1 (lemme de la trace). Soit V un $\mathbb{C}$-espace vectoriel de dimension finie n et G un groupe opérant fidèlement et $\mathbb{C}$-linéairement sur V de sorte que la représentation V de G soit irréductible. On suppose que la fonction $\chi\colon G \to \mathbb{C}$ (le « caractère ») associant à un $g \in G$ la trace de l'action $\rho(g)$ de g sur V, a une image finie de cardinal r. Montrer alors que $\operatorname{card} G \leq r^{n^2}$. Pour cela, on montrera (en utilisant un résultat de Burnside) qu'il existe n^2 éléments $g_1, \ldots, g_{n^2}$ de G qui (c'est-à-dire dont les images par $\rho\colon G \to \operatorname{End}_{\mathbb{C}}(V)$) forment une $\mathbb{C}$-base de $\operatorname{End}_{\mathbb{C}}(V) \cong \mathbb{M}_n(\mathbb{C})$, puis on montrera que les traces des hg_i, pour $h \in \operatorname{End}_{\mathbb{C}}(V)$, déterminent h.

Application (problème de Burnside pour les groupes linéaires) : Supposons que G soit un sous-groupe de $GL_n(\mathbb{C})$ tel que $g^N = 1$ pour tout $g \in G$ (l'exposant de G divise N) : montrer qu'alors $\operatorname{card} G \leq N^{n^3}$, d'abord en supposant que $\mathbb{C}^n$ est une représentation irréductible de G, puis sans cette hypothèse (en procédant par récurrence sur la dimension, en décomposant explicitement l'action de G).

Corrigé. D'après un résultat de Burnside, puisque V est une représentation irréductible (sur un corps algébriquement clos, en l'occurrence $\mathbb{C}$), l'application $\mathbb{C}[G] \to \operatorname{End}_{\mathbb{C}}(V)$ est surjective. Il s'ensuit qu'il existe n^2 éléments $g_1, \ldots, g_{n^2}$ de G dont les images dans $\operatorname{End}_{\mathbb{C}}(V) \cong \mathbb{M}_n(\mathbb{C})$ forment une base de celui-ci. Regardons à présent l'application $\mathbb{C}$-linéaire $\varepsilon\colon \operatorname{End}_{\mathbb{C}}(V) \to \mathbb{C}^{n^2}$ qui envoie $h \in \operatorname{End}_{\mathbb{C}}(V)$ sur l'ensemble des traces $\operatorname{tr}(h\rho(g_i))$ des (actions de) hg_i sur V. Si on a $\varepsilon(h) = 0$ alors $\operatorname{tr}(h\rho(g_i)) = 0$ pour tout i, donc $\operatorname{tr}(h\gamma) = 0$ pour tout $\gamma \in \operatorname{End}_{\mathbb{C}}(V)$, et en prenant pour γ les différents éléments de la base canonique de $\mathbb{M}_n(\mathbb{C})$, on voit que $h = 0$. Ceci prouve l'injectivité de ε. Mais alors G a un cardinal borné par son image par $\varepsilon \circ \rho$, soit au plus r^{n^2} (puisque chaque coordonnée de ε prend au plus r valeurs), comme annoncé.

Soit maintenant G un sous-groupe de $GL_n(\mathbb{C})$ tel que $g^N = 1$ pour tout $g \in G$. Dans un premier temps, supposons que $\mathbb{C}^n$ est irréductible sous G. Les valeurs propres d'un élément $g \in G$ sont toutes des racines N-ièmes de l'unité, dont la trace de g, qui est somme de n telles valeurs, peut prendre au plus N^n valeurs distinctes. Le résultat précédent montre alors que $\operatorname{card} G \leq (N^n)^{n^2} = N^{n^3}$.

