Université Aix-Marseille 2018–2019

Licence – Mathématiques
Algèbre 2

Examen terminal
corrigé

Exercice 1.

1. (a) Le reste de la division euclidienne de $n \in \mathbb{Z}$ par $k \in \mathbb{N}^*$ est l'unique entier $r \in [\![0, k-1]\!]$ tel qu'il existe $q \in \mathbb{Z}$ vérifiant $n = q.k + r$.
   (b) Pour toute permutation $\sigma \in \mathfrak{S}_n$, avec $n \geq 2$ entier, la signature de σ est égale à son image par l'unique morphisme de groupe non trivial allant de $\mathfrak{S}_n$ vers $\{\pm 1\}$. Cela correspond également à $(-1)^{t_\sigma}$, où t_σ est égale au nombre d'inversions de σ, c'est-à-dire de couples $(i, j) \in [\![1, n]\!]^2$ tels que $i < j$ et $\sigma(j) < \sigma(i)$.
   (c) Un idéal d'un anneau A est un sous-groupe $I \subset A$ pour l'addition, stable par multiplication à droite et à gauche par tout élément de A.
2. D'après le théorème de Lagrange, si H est un sous-groupe d'un groupe fini G, alors le cardinal de H divise le cardinal de G.
3. Soit A, B deux anneaux unitaires et $f : A \to B$ un isomorphisme unitaire d'anneaux. Puisque f est bijective, f^{-1} l'est aussi ; il suffit donc de montrer que f préserve l'addition, la multiplication et l'élément unité. Or, pour tout $b_1, b_2 \in B$, il existe $a_1, a_2 \in A$ tels que $f(a_1) = b_1$ et $f(a_2) = b_2$ par surjectivité de f. Dès lors, on a $f^{-1}(b_1 + b_2) = f^{-1}\big(f(a_1) + f(a_2)\big) = f^{-1}\big(f(a_1 + a_2)\big) = a_1 + a_2 = f^{-1}(b_1) + f^{-1}(b_2)$ puisque f préserve l'addition ; et $f^{-1}(b_1.b_2) = f^{-1}\big(f(a_1).f(a_2)\big) = f^{-1}\big(f(a_1.a_2)\big) = a_1.a_2 = f^{-1}(b_1).f^{-1}(b_2)$ puisque f préserve la multiplication. Enfin, $f(1_A) = 1_B$ car f est unitaire, donc $f^{-1}(1_B) = 1_A$.

Exercice 2.

1. (a) Considérons $k \in [\![0, 34]\!]$. L'élément $\overline{k} \in \mathbb{Z}/35\mathbb{Z}$ est un diviseur de zéro si et seulement si il existe $k' \in [\![1, 34]\!]$ tel que $k.k'$ soit un multiple de $35 = 5.7$. Mais alors, d'après le lemme d'Euclide, 5 et 7 doivent chacun diviser k ou k', mais les deux ne peuvent pas diviser k' car alors on aurait $k' \geq 35$. On en déduit que $\overline{k}$ est un diviseur de zéro si et seulement si il est divisible par 5 ou par 7. L'ensemble des diviseurs de zéros dans $\mathbb{Z}/35\mathbb{Z}$ est donc $\big\{\overline{0}, \overline{5}, \overline{7}, \overline{10}, \overline{14}, \overline{15}, \overline{20}, \overline{21}, \overline{25}, \overline{28}, \overline{30}\big\}$.
   (b) Commençons par écrire une relation de Bézout entre 183 et 247. Par divisions euclidiennes successives, on a
   - $247 = 183 + 64$;
   - $183 = 2.64 + 55$;
   - $64 = 55 + 9$;
   - $55 = 6.9 + 1$.

   On en déduit que

$$\begin{aligned} 1 &= 55 - 6.9 = 55 - 6.(64 - 55) = -6.64 + 7.55 \\ &= -6.64 + 7.(183 - 2.64) = 7.183 - 20.64 \\ &= 7.183 - 20.(247 - 183) = 27.183 - 20.247. \end{aligned}$$

   En considérant cette égalité modulo 247, on en déduit que $\overline{27}.\overline{183} = \overline{1}$.
2. (a) D'après la question précédente, on a, dans $\mathbb{Z}/247\mathbb{Z}$,

$$\begin{aligned} \overline{183}.x + \overline{236} = \overline{0} &\Leftrightarrow \overline{183}.x = -\overline{236} = \overline{11} \\ &\Leftrightarrow \overline{27}.\overline{183}.x = \overline{27}.\overline{11} \\ &\Leftrightarrow x = \overline{297} = \overline{50}. \end{aligned}$$

   (b) Par factorisation directe, on a $x^2 - \overline{3}.x + \overline{2} = (x - \overline{1}).(x - \overline{2})$. Or pour qu'un tel produit s'annule, il faut qu'ou bien un des facteurs soit nul, ou bien qu'ils soient tous les deux des diviseurs de zéros.

