2 vérifie (D).

Par l'absurde, s'il existait un isomorphisme entre $(\mathbb{Z}, +)$ et $(\mathbb{Q}, +)$, alors puisque $\mathbb{Q}$ vérifie la propriété (D), $\mathbb{Z}$ la vérifierait aussi ce qui n'est pas le cas d'après la première question. Il n'existe donc pas un tel isomorphisme.

3) *Applications.*

a) $\mathbb{R}^*$ ne vérifie pas (D) car $-1 \in \mathbb{R}^*$ et il n'existe pas de $x \in \mathbb{R}^*$ tel que $-1 = x^2$ (car $x^2 > 0$). Par contre, $\mathbb{R}_+^*$ vérifie la propriété (D) car si $x \in \mathbb{R}_+^*$, alors $x = \sqrt{x} \times \sqrt{x}$ et $\sqrt{x} \in \mathbb{R}_+^*$. D'après la question 2, on en déduit que $\mathbb{R}^*$ et $\mathbb{R}_+^*$ ne sont pas isomorphes.

b) Comme on l'a vu, $(\mathbb{R}^*, \times)$ ne vérifie pas (D). Cependant, $(\mathbb{C}^*, \times)$ la vérifie car pour tout $z \in \mathbb{C}^*$, il existe $z_2 \in \mathbb{C}^*$ tel que $z = z_2^2$ (car tout complexe admet une racine carrée dans $\mathbb{C}$, on peut le reprouver en passant par la forme exponentielle car $\rho e^{i\theta} = (\sqrt{\rho} e^{i\theta/2})^2$). D'après la question 2, on en déduit que $\mathbb{R}^*$ et $\mathbb{C}^*$ ne sont pas isomorphes.

Exercice 16. On pose $\varphi : \left\{ \begin{array}{ccc} \mathbb{R}_+^* \times \mathbb{U} & \to & \mathbb{C}^* \\ (x,u) & \to & xu \end{array} \right.$. φ est bien définie car $xu \neq 0$ car $x \neq 0$ et $u \neq 0$. On a $\varphi(1,1) = 1$ et pour $(x_1, u_1), (x_2, u_2) \in \mathbb{R}_+^* \times \mathbb{U}$, on a :

$$\begin{aligned}\varphi((x_1,u_1)*(x_2,u_2)) &= \varphi(x_1x_2,u_1u_2)\\ &= x_1x_2u_1u_2\\ &= x_1u_1\times x_2u_2\\ &= \varphi(x_1,u_1)\times\varphi(x_2,u_2).\end{aligned}$$

On en déduit que φ est un morphisme de groupe. Enfin, on sait que pour tout $z\in\mathbb{C}^*$, il existe un unique $r>0$ (le module) et un unique $z_0\in\mathbb{U}$ ($z_0=e^{i\theta}$ où θ est l'argument) tel que $z=rz_0=\varphi(r,z_0)$. On a donc bien que φ est bijectif. On a donc construit un isomorphisme entre $\mathbb{R}_+^*\times\mathbb{U}$ et $\mathbb{C}^*$, ce qui prouve que $(\mathbb{C}^*,\times)$ est isomorphe au groupe produit $(\mathbb{R}_+^*\times\mathbb{U})$.

Exercice 17.

1) f est bien définie car pour tout $x\in G$, x^{-1} existe et est dans G car G est un groupe. On remarque que $f\circ f=\mathrm{Id}_G$ (car pour tout $x\in G$, $f(f(x))=(x^{-1})^{-1}=x$). On en déduit que f est inversible et que $f^{-1}=f$. f est donc bien bijective.

2) On a toujours $f(e)=e^{-1}=e$. Montrons que f est un automorphisme si et seulement si $(G,*)$ est un groupe commutatif. Fixons $x,y\in G$. On a alors :

$$\begin{aligned}f(x*y)=f(x)*f(y) &\Leftrightarrow (x*y)^{-1}=x^{-1}*y^{-1}\\ &\Leftrightarrow y^{-1}*x^{-1}=x^{-1}*y^{-1}\\ &\Leftrightarrow (y^{-1}*x^{-1})^{-1}=(x^{-1}*y^{-1})^{-1}\\ &\Leftrightarrow x*y=y*x.\end{aligned}$$

On en déduit que f est un morphisme (donc un automorphisme car on sait qu'elle est bijective) si et seulement si G est un groupe commutatif.