À présent, supposons que $V = \mathbb{C}^n$ soit réductible en $V_1 \oplus V_2$ avec V_i de dimension $n_i > 0$ sur $\mathbb{C}$. En prenant une base de V adaptée à cette décomposition, un élément $g \in G$ s'écrit $\begin{pmatrix} g_1 & h \\ 0 & g_2 \end{pmatrix}$ avec $g_1 \in \operatorname{End}_{\mathbb{C}}(V_1) \cong \mathbb{M}_{n_1}(\mathbb{C})$ et $g_2 \in \operatorname{End}_{\mathbb{C}}(V_2) \cong \mathbb{M}_{n_2}(\mathbb{C})$. Soit G_1 (resp. G_2) l'ensemble des g_1 (resp. g_2) pour g parcourant G : manifestement il est bien un sous-groupe de $GL_{n_1}(\mathbb{C})$ (resp. $GL_{n_2}(\mathbb{C})$), d'exposant divisant N, donc une récurrence permet de supposer $\operatorname{card} G_i \leq N^{{n_i}^3}$. Mais le morphisme $G \to G_1 \times G_2$ est injectif : car si g est dans le noyau, l'hypothèse $g^N = 1$ donne immédiatement $Nh = 0$ donc $h = 0$ (le corps de base est de caractéristique zéro). Notamment, g_1 et g_2 déterminent g. Et alors $\operatorname{card} G \leq N^{n_1^3 + n_2^3} \leq N^{n^3}$, ce qui termine la démonstration. ✓

2 (radical de Jacobson). Soit A un anneau (associatif unitaire mais non nécessairement commutatif). On rappelle qu'un *A-module à gauche* (parfois dit « représentation » de A, mais on préfère garder ce terme pour le cas où A est une algèbre sur un corps k, ce que, d'ailleurs, on pourra éventuellement supposer) est un groupe abélien M muni d'un morphisme d'anneaux $A \to \operatorname{End}_{\mathbb{Z}}(M)$: naturellement, A lui-même est un A-module à gauche de façon évidente, et un sous-A-module de celui-ci (c'est-à-dire un sous-groupe additif de A stable par multiplication à gauche par A) sera appelé *idéal à gauche* de A. Un idéal à gauche est dit *maximal* lorsqu'il est strictement contenu dans A et maximal pour l'inclusion parmi les idéaux à gauche strictement contenus dans A. On dit par ailleurs qu'un A-module à gauche non nul est *simple* (ou *irréductible*) lorsque tout sous-A-module strict de celui-ci est nul.

Pour un élément $x \in A$ donné, montrer l'équivalence entre les affirmations suivantes : (i) x appartient à tous les idéaux à gauche maximaux de A, (ii) pour tout $a \in A$ l'élément $1 + ax$ est inversible à gauche dans A, et (iii) $xM = 0$ pour tout A-module à gauche simple M. En déduire que l'intersection de tous les idéaux à gauche maximaux de A est un idéal à droite (donc bilatère) de A, et que c'est l'intersection de tous les idéaux à droite maximaux de A (pour cela, on pourra trouver une condition semblable à (ii) mais symétrique entre droite et gauche).

Cette intersection commune aux idéaux à gauche maximaux de A et aux idéaux à droite maximaux de A sera appelée *radical de Jacobson* de A et notée $\operatorname{rad} A$.

Corrigé. Montrons que (i) implique (ii) : soit x contenu dans tous les idéaux à gauche maximaux de A ; si $a \in A$ et $1+ax$ n'est pas inversible à gauche, alors $1+ax$ engendre un idéal à gauche strict de A qui est donc contenu dans un idéal à gauche maximal $\mathfrak{m}$. Mais alors $x \in \mathfrak{m}$ donc $ax \in \mathfrak{m}$ donc $1 \in \mathfrak{m}$, une contradiction. Montrons maintenant que (ii) implique (iii) : soit x tel que $1 + ax$ soit inversible à gauche pour tout $a \in A$, et supposons $xv \neq 0$ pour un certain $v \in M$ avec M un A-module à gauche simple. Alors $A \cdot xv \neq 0$ donc $A \cdot xv = M$ (par simplicité) donc il existe $a \in A$ tel que $-axv = v$, et alors $(1 + ax)v = 0$ donc $v = 0$, une contradiction. Montrons enfin que (iii) implique (i) : soit x tel que $xM = 0$ pour tout A-module à gauche simple ; mais si $\mathfrak{m}$ est un idéal à gauche maximal de A alors $A/\mathfrak{m}$ est un A-module à gauche simple, donc on doit avoir $x(A/\mathfrak{m}) = 0$, donc $x \in \mathfrak{m}$. Ceci prouve l'équivalence souhaitée.

