CORRIGÉ DE L'EXAMEN PARTIEL DU 4 NOVEMBRE 2008

Exercice I — Soit k un corps et soit $n \geqslant 1$ un nombre entier naturel. On considère un élément *non nul* a de k.

1. Étant donnée une k-algèbre R, on désigne par $\mathrm{G}(\mathrm{R})$ le groupe multiplicatif des éléments inversibles de l'anneau $\mathrm{R}[\mathrm{T}]/(\mathrm{T}^2-a)$. Tout homomorphisme de k-algèbres $f : \mathrm{R} \to \mathrm{R}'$ induit naturellement un homomorphisme d'anneaux $\mathrm{R}[\mathrm{T}]/(\mathrm{T}^2-a) \to \mathrm{R}'[\mathrm{T}]/(\mathrm{T}^2-a)$, lequel donne à son tour naissance à un homomorphisme de groupes $\mathrm{G}(f) : \mathrm{G}(\mathrm{R}) \to \mathrm{G}(\mathrm{R}')$. On a clairement $\mathrm{G}(\mathrm{id}_\mathrm{R}) = \mathrm{id}_{\mathrm{G}(\mathrm{R})}$ et $\mathrm{G}(f\circ g) = \mathrm{G}(f)\circ \mathrm{G}(g)$, donc la correspondance

$$\mathrm{R} \mapsto \mathrm{G}(\mathrm{R}), \quad (\ \mathrm{R} \xrightarrow{f} \mathrm{R}'\ ) \mapsto (\ \mathrm{G}(\mathrm{R}) \xrightarrow{\mathrm{G}(f)} \mathrm{G}(\mathrm{R}')\ )$$

est un foncteur de la catégorie des k-algèbres dans celle des groupes.

Soit R une k-algèbre. Désignant par t la classe de T, $\mathrm{R}[\mathrm{T}]/(\mathrm{T}^2-a)$ est un R-module libre de base $(1,t)$ et la multiplication est donnée par l'identité $(u+tv)(u'+tv') = (uu'+avv') + (uv'+u'v)t$. La R-algèbre $\mathrm{R}[\mathrm{T}]/(\mathrm{T}^2-a)$ admet par ailleurs un automorphisme naturel σ, défini par $\sigma(u+tv) = u - tv$, et on a

$$(u+tv)\sigma(u+tv) = (u+tv)(u-tv) = u^2 - av^2$$

pour tous $u, v \in \mathrm{R}$.

Si un élément $x = u + tv$ de $\mathrm{R}[\mathrm{T}]/(\mathrm{T}^2-a)$ est inversible, il en est de même pour $\sigma(x)$ et l'identité ci-dessus montre qu'alors $u^2 - av^2$ est un élément inversible de R. Réciproquement, si $x = u+tv$ est un élément de $\mathrm{R}[\mathrm{T}]/(\mathrm{T}^2-a)$ tel que $x\sigma(x) = u^2 - av^2 \in \mathrm{R}^\times$, alors x est inversible, d'inverse $(x\sigma(x))^{-1}\sigma(x)$.

On a ainsi des bijections fonctorielles

$$\begin{array}{rcl} \mathrm{G}(\mathrm{R}) & \simeq & \{(u,v) \in \mathrm{R}^2 \mid u^2 - av^2 \in \mathrm{R}^\times\} \\ & \simeq & \{(u,v,w) \in \mathrm{R}\times\mathrm{R}\times\mathrm{R} \mid (u^2-av^2)w = 1\} \\ & \simeq & \mathrm{Hom}_{\mathbf{Alg}_k}(k[\mathrm{U},\mathrm{V},\mathrm{W}]/((\mathrm{U}^2 - a\mathrm{V}^2)\mathrm{W}-1), \mathrm{R}) \end{array}$$

qui montrent que le foncteur en ensembles G est représenté par la k-algèbre de type fini $k[\mathrm{U},\mathrm{V},\mathrm{W}]/((\mathrm{U}^2 - a\mathrm{V}^2)\mathrm{W}-1)$. Le foncteur G est donc un groupe algébrique sur k.

