Feuille d'exercices n° 9 : corrigé

MPSI Lycée Camille Jullian

9 décembre 2024

Exercice 1 (**)

On vérifie toutes les propriétés nécessaires pour avoir une loi de groupe :

- la loi $\star$ est bien une lci car $x \neq 0$ et $x' \neq 0$ (par hypothèse sur l'ensemble sur lequel s'applique $\star$, donc $xx' \neq 0$, et $(xx', xy' + yx'^n) \in \mathbb{R}^* \times \mathbb{R}$.
- la loi $\star$ est associative : $((x,y)\star(x',y'))\star(x'',y'') = (xx', xy'+yx'^n)\star(x'',y'') = (xx'x'', xx'y''+xy'x''^n+yx'^nx''^n)$, et $(x,y)\star((x',y')\star(x'',y'')) = (x,y)\star(x'x'', x'y''+y'x''^n) = (xx'x'', xx'y''+xy'x''^n+yx'^nx''^n)$. Les deux résultats obtenus sont les mêmes, ce qui prouve l'associativité. Notons que la loi $\star$ n'est commutative que pour $n = 1$. ensuite, on aura par exemple $(1,1)\star(2,1) = (2, 1+2^n)$, mais $(2,1)\star(1,1) = (2,3)$.
- le couple $(1,0)$ sera élément neutre de la loi $\star$: $(1,0)\star(x,y) = (x,y)$ et $(x,y)\star(1,0) = (x,y)$.
- un couple (x,y) admet pour symétrique (x',y') si $(x,y)\star(x',y') = (1,0)$, donc si $xx' = 1$ et $xy'+yx'^n = 0$, soit $x' = \dfrac{1}{x}$ (toujours bien défini puisque $x \neq 0$ et $y' = -\dfrac{y}{x^{n+1}}$ (également bien défini). Vérifions que le symétrique est bien le même « dans l'autre sens » : $\left(\dfrac{1}{x}, -\dfrac{y}{x^{n-1}}\right)\star(x,y) = \left(1, \dfrac{y}{x} - \dfrac{y}{x^{n-1}} \times x^n\right) = (1,0)$. Tout couple est donc symétrisable pour la loi $\star$.

Exercice 2 (*)

1. La loi est manifestivement commutative (x et y jouent un rôle symétrique dans la définition). Pour l'associativité, calculons $(x\star y)\star z = (x+y+x^2y^2)\star z = x+y+x^2y^2+z+(x+y+x^2y^2)^2z^2 = x+y+z+x^2y^2+x^2z^2+y^2z^2+x^4y^4z^2+2xyz^2+2x^3y^2z^2+2x^2y^3z^2$. Cette expression n'a aucune raison de donner une opération associative (aucune symétrie entre les trois variables à l'arrivée), cherchons donc un contre-exemple : $(1\star1)\star2 = 3\star2 = 30$ et $1\star(1\star2) = 1\star7 = 57$. Effectivement, $\star$ n'est pas le moins du monde associative (et ne peut donc pas être une loi de groupe).
2. Oui, 0 est un élément neutre assez évident.
3. Par définition, $1\star x = 0$ signifie que $1+x+x^2 = 0$, équation qui n'a aucune solution réelle. Même principe pour l'équation $1\star x = 1$ qui se ramène à $x+x^2 = 0$ et admet donc deux solutions : l'élément neutre $x = 0$ (normal) mais aussi l'élément $x = -1$ (ce qui prouve que, pour la loi $\star$ on ne peut pas « simplifier » une égalité du type $1\star x = 1$ par 1).

