Corrigé 4

1 octobre

A cette série, vous pouvez rendre pour correction l'exercice 5. Il faut le donner à un des assistants de votre salle d'exercices au plus tard lors de la séance d'exercices du 8 octobre.

Exercice 1. *Soit $z \in \mathbb{C}$, $z = x + y\mathrm{i}$, pour $x, y \in \mathbb{R}$. On définit le conjugué complexe de z, noté $\bar{z}$, comme suit : $\bar{z} = x - y\mathrm{i}$. Montrer que l'application $f : \mathbb{C} \to \mathbb{C}$ donnée par $f(z) = \bar{z}$ est un homomorphisme d'anneaux.*

Solution 1. On prend $z_1 = x_1 + y_1\mathrm{i}$ et $z_2 = x_2 + y_2\mathrm{i}$, pour $x_i, y_i \in \mathbb{R}$, $i = 1, 2$. On a

$$\overline{(x_1 + y_2\mathrm{i}) + (x_2 + y_2\mathrm{i})} = \overline{(x_1 + x_2) + (y_1 + y_2)\mathrm{i}} = (x_1 + x_2) - (y_1 + y_2)\mathrm{i} = x_1 - y_1\mathrm{i} + x_2 - y_2\mathrm{i} = \overline{x_1 + y_1\mathrm{i}} + \overline{x_2 + y_2\mathrm{i}},$$

ce qui montre que $f(z_1 + z_2) = f(z_1) + f(z_2)$. On a aussi

$$\overline{(x_1 + y_1\mathrm{i})(x_2 + y_2\mathrm{i})} = \overline{(x_1x_2 - y_1y_2) + (x_1y_2 + x_2y_1)\mathrm{i}} = (x_1x_2 - y_1y_2) - (x_1y_2 + x_2y_1)\mathrm{i}.$$

Et

$$\overline{x_1 + y_1\mathrm{i}} \cdot \overline{x_2 + y_2\mathrm{i}} = (x_1 - y_1\mathrm{i})(x_2 - y_2\mathrm{i}) = x_1x_2 - y_1y_2 - (x_1y_2 + y_1x_2)\mathrm{i},$$

d'où $f(z_1z_2) = f(z_1)f(z_2)$.

Enfin on vérifie que $\bar{1} = 1$. Ces trois calculs démontrent que la conjugaison complexe est un morphisme d'anneaux unitaires.

Exercice 2. *Soit $z \in \mathbb{C}$, $z = x + y\mathrm{i}$, pour $x, y \in \mathbb{R}$. On définit le module de z, un nombre réel, noté $|z|$ par $|z| = \sqrt{x^2 + y^2} \in \mathbb{R}$. Vérifier les propriétés suivantes :*

(a) $z\overline{z} = |z|^2$

(b) Pour $z \neq 0$, *on a* $z^{-1} = \frac{\overline{z}}{|z|^2}$.

(c) Pour $z \neq 0$, *on a* $\overline{z^{-1}} = \overline{z}^{-1}$.

(d) $|z_1 \cdot z_2| = |z_1| \cdot |z_2|$

Solution 2. (a) $z\overline{z} = (x + \mathrm{i}y)(x - \mathrm{i}y) = x^2 + y^2 + \mathrm{i}(xy - yx) = x^2 + y^2 = |z|^2$.
(b) découle de (a) et (c) découle de (b).
(d). En utilisant l'exercice précédent et la commutativité de la multiplication complexe, on obtient

$$|z_1 \cdot z_2|^2 = z_1 \cdot z_2 \cdot \overline{z_1 \cdot z_2} = z_1 \cdot z_2 \cdot \overline{z_1} \cdot \overline{z_2} = z_1 \cdot \overline{z_1} \cdot z_2 \cdot \overline{z_2} = |z_1|^2 \cdot |z_2|^2.$$

Exercice 3. *Utiliser l'exercice 1. pour montrer que si $z \in \mathbb{C}$ est une racine du polynôme $p(x) \in \mathbb{R}[x]$ alors $\bar{z}$ est aussi une racine de p.*

Solution 3. On a $p(x) = a_0 + a_1x + \cdots + a_mx^m$ pour certains $a_i \in \mathbb{R}$. Par l'hypothèse on a que $p(z) = 0 = a_0 + a_1z + \cdots + a_mz^m$.