2. Supposons que $a = \alpha^2$ soit un carré dans k et que le corps k soit de caractéristique différente de 2. Sous ces hypothèse, 2α est inversible dans k, donc dans toute k-algèbre R, et les idéaux $(\mathrm{T}-\alpha), (\mathrm{T}+\alpha)$ de $\mathrm{R}[\mathrm{T}]$ sont étrangers en vertu de l'identité $\frac{1}{2\alpha}(\mathrm{T}+\alpha) - \frac{1}{2\alpha}(\mathrm{T}-\alpha) = 1$. Comme $\mathrm{T}^2 - a = (\mathrm{T}-\alpha)(\mathrm{T}+\alpha)$, l'application

$$\mathrm{R}[\mathrm{T}]/(\mathrm{T}^2-a) \xrightarrow{\sim} \mathrm{R}[\mathrm{T}]/(\mathrm{T}-\alpha)\times \mathrm{R}[\mathrm{T}]/(\mathrm{T}+\alpha)\ , \quad f \bmod (T^2-a) \mapsto (f \bmod (\mathrm{T}-\alpha), f \bmod (\mathrm{T}+\alpha))$$

est un isomorphisme d'anneaux en vertu du théorème chinois des restes. Cet isomorphismes est fonctoriel R. En composant par l'isomorphisme canonique

$$\mathrm{R}[\mathrm{T}]/(\mathrm{T}-\alpha)\times \mathrm{R}[\mathrm{T}]/(\mathrm{T}+\alpha) \to \mathrm{R}\times\mathrm{R}, \ (f \bmod (T-\alpha), f \bmod (\mathrm{T}+\alpha)) \mapsto (f(\alpha), f(-\alpha)),$$

on obtient un isomorphisme de k-algèbres, fonctoriel en R, entre $\mathrm{R}[\mathrm{T}]/(\mathrm{T}^2-a)$ et $\mathrm{R}\times\mathrm{R}$. Comme $(\mathrm{R}\times\mathrm{R})^\times = \mathrm{R}^\times \times \mathrm{R}^\times$, le groupe G est isomorphe au groupe produit $\mathbb{G}_\mathrm{m}\times\mathbb{G}_\mathrm{m}$.

3. Supposons que $a = \alpha^2$ soit un carré dans k et que le corps k soit de caractéristique 2. Sous ces hypothèse, $\mathrm{T}^2 - a = \mathrm{T}^2 - \alpha^2 = (\mathrm{T} - \alpha)^2$ et, posant $\mathrm{X} = \mathrm{T} - \alpha$, on obtient un isomorphisme fonctoriel de R-algèbres $\mathrm{R}[\mathrm{T}]/(\mathrm{T}^2 - a) \simeq \mathrm{R}[\mathrm{X}]/(\mathrm{X}^2)$.

Désignant par x la classe de X, $\mathrm{R}[\mathrm{X}]/(\mathrm{X}^2)$ est le R-module libre $\mathrm{R} \oplus \mathrm{R}x$ muni de la multiplication $(u+vx)(u'+v'x) = uu' + (uv' + u'v)x$. Un élément $u + vx$ est inversible si et seulement si $u \in \mathrm{R}^\times$: la condition est évidemment nécessaire, et elle est suffisante car $u^{-2}(u+vx)(u-vx) = 1$. Ainsi, $(\mathrm{R}[\mathrm{T}]/(\mathrm{T}^2))^\times$ est le groupe d'ensemble sous-jacent $\mathrm{R}^\times \times \mathrm{R}$ et de loi de multiplication

$$(u,v) \bullet (u',v') = (uu', uv' + u'v).$$

L'application $\mathrm{R}^\times \times \mathrm{R} \to \mathrm{R}^\times \times \mathrm{R}, \quad (u,v) \mapsto (u, u^{-1}v)$ est une bijection transformant la loi de groupe $\bullet$ en la loi standard $(u,v)(u',v') = (uu', v+v')$. Comme cette application est fonctorielle en R, on en déduit finalement que le groupe G est isomorphe au groupe $\mathbb{G}_{\mathrm{m}} \times \mathbb{G}_{\mathrm{a}}$.