Exercice 18.

1) On pose $\varphi:\left\{\begin{array}{ccc}\mathbb{U}_2\times\mathbb{U}_3 & \to & \mathbb{U}_6\\ (z_1,z_2) & \mapsto & z_1z_2\end{array}\right.$. φ est clairement un morphisme de groupe ($\varphi(1,1)=1$ et on vérifie que $\varphi((z_1,z_2)\times(z_1',z_2'))=\varphi(z_1z_1')\varphi(z_2z_2')$. φ est également bien définie car si $z_1\in\mathbb{U}_2$ et $z_2\in\mathbb{U}_3$, alors $z_1z_2\in\mathbb{U}_6$ car $(z_1z_2)^6=z_1^6z_2^6=1$.

Il reste à montrer la bijectivité. On liste tous les cas :
— $\varphi(1,1)=1=e^{0i\pi/6}$
— $\varphi(-1,1)=-1=e^{6i\pi/6}$
— $\varphi(1,j)=j=e^{4i\pi/6}$
— $\varphi(-1,j)=-j=e^{10i\pi/6}$
— $\varphi(1,j^2)=j^2=e^{8i\pi/6}$
— $\varphi(-1,j^2)=-j^2=e^{14i\pi/6}=e^{2i\pi/6}$.
On atteint donc bien tous les éléments de $\mathbb{U}_6$ d'où la bijectivité.

2) On remarque que pour tous les éléments de $\mathbb{U}_2\times\mathbb{U}_2$, on a $(x,y)^2=(x^2,y^2)=(1,1)$. Ceci est faux dans $\mathbb{U}_4$ (par exemple, $i^2=-1\neq 1$. Si les deux groupes étaient isomorphes, on aurait alors $i=\varphi(x,y)$ avec $(x,y)\in\mathbb{U}_2\times\mathbb{U}_2$ et donc $i^2=(\varphi(x,y))^2=\varphi((x,y)^2)=\varphi(1,1)=1$: absurde !

Exercice 19.

1) Soit $x\geq 0$. On a alors $x=(\sqrt{x})^2$. On a donc :

$$\varphi(x)=\varphi((\sqrt{x})^2)=(\varphi(\sqrt{x}))^2\geq 0.$$

Soient à présent $x,y\in\mathbb{R}$ avec $x\leq y$. Il existe donc $h\geq 0$ tel que $x+h=y$. On a alors :

$$\begin{aligned}\varphi(y) &= \varphi(x+h)\\ &= \varphi(x)+\varphi(h)\\ &\geq \varphi(x).\end{aligned}$$

Ceci entraine que φ est croissante.

2) On a $\varphi(0) = 0$ et $\varphi(1) = 1$. Par récurrence, on prouve que $\forall n \in \mathbb{N},\ \varphi(n) = \varphi(1 + 1 + \ldots + 1) = n\varphi(1) = n$. Puisque $\varphi(-n) = -\varphi(n)$, on a alors :

$$\forall n \in \mathbb{Z},\ \varphi(n) = n.$$

On a enfin pour $p \in \mathbb{Z}$ et $q \in \mathbb{N}^*$:

$$q\varphi\left(\frac{p}{q}\right) = \varphi\left(q \times \frac{p}{q}\right) = \varphi(p) = p.$$

On a donc $\varphi\left(\frac{p}{q}\right) = \frac{p}{q}$. On a donc $\forall x \in \mathbb{Q},\ \varphi(x) = x$.

3) Soit $x \in \mathbb{R}$. En posant pour $n \in \mathbb{N}^*$, $x_n = \lfloor x/n \rfloor$ et $y_n = \lfloor x/n \rfloor + 1/n$, on a que $x_n, y_n \in \mathbb{Q}$ et que $x_n \leq x \leq y$. On en déduit par croissance de φ et d'après la question précédente que :

$$\varphi(x_n) \leq \varphi(x) \leq \varphi(y_n) \Leftrightarrow x_n \leq \varphi(x) \leq y_n.$$

Puisque (x_n) et (y_n) tendent vers x, on en déduit par passage à la limite dans les inégalités que :

$$x \leq \varphi(x) \leq x.$$

On en déduit que $\forall x \in \mathbb{R},\ \varphi(x) = x$ soit que $\varphi = \mathrm{Id}_{\mathbb{R}}$.