On utilise la conjugaison complexe, qui est un morphisme d'anneaux

$$0 = \overline{p(z)} = \overline{a_1 + a_1z + \cdots + a_mz^m} = \overline{a_0} + \overline{a_1z} + \cdots + \overline{a_mz^m} =$$

$$\overline{a_0} + \overline{a_1} \cdot \overline{z} + \cdots + \overline{a_m} \cdot \overline{z^m} = a_0 + a_1 \cdot \overline{z} + \cdots + a_m \cdot (\overline{z})^m.$$

L'égalité $0 = a_0 + a_1 \cdot \overline{z} + \cdots + a_m \cdot (\overline{z})^m$ montre que $\bar{z}$ est une racine de p.

Exercice 4. *Soit z une variable. Résoudre dans $\mathbb{C}$ l'équation suivante:*

$$\frac{z-3i}{2z+1} = \frac{4+3i}{2-i}$$

Solution 4. On calcule

$$\begin{aligned} \frac{z-3i}{2z+1} = \frac{4+3i}{2-i} &\iff (z-3i)(2-i) = (2z+1)(4+3i) \\ &\iff z(2-i) - 6i - 3 = z(8+6i) + 4 + 3i \\ &\iff z(-6-7i) = 7+9i \\ &\iff z = -\frac{7+9i}{6+7i} = -\frac{(7+9i)(6-7i)}{(6+7i)(6-7i)} = -\frac{105+5i}{85} = -\frac{21+i}{17}\ . \end{aligned}$$

Exercice 5. *(a) Soit $\phi : \mathbb{R}[t] \to \mathbb{C}$ l'application d'évaluation en* i*, c'est-à-dire que pour tout $p \in \mathbb{R}[t]$, $\phi(p) = p(\mathrm{i})$. On admet que ϕ est un morphisme d'anneaux et en particulier un morphisme de groupes de $(\mathbb{R}[t], +)$ dans $(\mathbb{C}, +)$. (C'est un bon exercice de vérifier que ϕ est un morphisme d'anneaux.) Trouver le sous-groupe* $\ker(\phi)$

(b) Soit $e_{\mathrm{i}} : \mathbb{C}[t] \to \mathbb{C}$ l'application d'évaluation en i. *Trouver* $\ker(e_{\mathrm{i}})$.

Solution 5. (a) On rappelle que $\ker(\phi) = \{p \in \mathbb{R}[t] \mid \phi(p) = 0\} = \{p \in \mathbb{R}[t] \mid p(\mathrm{i}) = 0\}$. Soit $p \in \ker(\phi)$. Par le cours, il existe $g \in \mathbb{C}[t]$ tel que $p = (t - \mathrm{i})g$. Par l'exercice 3, on a aussi que $p(-\mathrm{i}) = 0$ et donc $(-\mathrm{i} - \mathrm{i})g(-\mathrm{i}) = 0$ et on déduit que $g(-\mathrm{i}) = 0$. De nouveau par le cours, il existe $q \in \mathbb{C}[t]$ tel que $g = (t + \mathrm{i})q$, et en mettant ces résultats ensemble on obtient que $p = (t-\mathrm{i})(t+\mathrm{i})q = (t^2+1)q$. On déduit que $q \in \mathbb{R}[t]$. Donc $\ker(\phi) \subset \{q(t^2+1) \mid q \in \mathbb{R}[t]\}$. Il est aussi clair que $\{q(t^2+1) \mid q \in \mathbb{R}[t]\} \subset \ker(\phi)$, ce qui montre que

$$\ker(\phi) = \{q(t^2+1) \mid q \in \mathbb{R}[t]\} = \{(a_0 + a_1 t + \cdots + a_m t^m)(t^2+1) \mid m \in \mathbb{N}, a_i \in \mathbb{R}\}$$

$$= \{a_0 + a_1 t + (a_0 + a_2)t^2 + (a_1 + a_3)t^3 + \cdots + (a_{m-2} + a_m)t^m + a_{m-1}t^{m+1} + a_m t^{m+2} \mid m \in \mathbb{N}, a_i \in \mathbb{R}\}.$$

(b) On raisonne comme dans la partie précédente : si $p \in \ker(e_{\mathrm{i}})$ on a $p = (t - \mathrm{i})g$ pour un certain $g \in \mathbb{C}[t]$. On conclut que $\ker(e_{\mathrm{i}}) = \{(t - \mathrm{i})g \mid g \in \mathbb{C}[t]\}$.

Addendeum : Vérification que l'application d'évaluation est un morphisme d'anneaux.