Exercice 3 (*)

1. Le reste d'une division par 5 étant toujours un entier naturel strictement inférieur à 5, le seul risque serait que ce reste soit égal à 0. Or, si $x \in E$, x ne peut avoir pour facteurs dans sa décomposition en facteurs premiers que des 2 et des 3 (ou même aucun facteur premier si $x = 1$), et ce sera également le cas pour x^y, que que soit l'entier $y \geqslant 1$. En particulier, x^y ne contiendra jamais de facteur 5 et ne sera donc jamais divisible par 5, ce qui prouve que le reste de sa division par 5 ne peut pas être nul. La loi $\star$ est donc bien une lci. On remplit le tyableau de loi « à la main » en calculant toutes les puissances, par exemple $2^3 = 8 \equiv 3[5]$,

donc $2\star 3 = 3$, ou $4^2 = 16 \equiv 1[5]$ donc $4\star 2 = 1$. Dans le tableau qui suit, l'opérande de gauche est indiqué en ligne et celui de droite en colonne, comme d'habitude (la loi n'est clairement pas commutative) :

$\star$	1	2	3	4
1	1	1	1	1
2	2	4	3	1
3	3	4	2	1
4	4	1	4	1

2. Ce n'est pas du tout une loi de groupe, elle ne vérifie pas la « règle du Sudoku » et on peut trouver par exemple des contre-exemples à l'existence de l'élément neutre ou à l'associativité ($(2\star 1)\star 3 = 3$ mais $2\star(1\star 3) = 2$).
3. Le seul élément a pour lequel $a\star 2 = 1$ est $a = 1$, on est donc ramenés à la résolution de l'équation $3\star x = 1$, qui donne comme unique solution $x = 4$ (à chaque fois, on lit simplement dans le tableau).

   La deuxième équation ne peut avoir de solutions puisque $4\star a$ est toujours égal à 1 ou 4, jamais à 2.

   Enfin, pour la dernière, on doit nécessairement avoir $3\star x = 2$, donc l'unique solution est $x = 3$.

Exercice 4(*)

1. Le plus simple est de faire le tableau complet de la loi de groupe même si c'estun peu laborieux, en calculant toutes les composées, par exemple $f_5 \circ f_3(x) = \dfrac{\frac{x-1}{x}}{\frac{x-1}{x} - 1} = \dfrac{x-1}{-1} = 1 - x = f_6(x)$. On constate ainsi que la loi $\circ$ est interne sur G, l'associativité est évidente (la composition est toujours associative), le neutre est bien présent dans G (c'est f_1) et tout élément de G admet une réciproque appartenant à G, donc c'est un groupe. Il n'est pas abélien, par exemple $f_3 \circ f_5 = f_4 \neq f_5 \circ f_3$.

$\circ$	f_1	f_2	f_3	f_4	f_5	f_6
f_1	f_1	f_2	f_3	f_4	f_5	f_6
f_2	f_2	f_3	f_1	f_5	f_6	f_4
f_3	f_3	f_1	f_2	f_6	f_4	f_5
f_4	f_4	f_6	f_5	f_1	f_3	f_2
f_5	f_5	f_4	f_6	f_2	f_1	f_3
f_6	f_6	f_5	f_4	f_3	f_2	f_1

2. Un sous-groupe à deux éléments contient nécessairement le neutre f_1, et un deuxième élément qui est sa propre réciproque (pour avoir la stabilité par symétrisation). Réciproquement, un sous-ensemble constitué de deux tels éléments sera un sous-groupe. On a donc trois sous-groupes à deux éléments : $\{f_1, f_4\}$, $\{f_1, f_5\}$ et $\{f_1, f_6\}$.
3. Oui, H_1 est un sous-groupe, les stabilités sont évidentes à partir du tableau de la loi de groupe. Par contre, H_2 n'en est pas du tout un, par exemple $f_2 \circ f_2 = f_3 \notin H_2$.

Exercice 5 (*)

Les deux opérations Δ et $\cap$ sont certainement des lci. De plus, on a prouvé en début d'année que l'opération Δ était associative, commutative et distributive par rapport à l'intersection, preuves que je vais donc me dispenser de refaire ici ! L'intersection est elle-même associative et commutative.