Exercice 20. Soit $x \in A$. Par hypothèse, on a $(x+1)^2 = x+1$. Ceci entraine, après développement du carré (puisque $x+x = 2x$) que $x^2+2x+1 = x+1$. Or, on a $x^2 = x$. On a donc, après les différentes simplifications, que $2x = 0$.

Soient $x, y \in A$. On a $(x+y)^2 = x^2 + xy + yx + y^2$. Ceci entraine que $(x+y)^2 = x + xy + yx + y$. Or, on a également que $(x+y)^2 = x + y$. Après simplification, on en déduit que $xy + yx = 0$. On a donc $yx = -xy = (-x)y$. Or, puisque $2x = 0$, on a $x = -x$. On a donc $yx = xy$. La loi $\times$ est donc commutative.

Exercice 21. Soit A un anneau. Soit x est nilpotent. Il existe donc $n \in \mathbb{N}^*$ tel que $x^n = 0$. Notons n_0 le plus petit entier strictement positif vérifiant cette propriété (qui est l'indice de nilpotence de x). Un tel entier existe car on peut le définir comme le minimum de $\{n \in \mathbb{N}^* \ / \ x^n = 0\}$ qui est une partie de $\mathbb{N}^*$ non vide.

1) Supposons xy nilpotent d'indice n. On a alors en utilisant l'associativité $(yx)^{n+1} = y \times (xy)^n \times x = 0$. On a donc yx nilpotent.

2) Supposons x et y nilpotent qui commutent. Supposons $x^n = 0$ et $y^m = 0$. Alors, on peut utiliser la formule du binome (puisque x et y commutent). On a donc :

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

Or, tous les termes de cette somme sont nuls car soit $k \geq n$ et $x^k = 0$, soit $k < n$ et $y^{n+m-k} = 0$. On en déduit que $x + y$ est nilpotent.

De la même façon, $(xy)^n = x^n \times y^n = 0$ (puisque $x^n = 0$). On en déduit que xy est nilpotent.

3) Supposons par l'absurde x inversible d'inverse a. On a alors $a \times x = 1$. Multiplions cette égalité par x^{n_0-1} à droite. On obtient $a \times x \times x^{n_0-1} = x^{n_0-1}$, ce qui entraine que $0 = x^{n_0-1}$: absurde ! Ceci contredit la définition de l'indice de nilpotence. On en déduit que x n'est pas inversible.

On a par contre :

$$\begin{aligned}(1-x)\sum_{k=0}^{n_0-1} x^k &= \sum_{k=0}^{n_0-1}(x^k - x^{k+1}) \\ &= 1 - x^{n_0} \\ &= 1.\end{aligned}$$

On procède de même de l'autre côté, ce qui prouve que $1-x$ est inversible d'inverse $\sum_{k=0}^{n_0-1} x^k$ qui est bien un élément de A (car A est un anneau donc il est stable par sommes et multiplications).

Exercice 22. Soit $\mathbb{Z}[i] = \{a+ib,\ (a,b) \in \mathbb{Z}^2\}$.

1) Il est clair que les lois $+$ et $\times$ sont associatives et commutatives sur $\mathbb{Z}[i]$. $\mathbb{Z}[i]$ contient également 0 et 1. $(\mathbb{Z}[i], +)$ est un groupe (il est stable par addition et l'inverse de $a+bi$ est $-a-bi$). Il reste à montrer la stabilité pour la loi $\times$ pour avoir une structure d'anneau. Si $a, b, c, d \in \mathbb{Z}$, on a $(a+ib)(c+id) = (ac-bd) + i(ad+bc)$ et on a $ac - bd \in Z$ et $(ad-bc) \in \mathbb{Z}$. On a donc bien une structure d'anneau commutatif.

2) Raisonnons par analyse/synthèse. **Analyse :** Soit $z \in \mathbb{Z}[i]$ un élément inversible.