Soient $(A, +, \cdot)$ un anneau unitaire avec $K \subset A$ tel que $(K, +, \cdot)$ est un corps et 1_A est l'élément neutre pour la multiplication dans K. Pour $c \in A$ on a une application, dite "d'évaluation en c", $e_c : K[t] \to A$ définie par $e_c(b_1 + b_1 t + \cdots + b_m t^m) = b_0 + b_1 c + \cdots + b_m c^m$. On vérifie que e_c est un morphisme d'anneaux.

Soit $p = a_0 + a_1 t + \cdots + a_m t^m, q = b_0 + b_1 t + \cdots + b_n t^n \in \mathbb{K}[t]$. On suppose, sans perte de généralité, que $n \geq m$ et pour la preuve on pose $a_j = 0$ pour tout $j > m$. On a

$$\phi(p + q) = \phi((a_0 + b_0) + (a_1 + b_1)t + \cdots + (a_n + b_n)t^n)$$

$$= (a_0 + b_0) + (a_1 + b_1)c + \cdots + (a_n + b_n)c^n = (a_0 + a_1 c + \cdots + a_n c^n) + (b_0 + b_1 c + \cdots + b_n c^n) = \phi(p) + \phi(q).$$

La troisième égalité découle des axiomes de distributivité et la commutativité de l'addition dans A.

On a aussi

$$\phi(pq) = \phi(a_0 b_0 + (a_0 b_1 + a_1 b_0)t + \cdots + (\sum_{i+j=k} (a_i b_j))t^k + \cdots + a_n b_n t^{2n}$$

$$= a_0 b_0 + (a_0 b_1 + a_1 b_0)c + \cdots + (\sum_{i+j=k} (a_i b_j))c^k + \cdots + a_n b_n c^{2n} = (a_0 + a_1 c + \cdots a_n c^n)(b_0 + b_1 c + \cdots + b_n c^n) = \phi(p)\phi(q).$$

Ici l'avant dernière égalité découle des axiomes de distributivité et la commutativité de l'addition dans A.

Enfin, $e_c(1_K) = 1_K = 1_A$. Ca complète la vérification.

Exercice 6. *Vérifier que pour tout $\bar{c} \in \mathbb{F}_3$ on a $\bar{c}^3 - \bar{c} = \bar{0}$, et de même que dans $\mathbb{F}_5$ on a $\bar{b}^5 - \bar{b} = \bar{0}$ pour tout $\bar{b} \in \mathbb{F}_5$. Montrer que le polynôme $t^3 - t \in \mathbb{F}_3[t]$ est scindé et que le polynôme $t^5 - t \in \mathbb{F}_5[t]$ est scindé.*

Solution 6. On vérifie que $0^3 - 0 \equiv 0 \mod 3$; $1^3 - 1 \equiv 0 \mod 3$; et $2^3 - 2 \equiv 0 \mod 3$. De même,

$$0^5 - 0 \equiv 0 \mod 5;\ 1^5 - 1 \equiv 0 \mod 5;\ 2^5 - 2 \equiv 0 \mod 5;\ 3^5 - 3 \equiv 0 \mod 5;\ \text{et } 4^5 - 4 \equiv 0 \mod 5.$$

Maintenant, on sait d'après le cours que pour un corps K et $c \in K$, si c est une racine d'un polynôme $p \in K[t]$, alors $(t-c)$ est un facteur de p.

On utilise les calculs ci-dessus et on vérifé que $t^3 - t = t(t-\bar{1})(t-\bar{2})$ dans $\mathbb{F}_3[t]$ et

$$t^5 - t = t(t-\bar{1})(t-\bar{2})(t-\bar{3})(t-\bar{4}),\ \text{dans } \mathbb{F}_5[t].$$

Exercice 7. *Dans chacun des cas suivants, l'ensemble V est-il un K-espace vectoriel pour la loi évidente d'addition et la multiplication scalaire donnée?*

a) $K = \mathbb{C}$, $V = \mathbb{C}^2$ *et* $\lambda(x,y) = (\mathrm{Re}(\lambda)x, \mathrm{Re}(\lambda)y)$ *pour* $\lambda \in \mathbb{C}$ *et* $(x,y) \in V$.

b) $K = \mathbb{R}$, $V = \mathbb{R}^2$ *et* $\lambda(x,y) = (\lambda x, \lambda^2 y)$ *pour* $\lambda \in \mathbb{R}$ *et* $(x,y) \in V$.

c) $K = \mathbb{F}_2$, $V = \mathbb{F}_2^2$ *et* $\lambda(x,y) = (\lambda x, \lambda^2 y)$ *pour* $\lambda \in \mathbb{F}_2$ *et* $(x,y) \in V$.