Exercice II — ***Première partie*** — **1.** Pour toute k-algèbre R, on identifie les ensembles $\mathrm{GL}_n(\mathrm{R})$ et $\mathrm{Hom}_{\mathbf{Alg}_k}(\mathrm{A},\mathrm{R})$ en associant à une matrice $s \in \mathrm{GL}_n(\mathrm{R})$ l'unique homomorphisme de k-algèbres $\underline{s} : \mathrm{A} \to \mathrm{R}$ tel que

$$\underline{s}(\mathrm{X}_{ij}) = s_{ij} \quad \text{et} \quad \underline{s}(\mathrm{T}) = \det(s)^{-1}.$$

Lorsque $\mathrm{R} = k$, cette bijection est reliée aux conventions adoptées dans l'énoncé : étant donné $s \in \mathrm{GL}_n(k)$,

$$\underline{s}(\mathrm{X}_{ij}) = s_{ij} = \overline{X}_{ij}(s) \quad \text{et} \quad \underline{s}(\mathrm{T}) = \det(s)^{-1} = \overline{\mathrm{T}}(s)$$

et donc

$$\underline{s}(f) = \overline{f}(s)$$

pour tout $f \in \mathrm{A}$.

Étant donnés deux éléments s,t de $\mathrm{GL}_n(\mathrm{R})$, leur produit st dans $\mathrm{GL}_n(\mathrm{R})$ correspond à l'homomorphisme de k-algèbres

$$\overline{st} : \ \mathrm{A} \xrightarrow{\Delta} \mathrm{A} \xrightarrow{(\underline{s},\underline{t})} \mathrm{R} \ ,$$

où $(\underline{s},\underline{t})$ désigne l'unique homomorphisme de k-algèbres $\mathrm{A} \otimes_k \mathrm{A} \to \mathrm{R}$ tel que $(\underline{s},\underline{t})(a \otimes 1) = \underline{s}(a)$ et $(\underline{s},\underline{t})(1 \otimes a) = \underline{t}(a)$.

Considérons finalement un élément f de A et écrivons $\Delta(f)$ sous la forme $\Delta(f) = \sum_{i \in \mathrm{I}} g_i \otimes h_i$. On a

$$\underline{st}(f) = ((\underline{s},\underline{t}) \circ \Delta)(f) = (\underline{s},\underline{t})\Delta(f) = (\underline{s},\underline{t}) \left(\sum_{i \in \mathrm{I}} (g_i \otimes 1)(1 \otimes h_i) \right) = \sum_{i \in \mathrm{I}} \underline{s}(g_i)\underline{t}(h_i)$$

et, si $\mathrm{R} = k$, cette identité se réécrit de manière équivalente sous la forme

$$\overline{f}(st) = \sum_{i \in \mathrm{I}} \overline{g_i}(s)\overline{h_i}(t).$$

2. Soit B la k-bigèbre du groupe algébrique G. Identifiant les foncteurs GL_n et $\mathrm{Hom}_{\mathbf{Alg}_k}(\mathrm{A},\cdot)$ (resp. G et $\mathrm{Hom}_{\mathbf{Alg}_k}(\mathrm{B},\cdot)$), l'homomorphisme $i : \mathrm{G} \to \mathrm{GL}_n$ provient d'un homomorphisme de k-algèbres $i^* : \mathrm{A} \to \mathrm{B}$ *surjectif*. Considérons alors le diagramme commutatif

$$\begin{tikzcd}
\mathrm{G}(k) \arrow[r, "i_k"] \arrow[d, "\simeq"'] & \mathrm{GL}_n(k) \arrow[d, "\simeq"] \\
\mathrm{Hom}_{\mathbf{Alg}_k}(\mathrm{B},k) \arrow[r, "(-)\circ i^*"'] & \mathrm{Hom}_{\mathbf{Alg}_k}(\mathrm{A},k)
\end{tikzcd}$$

La flèche horizontale inférieure étant l'injection d'image $\{v \in \mathrm{Hom}_{\mathbf{Alg}_k}(\mathrm{A},k) \mid v(\mathfrak{I}) = 0\}$, la flèche horizontale supérieure induit une bijection entre $\mathrm{G}(k)$ et le sous-ensemble fermé

$$\{s \in \mathrm{GL}_n(k) \mid \overline{f}(s) = 0 \text{ pour tout } f \in \mathfrak{I}\}$$

de $\mathrm{GL}_n(k)$. Noter que ce sous-ensemble de $\mathrm{GL}_n(k)$ est un fait un sous-groupe puisque i_k est un homomorphisme de groupes.