Montrons à présent que la condition (iii) est stable par multiplication à droite : or si $xM = 0$, pour M un A-module à gauche simple, et si $b \in A$ alors $xbM \subseteq xM = 0$. Grâce à l'équivalence entre (i) et (iii), on voit que l'intersection de tous les idéaux à gauche maximaux de A est bien un idéal à droite. À présent, montrons que (ii) est encore équivalent à l'affirmation (ii *bis*) : pour tous $a, b \in A$, l'élément $1 + axb$ est inversible (est une unité de A). Il est évident que (ii *bis*) implique (ii). Pour ce qui est de la réciproque, supposons que x vérifie (i)–(iii) : alors on vient de voir que xb les vérifie encore, donc $1 + axb$ est inversible à gauche ; mais si $u(1 + axb) = 1$, on a $u = 1 - uaxb$ donc (d'après le raisonnement qu'on vient de faire) u est lui-même inversible à gauche, donc u est une unité, donc $1+axb$ en est une (et est son inverse). Comme la condition (ii *bis*) est symétrique, on a prouvé que l'intersection de tous les idéaux à gauche maximaux de A était aussi l'intersection de tous les idéaux à droite maximaux de A. ✓

3 (semisimplicité). Cet exercice fait suite à l'exerice 2. Soit k un corps et A une k-algèbre (associative unitaire mais non nécessairement commutative) qu'on supposera tout du long être de dimension finie sur k ainsi que tous les modules qui vont intervenir. On rappelle que A est dite *semisimple* (a priori « à gauche », mais en fait cette condition est symétrique comme on va le voir) lorsque tout sous-A-module à gauche N d'un A-module à gauche M admet un supplémentaire (i.e., on peut écrire $M = N \oplus N'$ pour un certain sous-A-module à gauche N' de M) ; on rappelle aussi que A est semisimple si et seulement si A, vu comme A-module à gauche de la façon naturelle, est somme de A-modules à gauche simples (qui sont donc des idéaux à gauche non nuls minimaux pour l'inclusion).

On suppose que le radical de Jacobson de A est nul : montrer que pour une certaine famille finie $\mathfrak{m}_1, \ldots, \mathfrak{m}_r$ d'idéaux à gauche maximaux de A la flèche naturelle $A \to \bigoplus_i (A/\mathfrak{m}_i)$ est injective. En déduire que A est semisimple.

Réciproquement, si A est semisimple, montrer que son radical de Jacobson est nul (on pourra écrire un supplémentaire du radical).

Corrigé. Supposons que le radical de Jacobson de A est nul et montrons l'affirmation concernant l'injectivité de $A \to \bigoplus_i (A/\mathfrak{m}_i)$. Comme l'intersection de tous les $\mathfrak{m}$ (idéaux à gauche maximaux de A) est nulle par hypothèse, et comme A est de dimension finie sur k, il doit exister une famille finie $\mathfrak{m}_1, \ldots, \mathfrak{m}_r$ (d'idéaux à gauche maximaux de A) dont l'intersection est nulle : or ceci montre précisément que la flèche $\psi\colon A \to \bigoplus_{i=1}^r (A/\mathfrak{m}_i)$ (dont le noyau est justement cette intersection) est injective. Par le même raisonnement qu'on a fait ci-dessus, on peut réduire l'ensemble des i tels que l'image de ψ soit précisément égal à cette somme directe. Par conséquent, A est semisimple.