d) $K = \mathbb{R}$, $V = \{f \in \mathbb{R}[t] \mid f(a) = 0\}$ *pour* $a \in \mathbb{R}$ *fixé et la multiplication scalaire au sens usuel.*

e) $K = \mathbb{R}$, $V = \{f \in \mathbb{R}[t] \mid f(-a) = -f(a)\ \forall a \in \mathbb{R}\}$ *et la multiplication scalaire au sens usuel.*

Solution 7. a) Non, car par exemple, si $\lambda = 2 + \mathrm{i}$ et $\mu = \mathrm{i}$ on a que

$$(\lambda\mu)(1,1) = (-1+2\mathrm{i})(1,1) = (-1,-1),\ \text{et}$$
$$\lambda(\mu(1,1)) = (2+\mathrm{i})(0,0) = (0,0).$$

b) Non, car si $\lambda, \mu \in \mathbb{R}$ sont les deux non nuls,

$$(\lambda+\mu)(x,y) = ((\lambda+\mu)x, (\lambda+\mu)^2 y) \neq \lambda(x,y) + \mu(x,y) = ((\lambda+\mu)x, (\lambda^2+\mu^2)y).$$

c) Oui, cela est évident si on tient compte du fait que $\lambda^2 = \lambda\ \forall \lambda \in \mathbb{F}_2$.

d) Tous les axiomes définissant un espace vectoriel sont facilement vérifiés.

e) Tous les axiomes définissant un espace vectoriel sont facilement vérifiés. L'espace vectoriel V est constitué par les polynômes ayant uniquement des termes de degré impair.

Exercice 8. *Dans chacun des cas suivants, l'ensemble V est-il un K-espace vectoriel (pour les lois évidentes d'addition et de multiplication scalaire)?*

a) $K = \mathbb{R}$, $V = \{f : \mathbb{R} \to \mathbb{R} \mid f(n) \geq 0,\ \forall\, n \in \mathbb{Z}\}$,

b) $K = \mathbb{R}$, $V = \{a + bt \in \mathbb{R}[t] \mid a, b \in \mathbb{R}\}$,

c) $K = \mathbb{C}$, $V = \{f \in \mathbb{C}[t] \mid f(0) \in \mathbb{R}\}$,

d) $K = \mathbb{R}$, $V = \{f \in \mathbb{C}[t] \mid f(0) \in \mathbb{R}\}$.

Solution 8. a) Non, car si $f \in V$ tel que $f(n) > 0$ pour un certain $n \in \mathbb{N}$, alors $-f(n) < 0$, donc $-f \notin V$.

b) Oui. Les vérifications des axiomes sont faciles.

c) Non, car si $f \in V$ tel que $0 \neq f(0) \in \mathbb{R}$, alors $\mathrm{i}f(0) \notin \mathbb{R}$ et donc $\mathrm{i}f \notin V$.

d) Oui. Les vérifications des axiomes sont faciles.

Exercice 9. *On pose $\mathcal{A}$ l'ensemble des fonctions de $\mathbb{R}$ dans $\mathbb{R}$ dont la dérivée est définie sur $\mathbb{R}$, donc $\mathcal{A} \subset \mathcal{F}(\mathbb{R},\mathbb{R})$, l'anneau des fonctions de $\mathbb{R}$ dans $\mathbb{R}$ (comme défini en cours). Alors comme la somme de deux fonctions dérivables est dérivable, le produit de deux fonctions dérivables l'est aussi, et la fonction $f(x) = 1$ pour tout $x \in \mathbb{R}$ est également dérivable, $\mathcal{A}$ est un anneau unitaire avec les lois de $+$ et $\cdot$ héritées de $\mathcal{F}(\mathbb{R},\mathbb{R})$. On considère l'application $D : \mathcal{A} \to \mathcal{F}(\mathbb{R},\mathbb{R})$, donnée par $D(f) = f'$, c'est-à-dire, D est l'application qui associe à une fonction f sa dérivée.*

1. *Montrer que D est un homomorphisme de groupes du groupe $(\mathcal{A}, +)$ dans le groupe $(\mathcal{F}(\mathbb{R}, \mathbb{R}), +)$.*
2. *Montrer que D n'est pas un homomorphisme d'anneaux entre les anneaux $(\mathcal{F}(\mathbb{R}, \mathbb{R}), +, \cdot)$ et $(\mathcal{A}, +, \cdot)$.*

Solution 9. On rappelle que $(f+g)' = f' + g'$ et donc $D(f+g) = D(f) + D(g)$ pour tout $f, g \in \mathcal{A}$, et on déduit que D est un homomorphisme de groupes. Par contre, comme $(fg)' = f'g + fg'$, nous n'avons pas que $D(fg) = D(f)D(g)$ et D ne préserve pas la loi de multiplication dans les deux anneaux. Par exemple, $D(x \cdot x) = D(x^2) = 2x \neq D(x) \cdot D(x) = 1 \cdot 1 = 1$. Ceci montre que D n'est pas un homomorphisme d'anneaux.