Dans le premier cas, on trouve les solutions $\overline{1}$ et $\overline{2}$. Dans le second cas, en notant $x = \overline{k}$ et d'après la question 1.(a), il faut que $\overline{k-1}, \overline{k-2} \in \left\{\overline{0}, \overline{5}, \overline{7}, \overline{10}, \overline{14}, \overline{15}, \overline{20}, \overline{21}, \overline{25}, \overline{28}, \overline{30}\right\}$; or les seules paires d'entiers consécutifs sont $(14, 15)$ et $(20, 21)$, lesquels vérifient bien $\overline{15}.\overline{14} = \overline{21}.\overline{20} = \overline{0}$. Au final, l'ensemble des solutions de l'équation est donc $\left\{\overline{1}, \overline{2}, \overline{16}, \overline{22}\right\}$.

Exercice 3.

1. Si $a \in A$ est nilpotent, alors il existe $n \in \mathbb{N}^*$ tel que $a^n = 0$ et donc, pour tout $b \in A$, on a $(a.b)^n = a^n.b^n = 0.b^n = 0$ puisque A est commutatif. L'élément $a.b$ est donc lui aussi nilpotent.
2. D'après la question précédente, $\mathcal{N}(A)$ est stable par multiplication (à droite et à gauche puisque A est commutatif) par tout élément de A. Pour montrer qu'il s'agit d'un idéal, il suffit donc de montrer que $\mathcal{N}(A)$ est un sous-groupe additif de A. Pour cela, on considère $a, b \in \mathcal{N}(A)$; il existe donc $n_a, n_b \in \mathbb{N}^*$ tels que $a^{n_a} = b^{n_b} = 0$. En posant $N = n_a + n_b \in \mathbb{N}^*$, on a alors d'après le formule du binôme de Newton

$$\begin{aligned}
(a-b)^N &= \sum_{k=0}^{N} \binom{N}{k} a^k.(-b)^{N-k} \\
&= \sum_{k=0}^{n_a-1} (-1)^{N-k}.\binom{N}{k} a^k.b^{n-k} + \sum_{k=n_a}^{N} (-1)^{N-k}.\binom{N}{k} a^k.b^{N-k} \\
&= \sum_{k=0}^{n_a-1} (-1)^{N-k}.\binom{N}{k} a^k.b^{n_b}.b^{N-k-n_b} + \sum_{k=n_a}^{N} (-1)^{N-k}.\binom{N}{k} a^{n_a}.a^{k-n_a}.b^{N-k} \\
&= \sum_{k=0}^{n_a-1} (-1)^{N-k}.\binom{N}{k} a^k.0.b^{N-k-n_b} + \sum_{k=n_a}^{N} (-1)^{N-k}.\binom{N}{k} 0.a^{k-n_a}.b^{N-k} \;=\; 0
\end{aligned}$$

puisque, si $k \leq n_a$, $N - k - n_b = n_a + n_b - k - n_b = n_a - k > 0$. On en déduit que $a - b \in \mathcal{N}(A)$ et donc que $\mathcal{N}(A)$ est un idéal.
3. Soit $a \in \mathcal{N}(A)$ et $n \in \mathbb{N}^*$ tel que $a^n = 0$. Par identité remarquable, on a alors $(1-a).(1 + a + \cdots + a^{n-1}) = 1 - a^n = 1$, montrant que $1 - a$ est donc inversible. Appliqué en $-a$, lequel est encore nilpotent d'après la question 1., cela montre que $1 - (-a) = 1 + a$ est aussi inversible.

Exercice 4.