Il existe alors $z' \in \mathbb{Z}[i]$ tel que $zz' = 1$. On remarque alors, en considérant les modules que $|z||z'| = 1$. Un de ces deux éléments a donc un module inférieur ou égal à 1. Supposons par exemple que $z = a+ib$ soit de module inférieur ou égal à 1. On a donc $a^2 + b^2 \leq 1$ avec $a, b \in \mathbb{Z}$. On en déduit que a et b sont à valeurs dans $\{-1, 0, 1\}$ (car a et b sont des entiers relatifs). Ceci entraine que a et b ne peuvent également pas être égaux à 1 en même temps (on aurait alors un module égal à $\sqrt{2}$). On peut donc alors tester toutes les valeurs possibles :

— si $a = b = 0$, z n'est pas inversible.
— si $a = \pm 1$ et $b = 0$, on a $z = \pm 1$ qui est inversible d'inverse $z' = \pm 1$.
— si $a = 0$ et $b = \pm 1$, on a $z = \pm i$ qui est inversible d'inverse $z' = \pm i$.

Synthèse : on a testé toutes les possibilités. On a donc montré que les éléments inversibles de $\mathbb{Z}[i]$ sont $1, -1, i, -i$.

Exercice 23. Posons $\mathbb{Q}[\sqrt{2}] = \{a+b\sqrt{2},\ (a,b) \in \mathbb{Q}^2\}$. Montrons qu'il s'agit d'un sous-corps de $(\mathbb{R}, +, \times)$.

- $\mathbb{Q}[\sqrt{2}]$ est non vide (il contient 0, 1, etc.) et $\mathbb{Q}[\sqrt{2}] \subset \mathbb{R}$.

- $(\mathbb{Q}[\sqrt{2}], +)$ est un sous-groupe de $(\mathbb{R}, +)$. Il contient le neutre 0, il est bien stable par addition et par passage à l'opposé.

- Vérifions que $(\mathbb{Q}[\sqrt{2}] \setminus \{0\}, \times)$ est un sous-groupe de $(\mathbb{R}^*, \times)$. Il contient le neutre 1. Il est stable par produit : si $x, y \in \mathbb{Q}[\sqrt{2}]$, il existe $a, b, c, d \in \mathbb{Q}$ tels que $x = a+b\sqrt{2}$ et $y = c+d\sqrt{2}$. On a alors $xy = (ac+2bd) + (ad+bc)\sqrt{2}$ avec $ac+2bd \in \mathbb{Q}$ et $ad+bc \in \mathbb{Q}$. Il est également stable par passage à l'inverse. Si $x \in \mathbb{Q}[\sqrt{2}] \setminus \{0\}$, il existe $a, b \in \mathbb{Q}$ tels que $x = a+b\sqrt{2}$. On a alors $x \neq 0$ (sinon on aurait $\sqrt{2} \in \mathbb{Q}$: absurde !), ($a - b\sqrt{2} \neq 0$ pour la même raison) et :

$$\begin{aligned}\frac{1}{x} &= \frac{1}{a+b\sqrt{2}} \\ &= \frac{a-b\sqrt{2}}{a^2-2b^2} \\ &= \frac{a}{a^2-2b^2} + \frac{-b}{a^2-2b^2}\sqrt{2}.\end{aligned}$$

On a $\frac{a}{a^2-2b^2} \in \mathbb{Q}$ et $\frac{-b}{a^2-2b^2} \in \mathbb{Q}$. $\mathbb{Q}[\sqrt{2}] \setminus \{0\}$ est donc stable par passage à l'inverse. On a donc vérifié que $(\mathbb{Q}[\sqrt{2}] \setminus \{0\}, \times)$ est un sous-groupe de $(\mathbb{R}^*, \times)$.

On a donc montré que $(\mathbb{Q}[\sqrt{2}], +, \times)$ est un sous-corps de $\mathbb{R}$.

Exercice 24. Soit K un sous-corps de $(\mathbb{Q}, +, \times)$. On a donc $1 \in K$. Puisque K est un corps, c'est en particulier un anneau donc pour tout $n \in \mathbb{Z}$, $n \in K$. De plus, K^* est stable par passage à l'inverse donc en particulier, pour tout $n \in \mathbb{Z}^*$, $\dfrac{1}{n} \in K$. Toujours puisque K est un anneau, on a alors pour tout $p \in \mathbb{Z}$, $\dfrac{p}{n} \in K$. Puisque n est quelconque dans $\mathbb{Z}^*$, on en déduit que $\mathbb{Q} \subset K$. Puisque $K \subset \mathbb{Q}$ par définition d'un sous corps, on en déduit que $K = \mathbb{Q}$.