Exercice 10 (Facultatif)**.** *Soient $d, n \in \mathbb{Z}$ avec $d \geq 1$ et $n \geq 1$ où d est un diviseur de n (c'est-à-dire que n est un multiple entier de d). Pour cet exercice on ecrira $\bar{a}$ pour un élément de $\mathbb{Z}/d\mathbb{Z}$ et $[b]$ pour un élément de $\mathbb{Z}/n\mathbb{Z}$, pour bien distinguer à quel ensemble chaque élément appartient. Montrer que l'application*

$$f : \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/d\mathbb{Z}, \text{ donnée par } f([b]) = \bar{b}$$

est bien définie. Ensuite, montrer que f est un morphisme d'anneaux.

Solution 10. Pour la première partie, on doit montrer que si $[a] = [b]$ alors $f([a]) = f([b])$. On suppose donc que $[a] = [b]$, ce qui est vrai si et seulement si $b = a + kn$ pour un entier k. On rappelle que d divise n, donc $n = dm$ pour un entier m. On trouve ainsi que $b = a + kn = a + kdm$, ce qui implique que $\bar{b} = \bar{a}$ dans $\mathbb{Z}/d\mathbb{Z}$ et de suite que $f([a]) = f([b])$ comme souhaité.

Pour les propriétés d'un morphisme d'anneaux : $f([a] + [c]) = f([a + c]) = \overline{a + c} = \bar{a} + \bar{c} = f([a]) + f([c])$, où la première et la troisième égalités proviennent de la définition de la loi $+$ dans $\mathbb{Z}/n\mathbb{Z}$, et $\mathbb{Z}/d\mathbb{Z}$.

Pour la deuxième loi $\cdot$, l'argument est pareil et $f([1]) = \bar{1}$, ce qui complète la vérification que f est un morphisme d'anneaux.

Exercice 11 (Facultatif)**.** *On définit une loi de composition $*$ sur l'ensemble $E = \mathbb{R} \setminus \{0\}$ comme suit : pour tout $x, y \in E$ on a $x * y = |x|y$.*

(i) *Montrer que $*$ est associative.*

(ii) *Montrer qu'il existe un élément neutre e à gauche pour $*$, c'est-à-dire qu'il existe $e \in E$ tel que $e * b = b$ pour tout $b \in E$.*

(iii) *Montrer qu'il n'existe aucun élément neutre à droite.*

(iv) *Montrer que tout élément $a \in E$ possède un inverse à droite, c'est-à-dire qu'il existe $a' \in E$ tel que $a * a' = e$, où e est l'élément neutre à gauche trouvé dans (ii).*

On remarque donc que $(E, *)$ n'est pas un groupe et que l'existence d'une loi de composition associative, d'un élément neutre à gauche et des inverses à droite n'est pas suffisant pour définir une structure de groupe.

Solution 11. Pour (i), on a que $(a * b) * c = |a * b| \cdot c = ||a|b| \cdot c = ||a|| \cdot |b| \cdot c = |a| \cdot |b| \cdot c$, et $a * (b * c) = |a|(b * c) = |a| \cdot (|b|c) = |a| \cdot |b| \cdot c = (a * b) * c$. Pour (ii), on vérifie que $1 * a = |1|a = a$ pour tout $a \in E$, donc 1 est un élément neutre à gauche. (iii) Pour $a, f \in E$, on a que $a * f = |a|f = a$ si et seulement si $f = \frac{a}{|a|}$ et si $a > 0$, on trouvera $f = 1$ et si $a < 0$ on trouvera $f = -1$. Donc il n'existe aucun élément de E qui satisfait la condition pour être un élément neutre à droite. Enfin pour (iv), comme $a * \frac{1}{|a|} = |a| \frac{1}{|a|} = 1$, l'élément $\frac{1}{|a|}$ est un inverse à droite de l'élément a.