Il reste donc à vérifier la présence des deux éléments neutres et la symétrisabilité pour la différence symétrique. Le neutre pour l'intersection est E tout entier, le neutre pour l'opération Δ est $\emptyset$: $A\Delta\emptyset = (A \cup \emptyset)\backslash(A \cap \emptyset) = A\backslash\emptyset = A$. Enfin, tout élément de $\mathcal{P}(E)$ admet un symétrique pour l'opération Δ qui est tout simplement lui-même : $A\Delta A = (A \cup A)\backslash(A \cap A) = A\backslash A = \emptyset$. On est bien en présence d'un anneau commutatif. Les unités de cet anneau sont les sous-ensembles de E admettant un symétrique pour l'opération d'intersection, c'est-à-dire uniquement l'ensemble E lui-même (A admet un symétrique pour $\cap$ si et seulement s'il existe $B \subset E$ tel que $A \cap B = E$, ce qui implique immédiatement $A = B = E$).

Exercice 6 (*)

On va en fait montrer que $\mathbb{Q}[\sqrt{3}]$ est un sous-corps de $\mathbb{R}$. Pour cela, on doit vérifier les propriétés suivantes :

- $\mathbb{Q}[\sqrt{3}]$ est un sous-groupe additif de $\mathbb{R}$. En effet, il contient l'élément neutre 0 (il suffit de prendre $a = b = 0$, est stable par somme : $(a + b\sqrt{3}) + (c + d\sqrt{3}) = (a + c) + (b + d)\sqrt{3}$, avec $a + b$ et $c + d$ rationnels comme somme de rationnels. Et il est stable par passage à l'opposé de façon évidente.
- $\mathbb{Q}[\sqrt{3}]$ est un sous-anneau de $\mathbb{R}$. En plus de ce qui précède, on vérifie que notre sous-ensemble contient le neutre multiplicatif 1 (c'est le cas en posant $a = 1$ et $b = 0$), et qu'il est stable par produit : $(a + b\sqrt{3})(c + d\sqrt{3}) = ac + ad\sqrt{3} + bc\sqrt{3} + 3bd = (ac + 3bd) + (ad + bc)\sqrt{3}$. Les deux coefficients $ac + 3bd$ et $ad + bc$ étant bien rationels, notre ensemble est stable par multiplication, c'est bien un sous-anneau de $\mathbb{R}$.
- Enfin, pour avoir un sous-corps, il faut que notre ensemble (privé de 0) soit stable par passage à l'inverse. Il suffit pour le prouver d'avoir en tête le produit par la quantité conjuguée : $\dfrac{1}{a + b\sqrt{3}} = \dfrac{a - b\sqrt{3}}{a^2 - 3b^2} = \dfrac{a}{a^2 - 3b^2} - \dfrac{b}{a^2 - 3b^2}\sqrt{3}$, qui appartient bien à notre ensemble (le dénominateur $a^2 - 3b^2$ ne peut pas s'annuler car $\sqrt{3}$ est un nombre irrationnel). On a bien prouvé qu'il s'agit d'un sous-corps de $\mathbb{R}$.

Exercice 7 (**)