Réciproquement, si A est semisimple, soit $\mathfrak{A} = \operatorname{rad} A$ son radical de Jacobson et $\mathfrak{B}$ un idéal à gauche tel que $A = \mathfrak{A} \oplus \mathfrak{B}$. L'idéal à gauche $\mathfrak{B}$ doit être contenu dans un idéal à gauche maximal, $\mathfrak{m}$, mais comme $\mathfrak{A}$ est le radical de Jacobson, on a aussi $\mathfrak{m} \supseteq \mathfrak{A}$, donc $\mathfrak{m}$ devrait contenir $\mathfrak{A} \oplus \mathfrak{B}$, ce qui est impossible. ✓

4. Soit Q le groupe des quaternions, i.e., le groupe ayant huit éléments $1, s_i, s_j, s_k, t, ts_i, ts_j, ts_k$, où t est central, $t^2 = 1$, et $s_i^2 = s_j^2 = s_k^2 = s_i s_j s_k = t$. On appelle $\mathbb{R}[Q]$ l'algèbre de groupe sur Q à coefficients dans $\mathbb{R}$ (c'est-à-dire les combinaisons $\mathbb{R}$-linéaire formelles d'éléments de Q, la multiplication provenant de celle sur Q). On rappelle qu'une représentation de Q signifie la même chose qu'une représentation de $\mathbb{R}[Q]$ (un $\mathbb{R}[Q]$-module à gauche).

Déterminer quatre représentations de Q de dimension 1 sur $\mathbb{R}$. Montrer que le plongement évident (soit $t \mapsto -1$, $s_i \mapsto i$, $s_j \mapsto j$ et $s_k \mapsto k$) de Q dans l'algèbre $\mathbb{H}$ des quaternions réels[1] définit une représentation irréductible (= simple) de Q de dimension 4 sur $\mathbb{R}$. En déduire une écriture explicite de la $\mathbb{R}$-algèbre (semisimple) $\mathbb{R}[Q]$ comme produit d'algèbres simples.

En déduire une écriture de $\mathbb{C}[Q]$ comme produit d'algèbres de matrices (on rappelle — ou on admet — que $\mathbb{H} \otimes_{\mathbb{R}} \mathbb{C} \cong \mathbb{M}_2(\mathbb{C})$). Quelles sont les représentations irréductibles complexes de Q ?

Corrigé. On dispose tout d'abord de la représentation triviale U, autrement dit l'action de Q sur $\mathbb{R}$ par l'identité. Par ailleurs, le groupe Q admet trois sous-groupes (distingués) d'indice 2, à savoir $H_i = \{1, s_i, t, ts_i\}$, $H_j = \{1, s_j, t, ts_j\}$ et $H_k = \{1, s_k, t, ts_k\}$, ses quotients par lesquels sont d'ordre 2 : à partir de la représentation V du groupe $\mathbb{Z}/2\mathbb{Z}$ sur $\mathbb{R}$ dans laquelle l'unique élément s non trivial agit comme $x \mapsto -x$, on obtient trois représentations V_i, V_j et V_k de dimension 1 de Q (ainsi, sur V_i, les éléments $1, s_i, t, ts_i$ agissent comme l'identité tandis que s_j, s_k, ts_j, ts_k agissent comme $x \mapsto -x$).

Le plongement de Q dans le groupe $\mathbb{H}^\times$ des quaternions non nuls donné par $t \mapsto -1$, $s_i \mapsto i$, $s_j \mapsto j$ et $s_k \mapsto k$ fait de $W = \mathbb{H}$ une représentation de dimension 4 de Q. Cette représentation est irréductible : en effet, un sous-espace de $W = \mathbb{H}$ qui serait laissé stable par Q serait stable par multiplication par tout élément de $\mathbb{H}$ (puisque i, j, k l'engendrent comme algèbre), mais comme $\mathbb{H}$ est une algèbre à division (pour tout $q \in \mathbb{H} \setminus \{0\}$ il existe $q' \in \mathbb{H} \setminus \{0\}$ tel que $qq' = 1$), ce sous-espace est nécessairement soit 0 soit W tout entier.