1. (a) i. On a $P(\sigma_1)_{ik}.P(\sigma_2)_{kj} \neq 0$ si et seulement si $P(\sigma_1)_{ik}$ et $P(\sigma_2)_{kj}$ sont chacun non nuls, et par définition cela n'est le cas, pour le premier, que si $i = \sigma_1(k)$, c'est-à-dire si $k = \sigma_1^{-1}(i)$ et, pour le second, que si $k = \sigma_2(j)$.
   ii. D'après la formule définissant le produit des matrices, le coefficient sur la $i^{\text{ième}}$ ligne et la $j^{\text{ième}}$ colonne de $P(\sigma_1).P(\sigma_2)$ vaut $\sum_{k=1}^{n} P(\sigma_1)_{ik}.P(\sigma_2)_{kj}$. Or, selon la question précédente, tous les termes de cette somme n'annulent lorsque $\sigma_1^{-1}(i) \neq \sigma_1(j)$, c'est-à-dire lorsque $i \neq (\sigma_1 \circ \sigma_2)(j)$; et lorsque $i = (\sigma_1 \circ \sigma_2)(j)$, seul le terme correspondant à $k = \sigma_2(j)\big(= \sigma_1^{-1}(i)\big)$ est non nul, valant alors 1. En résumé, le coefficient vaut 1 si $i = (\sigma_1 \circ \sigma_2)(j)$ et 0 sinon. On a donc bien $P(\sigma_1).P(\sigma_2) = P(\sigma_1 \circ \sigma_2)$.

   (b) i. Si τ est une transposition élémentaire, alors $P(\tau)$ est diagonale par blocs :

$$\begin{pmatrix}
1 & & & & & & \\
& \ddots & & & & 0 & \\
& & 1 & & & & \\
& & & \boxed{\begin{matrix} 0 & 1 \\ 1 & 0 \end{matrix}} & & & \\
& & & & 1 & & \\
& 0 & & & & \ddots & \\
& & & & & & 1
\end{pmatrix}.$$

   Le déterminant vaut donc le produit des déterminants des blocs (autrement, on peut

développer selon toutes les lignes autres que cells du bloc 2×2) et on a donc

$$\det\big(P(\tau)\big) = \begin{vmatrix} 0 & 1 \\ 1 & 0 \end{vmatrix} = -1.$$

ii. Soit $\sigma \in \mathfrak{S}_n$. On sait que σ peut s'écrire comme un produit $\tau_1 \circ \cdots \circ \tau_r$ de $r \in \mathbb{N}$ transpositions élémentaires. D'après la question et la question 1.(a).ii, on a alors

$$\det\big(P(\sigma)\big) = \det\big(P(\tau_1 \circ \cdots \circ \tau_r)\big) = \det\big(P(\tau_1).\cdots.P(\tau_r)\big) = \det\big(P(\tau_1)\big).\cdots.\det\big(P(\tau_r)\big) = (-1)^r,$$

ce qui n'est autre que la signature de σ puisque σ s'écrit donc comme un produit de r transpositions.

2. Pour montrer que l'application P est bien définie, il faut vérifier que son image est bien dans $\mathrm{GL}_n(\mathbb{R})$, or nous venons de voir que $\det\big(P(\sigma)\big) = \pm 1 \neq 0$ pour tout $\sigma \in \mathfrak{S}_n$. Pour montrer qu'il s'agit d'un morphisme de groupe, il faut vérifier que $P(\sigma_1 \circ \sigma_2) = P(\sigma_1).P(\sigma_2)$ pour tout $\sigma_1, \sigma_2 \in \mathfrak{S}_n$, ce qui a été fait à la question 1.(a).ii. Pour montrer qu'il s'agit d'un monomorphisme, il ne suffit donc plus qu'à montrer que P est injective. Pour cela, on considère $\sigma \in \mathrm{Ker}(P)$. Pour tout $i \in [\![1, n]\!]$, le seul coefficient non nul dans la $i^{\text{ième}}$ colonne de $P(\sigma) = \mathrm{Id}$ est donc sur la $i^{\text{ième}}$ ligne, ce qui, par définition, indique que $\sigma(i) = i$; on a donc bien $\sigma = \mathrm{Id}_{[\![1,n]\!]}$.
3. D'après le théorème de Cayley, pour tout groupe fini G d'ordre n, il existe un monomorphisme de groupes $\psi_G : G \to \mathfrak{S}_n$. En composant avec P, on obtient donc un monomorphisme de groupes $P \circ \psi_G : G \to \mathrm{GL}_n(\mathbb{R})$, lequel induit un isomorphisme de groupes entre G et $\mathrm{Im}(P \circ \psi_G) \subset \mathrm{GL}_n(\mathbb{R})$.