1. Vérifions que τ_a est un morphisme de groupes multiplicatifs : si $(x, y) \in G^2$, alors $\tau_a(x)\tau_a(y) = axa^{-1}aya^{-1} = axeya^{-1} = axya^{-1} = \tau_a(xy)$. De plus, τ_a est à valeurs dans G, ce qui prouve que τ_a est un endomorphisme. Enfin, τ_a a une réciproque assez évidente qui est $\tau_{a^{-1}}$ puisque $\tau_{a^{-1}}(\tau_a(x)) = a^{-1}(axa^{-1})a = exe = x$ et $\tau_a(\tau_{a^{-1}}(x)) = a(a^{-1}ax)a^{-1} = exe = e$. Ce calcul n'est d'ailleurs qu'un cas particulier de celui qu'on va faire à la question suivante.
2. Calculons : $\tau_a(\tau_b(x)) = a(bxb^{-1})a^{-1} = (ab)x(ab)^{-1} = \tau_{ab}(x)$, donc $\tau_a \circ \tau_b = \tau_{ab}$. De façon évidente, $\tau_e = \mathrm{id}_G$.
3. On a déjà prouvé que l'application (appelons là φ) était à valeurs dans $\mathrm{Aut}(G)$, mais aussi qu'il s'agissait d'un morphisme (c'est le calcul de la question précédente). Reste donc à déterminer son noyau : $\varphi_(a) = \mathrm{id}_G \Leftrightarrow \tau_a = \mathrm{id}_G$. Autrement dit, on doit avoir, $\forall x \in G$, $axa^{-1} = x$, ce qu'on peut écrire sous la forme $ax = xa$. L'élément a doit donc commuter avec tous les autres éléments du groupe G. On appelle l'ensemble de ces éléments centre du groupe G, et on le note habituellement $Z(G)$.

Exercice 8 (***)

1. Dans un groupe additif, un élément est d'ordre fini s'il vérifie $x + x + \cdots + x = nx = 0$, ce qui n'est le cas dans $\mathbb{R}$ que de 0 lui-même (dont on peut dire qu'il est d'ordre 1, c'est d'ailleurs le seul élément vérifiant cette propriété). Dans $\mathbb{C}^*$, un élément z est d'ordre fini s'il existe un entier n tel que $z^n = 1$, autrement dit si z est une racine n-ème de l'unité pour un certain entier n. On peut écrire cet ensemble sous la forme $\bigcup_{n\in\mathbb{N}^*} \mathbb{U}_n$.

2. L'ensemble H contient l'élément neutre multiplicatif 1 puisque $x^0 = 1$. De plus, si on considère deux éléments de H de la forme x^k et x^l, alors leur produit x^{k+l} peut toujours être ramené à une puissance de x strictement inférieure à n en utilisant le fait que $x^n = 1$: soit $k+l < n$ et il n'y a rien à faire, soit $x^{k+l} = x^n \times x^{k+l-n} = x^{k+l-n}$, avec $k+l-n < n$. L'ensemble H est donc stable par multiplication. Il l'est également par passage à l'inverse puisque $(x^k)^{-1} = x^{n-k}$ (en effet, par hypothèse, $x^k x^{n-k} = x^n = 1$). La seule valeur de k pour laquelle x^{n-k} pourrait ne pas appartenir à H est $k = 0$, mais dans ce cas $x^0 = 1$ est son propre inverse. Finalement, H est bien un sous-groupe multiplicatif de G.
3. De façon assez évidente, $(x^{-1})^k = (x^k)^{-1}$. On peut le prouver rigoureusement en faisant une petite récurrence : c'est vrai de façon évidente au rang 1, et en le supposant au rang k, alors $(x^{-1})^{k+1}x^{k+1} = x^{-1}(x^{-1})^k x^k x = x^{-1}x = 1$, ce qui prouve l'hérédité (le produit dans l'autre sens se simplifie de la même façon). En particulier, on a donc $(x^{-1}) = x^n = 1$, ce qui prouve que x^{-1} est aussi d'ordre fini. Il ne peut pas avoir un ordre strictement plus petit que x, car $x^{-k} = 1 \Rightarrow x^k = 1$ d'après ce qui précède, donc les deux éléments ont bien le même ordre.
4. On peut en fait simplifier l'écriture de $(yxy^{-1})^k$ en $yx^k y^{-1}$ (là encore c'est une récurrence facile si on veut être rigoureux, c'est évident au rang 1, et une fois supposé au rang k, on écrit $(yxy^{-1})^{k+1} = (yxy^{-1})(yxy^{-1})^k = yxy^{-1}yx^k y^{-1} = yx^{k+1}y^{-1}$ en simplifiant « par le milieu »). On en déduit notamment que $(yxy^{-1})^n = yx^n y^{-1} = yy^{-1} = 1$, ce qui prouve que yxy^{-1} est d'ordre fini. Encore une fois, l'ordre ne peut pas être plus petit, car en supposant $(yxy^{-1})^k = 1$, on aurait $yx^k y^{-1} = 1$, donc $yx^k = y$ puis $x^k = 1$, ce qui est exclu si $k < n$.
5. Supposons donc $(xy)^n = xyxyxy \dots xy = 1$, et notons $z = (yx)^n = yxyx \dots yx$, alors $xz = (xy)^n x = x$, ce qu'on a le droit de simplifier par x pour obtenir $z = 1$, donc yx est d'ordre fini. De plus l'ordre de yx est nécessairement inférieur ou égal à celui de xy. Mais l'argument étant bien sûr symétrique, l'ordre de xy doit lui-même être inférieur ou égal à celui de yx, ce qui prouve que les ordres des deux éléments sont nécessairement égaux.