On a donc déterminé un morphisme φ de $\mathbb{R}[Q]$ vers $\mathbb{R} \times \mathbb{R} \times \mathbb{R} \times \mathbb{R} \times \mathbb{H}$, envoyant un élément $a \in \mathbb{R}[Q]$ sur son action sur les représentations U, V_i, V_j, V_k et W respectivement (la première composante envoie chaque élément de Q sur 1, la seconde envoie $1, t, s_i, ts_i$ sur 1 et s_j, s_k, ts_j, ts_k sur -1, la troisième et la quatrième sont analogues, et la dernière envoie 1 sur 1, t sur -1, s_i sur i, s_j sur j et s_k sur k).

Le plus facile est de vérifier directement la surjectivité de φ : l'élément $\frac{1}{8}(1+s_i+s_j+s_k+t+ts_i+ts_j+ts_k)$ a pour image $(1,0,0,0,0)$, l'élément $\frac{1}{8}(1+s_i-s_j-s_k+t+ts_i-ts_j-ts_k)$ a pour image $(0,1,0,0,0)$, l'élément $\frac{1}{2}(1-t)$ a pour image $(0,0,0,0,1)$ et l'élément $\frac{1}{2}(s_i - ts_i)$ a pour image $(0,0,0,0,i)$, tout ceci (ainsi que les éléments analogues pour j et k au lieu de i) attestant de la surjectivité de φ.

([1]) C'est-à-dire (voir exercice 4 de la feuille n°2) l'algèbre de dimension 4 sur $\mathbb{R}$ engendrée par les trois éléments i, j, k soumis aux relations $i^2 = j^2 = k^2 = ijk = -1$. Il s'agit d'une algèbre à divisions (« corps gauche »), i.e., tout élément non nul de $\mathbb{H}$ admet un inverse.

L'injectivité de φ résulte de sa surjectivité par égalité des dimensions. On a donc $\mathbb{R}[Q] \cong \mathbb{R} \times \mathbb{R} \times \mathbb{R} \times \mathbb{R} \times \mathbb{H}$.

On peut également préférer justifier la bijectivité de φ par un raisonnement plus abstrait[2] : l'algèbre semisimple $A = \mathbb{R}[Q]$ est le produit de ses composantes simples B_λ, à chacune desquelles correspond une représentation irréductible V_λ de A pour laquelle B_λ est l'image de A dans $\mathrm{End}_k(V_\lambda)$. Ici, en prenant pour V_λ les représentations irréductibles qu'on a trouvées, A se surjecte bien sur le produit des B_λ (qui sont respectivement quatre fois $\mathbb{R}$ et une fois $\mathbb{H}$).

Comme manifestement $\mathbb{C}[Q] \cong \mathbb{R}[Q] \otimes_{\mathbb{R}} \mathbb{C}$, on peut en déduire $\mathbb{C}[Q] \cong \mathbb{C} \times \mathbb{C} \times \mathbb{C} \times \mathbb{C} \times \mathbb{M}_2(\mathbb{C})$ où la dernière composante de l'isomorphisme $\varphi_{\mathbb{C}}$ en question envoie $1, s_i, s_j, s_k, t, ts_i, ts_j, ts_k$ respectivement sur les matrices $1, \sigma_i, \sigma_j, \sigma_k, -1, -\sigma_i, -\sigma_j, -\sigma_k$ où on a posé $\sigma_i = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}$, $\sigma_j = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ et $\sigma_k = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}$. Pour ce qui est des représentations complexes de Q, on a les représentations $U_{\mathbb{C}}$ (triviale), $V_{i,\mathbb{C}}$, $V_{j,\mathbb{C}}$ et $V_{k,\mathbb{C}}$ obtenues par tensorisation de U, V_i, V_j et V_k respectivement avec $\mathbb{C}$ (et exactement analogues), et une représentation $\tilde{W}$ de dimension 2 donnée par les matrices $\sigma_i, \sigma_j, \sigma_k$ définies ci-dessus : la représentation réelle irréductible W, complexifiée en $W \otimes_{\mathbb{R}} \mathbb{C}$, devient réductible comme $W \otimes_{\mathbb{R}} \mathbb{C} \cong \tilde{W} \oplus \tilde{W}$, l'isomorphisme envoyant $1 \in \mathbb{H}$ sur le couple des deux vecteurs colonne $\begin{pmatrix} 1 \\ 0 \end{pmatrix}$ et $\begin{pmatrix} 0 \\ 1 \end{pmatrix}$ dans $\tilde{W} \oplus \tilde{W}$. ✓