Exercice 9 (**)

1. C'est assez évident : si l'élément neutre appartient à chacun des sous-groupes, il appartiendra aussi à leur intersection. Supposons désormais que x et y soient deux éléments appartenant à chacun des sous-groupes de l'intersection, alors $x \star y^{-1}$ (en notant la loi $\star$ et le symétrique comme un inverse) appartient aussi à chacun de ces sous-groupes (puisque ces sous-groupes sont stables par $\star$ et par passage au symétrique), donc appartient également à leur intersection, qui est donc un sous-groupe de G.
2. Notons C_x le centralisateur de x. L'élément neutre commutant avec tous les éléments de G, il commute en particulier avec x et appartient donc à C_x. Supposons maintenant que deux éléments x et y appartient à C_x. On a donc $y \star x = x \star y$ (on garde les notations de la première question) et $z \star x = x \star z$. En composant cette deuxième égalité par z^{-1} à droite, on en déduit $z \star x \star z^{-1} = x \star z \star z^{-1} = x$, puis en composant à gauche par ce même z^{-1}, $z^{-1} \star z \star x \star z^{-1} = z^{-1} \star x$, soit $x \star z^{-1} = z^{-1} \star x$ (ce qui prouve au passage la stabilité de C_x par symétrisation). On peut maintenant écrire $x \star y \star z^{-1} = y \star x \star z^{-1} = y \star z^{-1} \star x$, ce qui prouve que $y \star z^{-1} \in C_x$, et donc que C_x est bien un sous-groupe de G.
3. Notons $Z(G)$ le centre de G (notation traditionnelle pour cet ensemble). Absolument aucune vérification à faire dans cette question, on peut tout bêtement utiliser les deux précédentes : $Z(G) = \bigcap_{x \in G} C_x$ est un sous-groupe de G en tant qu'intersection de sous-groupes de G (un élément qui appartient à tous les centralisateurs est par définition un élément qui commute avec tout le monde).

Exercice 10 (***)

1. Vérifions les trois propriétés :

- la relation est réflexive car $\forall x \in G$, $x = x \star e$, où l'élément neutre e appartient nécessairement au sous-groupe H.
- si $x\mathcal{R}y$, il existe un élément $z \in H$ tel que $y = x \star z$, mais cela implique $y \star z^{-1} = x$, où z^{-1} est le symétrique de z, qui appartient aussi à H (c'est un sous-groupe, il est stable par symétrisation). La relation est donc symétrique.
- si $x\mathcal{R}y$ et $y\mathcal{R}w$, il existe deux éléments z et z' de H tels que $y = x \star z$ et $w = y \star z'$. Mais alors $x = (x \star z) \star z' = x \star (z \star z')$, avec $z \star z' \in H$ puisqu'un sous-groupe est stable par $\star$. Ceci prouve la transitivité de la relation.

La classe d'équivalence de x est simplement l'ensemble (souvent noté $x \star H$ des éléments $x \star z$ lorsque z parcourt H. Tous ces éléments sont nécessairement distincts car, dans un groupe, $x \star z = x \star z' \Rightarrow z = z'$.

2. D'après ce qu'on a dit à la question précédente, toute classe d'équivalence contient autant d'éléments que le sous-groupe H. D'ailleurs, H lui-même correspond à la classe d'équivalence de l'élément neutre e.
3. On sait que G est l'union disjointe des classes d'équivalence, qui contiennent chacune $|H|$ éléments (on note ici $|H|$ le nombre d'éléments de l'ensemble fini H). En notant k le nombre de classes d'équivalence, on a donc $|G| = k|H|$, et le nombre d'éléments de G est donc multiple de celui de H.
4. Puisqu'un nombre premier n'a pour diviseurs que 1 et lui-même, les sous-groupes ne peuvent contenir qu'un seul élément (forcément égal à l'élément neutre), ou tous les éléments. Il n'y a donc que les deux sous-groupes triviaux : $\{e\}$ et G tout entier.

Exercice 11 (**)

1. Effectuons toutes les vérifications d'usage :
   - A contient le neutre additif 0 (il suffit de poser $p = 0$) et il est stable par soustraction : si $x = \dfrac{p}{2^n}$ et $y = \dfrac{q}{2^m}$ alors $x - y = \dfrac{2^m p - 2^n q}{2^{n+m}}$, avec $n + m \in \mathbb{N}$ et $2^m p - 2^n q \in \mathbb{Z}$ (même pas besoin de s'embêter à se demander si la fraction se simplifie), donc A est un sous-groupe additif de $\mathbb{Q}$.
   - A contient le neutre multiplicatif 1 (on pose par exemple $p = 1$ et $n = 0$, mais il existe plein d'autres possibilités tout aussi valables !).
   - A est stable par produit : $\dfrac{p}{2^n} \times \dfrac{q}{2^m} = \dfrac{pq}{2^{n+m}}$, c'est complètement évident.
2. On doit donc chercher les éléments de A inversibles **dans** A, autrement dit les éléments de la forme $\dfrac{p}{2^n}$ dont l'inverse $\dfrac{2^n}{p}$ a lui aussi un dénominateur qui est une puissance de 2. Quitte à supposer la fraction réduite, cela signifie que p est lui-même de la forme $\pm 2^k$, avec $k \in \mathbb{N}$ (sa décomposition en facteurs premiers ne peut pas contenir d'autre facteur premier que 2). Autrement dit, les seules unités dans A sont les nombres de la forme $x = \pm 2^k$, avec $k \in \mathbb{Z}$.
3. L'ensemble des décimaux peut être défini par $D = \left\{ \dfrac{p}{10^n} \mid (p, n) \in \mathbb{Z} \times \mathbb{N} \right\}$. La vérification du faut que D est un sous-anneau de $\mathbb{Q}$ est alors rigoureusement la même que pour l'ensemble A, ça n'a aucun intérêt de tout refaire. Les éléments inversibles de D sont alors ceux qui ont un numérateur (après simplification) de la forme $\pm 2^k 5^l$ (cette fois-ci le dénominateur 10^n a deux facteurs premiers qui sont 2 et 5), ce qui donne finalement comme éléments inversibles tous les éléments de la forme $x = \pm 2^k 5^l$, avec $(k, l) \in \mathbb{Z}^2$.

Exercice 12 (***)

1. Si x est un élément nilpotent non nul, on peut écrire $x \times x^{n-1} = 0$, avec $x^{n-1} \neq 0$ quitte à choisir le plus petit entier n pour lequel $x^n = 0$ (cet entier est d'ailleurs appelé indice de

nilpotence de l'élément x). On a alors un produit de deux éléments non nuls qui égal à 0, ce qui prouve que A n'est pas intègre. Par contraposée, si A est intègre, 0 est le seul élément nilpotent.