5. Soit C_n le groupe cyclique d'ordre n. Montrer que pour tout corps k on a $k[C_n] \cong k[t]/(t^n - 1)$: en particulier, que vaut $\mathbb{C}[C_n]$ et quelles sont les représentations irréductibles de C_n sur $\mathbb{C}$? et que vaut $\mathbb{Q}[C_n]$ et quelles sont les représentations irréductibles de C_n sur $\mathbb{Q}$?

Corrigé. Soit σ un générateur de C_n. Le morphisme $\psi\colon k[t] \to k[C_n]$ envoyant t sur σ (ce qui le définit uniquement) passe au quotient à $k[t]/(t^n - 1)$ puisque $\sigma^n = 1$ dans C_n (donc dans $k[C_n]$). Le morphisme $\bar{\psi}\colon k[t]/(t^n - 1) \to k[C_n]$ ainsi défini est bijectif car il envoie la k-base de $k[t]/(t^n - 1)$ formée des classes des t^k pour $0 \leq k < n$ sur la k-base de $k[C_n]$ formée des σ^k.

Lorsque $k = \mathbb{C}$ (ou du moins contient une racine primitive n-ième de l'unité, sous-entendu n non multiple de la caractéristique de k) alors $t^n - 1$ se factorise comme $\prod_{\ell=0}^{n-1}(t - \zeta^\ell)$ avec $\zeta = e^{2i\pi/n}$ racine primitive n-ième de l'unité, et alors $\mathbb{C}[C_n] \cong \mathbb{C}[t]/(t^n - 1) \cong \prod_{\ell=0}^{n-1} \mathbb{C}$ où l'isomorphisme $\mathbb{C}[t]/(t^n - 1) \cong \prod_{\ell=0}^{n-1} \mathbb{C}$ (résultant du théorème chinois, si l'on veut) envoie t sur la famille des $(1, \zeta, \ldots, \zeta^{n-1})$. Autrement dit, les représentations de C_n sur $\mathbb{C}$ sont les V_ℓ, toutes de dimension 1, où σ agit sur V_ℓ par multiplication par ζ^ℓ (remarquer que V_0 est la représentation triviale).

Lorsque $k = \mathbb{Q}$, alors $t^n - 1$ se factorise comme $\prod_{d|n} \Phi_d(t)$ avec Φ_d le d-ième polynôme cyclotomique, et alors $\mathbb{Q}[C_n] \cong \mathbb{Q}[t]/(t^n - 1) \cong \prod_{d|n} \mathbb{Q}[\zeta_d]$ où $\mathbb{Q}[\zeta_d]$ est l'extension de corps de degré d de $\mathbb{Q}$ obtenue en y rajoutant une racine primitive d-ième de l'unité, ζ_d. Autrement dit, les représentations de C_n sur $\mathbb{Q}$ sont les U_d, de dimension $\varphi(d)$, où U_d est le $\mathbb{Q}$-espace vectriel $\mathbb{Q}[\zeta_d]$ sur lequel σ agit par multiplication par ζ_d. ✓

(2) Noter cependant qu'on utilise ici la théorie des algèbres semisimples sur un corps, à savoir $\mathbb{R}$, qui n'est pas algébriquement clos : une $\mathbb{R}$-algèbre (de dimension finie) simple est un anneau de matrices sur une algèbre à divisions sur $\mathbb{R}$, laquelle peut être $\mathbb{R}$ lui-même ou bien $\mathbb{C}$ ou $\mathbb{H}$.