2. Commençons par le produit : si x et y commutent, on peut écrire, $\forall k \geqslant 1$, $(xy)^k = x^k y^k$. En prenant $k = n$, où n est l'indice de nilpotence de x, on a alors $(xy)^n = 0y^n = 0$, ce qui prouve la nilpotence de xy (l'indice de nilpotence de xy sera logiquement le plus petit parmi ceux de x et de y).

   Pour la somme, on fait appel à notre ami Newton : notons n l'indice de nilpotence de x et m celui de y, alors $(x+y)^{n+m} = \sum_{k=0}^{n+m} \binom{n}{k} x^k y^{n+m-k}$. Dans cette somme, tous les termes à partir de l'indice n sont nuls car on a alors $x^k = x^n \times x^{k-n} = 0$ puisque $x^n = 0$. Mais tous ceux qui précédent sont nuls car si $k < n$, $n + m - k > m$, donc $y^{n+m-k} = 0$. Finalement, on est en train de calculer une somme de termes nuls, donc $(x+y)^{n+m} = 0$, ce qui prouve la nilpotence de $x + y$ (les plus attentifs auront remarqué qu'on pouvait en fait se contenter de $(x+y)^{n+m-1}$ pour obtenir une valeur nulle, $n + m - 1$ est en général l'indice de nilpotence de $x + y$).

3. Il faut penser à exploiter la factorisation de $a^n - b^n$ évoquée en cours. Ici, on l'applique pour $a = 1$ et $b = x$ (éléments qui commutent toujours puisque le neutre 1 commute avec tout le monde) : $1 - x^n = (1-x)\sum_{k=0}^{n-1} x^k$. Or, $x^n = 0$, donc en posant $y = \sum_{k=0}^{n-1} x^k$, on a plus simplement $(1-x)y = 1$ (et similairement $y(1-x) = 1$, ce qui prouve que $1 - x$ est bien inversible, et que son inverse est y.

Exercice 13 (**)

1. On peut par exemple appliquer l'hypothèse à l'opposé de x : $(-x)^2 = -x$, donc $x^2 = -x$. Mais comme par ailleurs $x^2 = x$, on a donc $-x = x$, ce qui implique bien $2x = 0$. Autrement possibilité : on applique l'hypothèse à l'élément $x+1$: $(x+1)^2 = x+1$, donc $x^2+2x+1 = x+1$, ce qui donne bien $2x = 0$ puisque $x^2 = x$.
2. Soient $x, y \in A^2$, alors $(x+y)^2 = x+y$, donc $x^2+y^2+xy+yx = x+y$. Or $x^2 = x$ et $y^2 = y$, ce qui permet de simplifier l'égalité en $xy+yx = 0$, donc $xy = -yx$. Or, comme tout élément de A, yx vérifie $-yx = yx$, donc on a bien $xy = yx$ et les deux éléments commutent toujours.
3. Développons : $xy(x+y) = xyx+xy^2 = x^2y+xy^2$ puisque x et y commutent. Mais ces carrés ne servent à rien, donc $xy(x+y) = xy+xy = 2xy = 0$.
4. Supposons que A contienne un élément x différent de 0 et de 1. En appliquant la question précédente, $1 \times x(1+x) = 0$, donc $x(1+x) = 0$. Or, $x \neq 0$ par hypothèse, et $1 + x$ ne peut pas être nul sinon on aurait $x = -1 = 1$, ce qui est aussi exclu. Un produit de deux éléments non nuls est donc nul, l'anneau n'est pas intègre.

Exercice 14 (***)

1. Les vérifications ne sont pas très difficiles : $\mathbb{Z}[\alpha]$ contient tous les entiers relatifs (en posant $q = 0$) donc a fortiori les deux éléments neutres 0 et 1. La stabilité par somme ou par soustraction est évidente : $p + \alpha q + p' + \alpha q' = (p+p') + \alpha(q+q') \in \mathbb{Z}[\alpha]$, donc $\mathbb{Z}[\alpha]$ est un sous-groupe additif de $\mathbb{C}$. Il ne reste plus pour avoir un sous-anneau qu'à vérifier la stabilité par produit : $(p+\alpha q)(p'+\alpha q') = pp' + \alpha(pq'+p'q) + \alpha^2 qq'$. Or, par hypothèse, α est solution de l'équation $z^2 + z + 2 = 0$, donc $\alpha^2 = -\alpha - 2$, ce qui permet d'écrire $(p+\alpha q)(p'+\alpha q') = (pp' - 2qq') + \alpha(pq' + p'q - qq') \in \mathbb{Z}[\alpha]$ (les coefficients étant tous entiers), donc $\mathbb{Z}[\alpha]$ est aussi stable par produit, c'est un sous-anneau de $\mathbb{C}$.

2. Notre équation étant à coefficients réels, ses racines sont conjuguées, donc $\alpha+\overline{\alpha}$ est la somme des racines de z^2+z+2, soit $\alpha+\overline{\alpha}=-1$ et de même $\alpha\overline{\alpha}=2$.
3. D'après la question précédente, $\overline{\alpha}=-1-\alpha$, donc $\overline{p+\alpha q}=p+\overline{\alpha}q=p-q-\alpha q\in\mathbb{Z}[\alpha]$.
4. En effet, $(p+\alpha q)(p+\overline{\alpha}q)=p^2+pq(\alpha+\overline{\alpha})+pq\alpha\overline{\alpha}=p^2-pq+2q^2$. Cette valeur est clairement entière, et tout aussi clairement positive si p et q sont de signe opposé. Dans le cas contraire, $p^2-pq+2q^2\geqslant p^2-2pq+q^2=(p-q)^2\geqslant 0$, donc notre entier est toujours un entier naturel.
5. Sauf dans le cas où $z=0$, z sera toujours inversible dans $\mathbb{C}$, d'inverse $\dfrac{\overline{z}}{z\overline{z}}=\dfrac{p-q}{p^2-pq+2q^2}-\dfrac{q}{p^2-pq+2q^2}\alpha$. Pour que cet inverse appartienne à $\mathbb{Z}[\alpha]$, on doit avoir $\dfrac{p-q}{p^2-pq+2q^2}\in\mathbb{Z}$ et $\dfrac{q}{p^2-2pq+2q^2}\in\mathbb{Z}$. C'est évidemment le cas si lé dénominateur est égal à 1. Sinon, par différence, on doit aussi avoir $\dfrac{p}{p^2-2pq+2q^2}\in\mathbb{Z}$. Or, si p et q sont de signe opposé, $p^2-2pq+2q^2$ est très supérieur à p ou à q, donc la fraction ne peut sûrement pas se simplifier. S'ils sont de même signe (positif, sinon on change tous les signes), avec par exemple $p\leqslant q$, $p^2+2q^2-pq\geqslant p^2+2q^2-q^2\geqslant q^2+p^2$ qui est à nouveau largement supérieur à p et q. Il est donc impossible d'obtenir des coefficients entiers quand $p^2+2q^2-pq\neq 1$.
6. C'est évident puisque dans ce cas p^2+2q^2-pq est une somme de trois entiers strictement positifs, donc sûrement pas égal à 1.
7. On a déjà fait le calcul plus haut : dans ce cas, $p^2+2q^2-pq\geqslant p^2+q^2$, donc ne peut pas non plus être égal à 1.
8. Les seuls candidats possibles sont ceux pour lesquels $p=0$ ou $q=0$. Si $p=0$, z est un entier relatif, et $p^2+2q^2-pq=1$ seulement si $z=\pm 1$. Si $p=0$, on doit cette fois avoir $2q^2=1$, ce qui est évidemment impossible avec q entier relatif. Les seules unités de $\mathbb{Z}[\alpha]$ sont donc 1 et -1.