3. Pour tout idéal $\mathfrak{I}$ de A, la bijection $\left(\mathrm{GL}_n(k) \xrightarrow{\sim} \mathrm{Hom}_{\mathbf{Alg}_k}(\mathrm{A},k),\ s \mapsto \underline{s}\right)$ introduite à la question 1 identifie les sous-ensembles $\mathrm{V}(\mathfrak{I}) = \{s \in \mathrm{GL}_n(k) \mid \overline{f}(s) = 0 \text{ pour tout } f \in \mathfrak{I}\}$ et $\mathrm{Hom}_{\mathbf{Alg}_k}(\mathrm{A}/\mathfrak{I},k)$. Il nous faut donc vérifier l'identité $\Gamma = \mathrm{V}(\mathrm{J})$.

L'inclusion $\Gamma \subset \mathrm{V}(\mathrm{J})$ est évidente : pour tout $\gamma \in \Gamma$ et tout $f \in \mathrm{J}$, $\overline{f}(\gamma) = 0$ et donc $\gamma \in \mathrm{V}(\mathrm{J})$. Pour établir l'inclusion réciproque, on commence par remarquer que l'on a une inclusion $\mathrm{I} \subset \mathrm{J}$ car $\overline{f}_{|\Gamma} = 0$ pour tout $f \in \mathrm{I}$; quel que soit alors l'élément s de $\mathrm{V}(\mathrm{J})$, $\overline{f}(s) = 0$ pour tout $f \in \mathrm{I}$ et donc $s \in \Gamma$. On obtient ainsi l'identité $\Gamma = \mathrm{V}(\mathrm{J})$.

4. On dispose pour toute k-algèbre C de bijections canoniques

$$\mathrm{Hom}_{\mathbf{Alg}_k}(\mathrm{B} \otimes_k \mathrm{B},\mathrm{C}) \cong \mathrm{Hom}_{\mathbf{Alg}_k}(\mathrm{B},\mathrm{C})^2 \cong \{(u,v) \in \mathrm{Hom}_{\mathbf{Alg}_k}(\mathrm{A},\mathrm{C})^2 \mid u(\mathrm{J}) = v(\mathrm{J}) = 0\}.$$

La bijection canonique

$$\mathrm{Hom}_{\mathbf{Alg}_k}(\mathrm{A},\mathrm{C})^2 \cong \mathrm{Hom}_{\mathbf{Alg}_k}(\mathrm{A} \otimes_k \mathrm{A},\mathrm{C}),$$

faisant correspondre à tout couple $(u,v) \in \mathrm{Hom}_{\mathbf{Alg}_k}(\mathrm{A},\mathrm{C})^2$ l'unique homomorphisme de k-algèbres $w : \mathrm{A} \otimes_k \mathrm{A} \to \mathrm{C}$ tel que $w(a \otimes 1) = u(a)$ et $w(1 \otimes a) = v(a)$, induit une bijection

$$\begin{aligned}\mathrm{Hom}_{\mathbf{Alg}_k}(\mathrm{A},\mathrm{C})^2 \mid u(\mathrm{J}) = v(\mathrm{J}) = 0\} &\cong \{w \in \mathrm{Hom}_{\mathbf{Alg}_k}(\mathrm{A},\mathrm{C}) \mid w(\mathrm{J} \otimes_k \mathrm{A}) = w(\mathrm{A} \otimes_k \mathrm{J}) = 0\}\\ &\cong \mathrm{Hom}_{\mathbf{Alg}_k}(\mathrm{A} \otimes_k \mathrm{A}/(\mathrm{J} \otimes_k \mathrm{A} + \mathrm{A} \otimes_k \mathrm{J}),\mathrm{C}).\end{aligned}$$

En vertu du lemme de Yoneda, la k-algèbre $\mathrm{B} \otimes_k \mathrm{B}$ est ainsi canoniquement isomorphe au quotient de $\mathrm{A} \otimes_k \mathrm{A}$ par l'idéal $\mathrm{J} \otimes_k \mathrm{A} + \mathrm{A} \otimes_k \mathrm{J}$. (Si l'on explicite toutes les bijections ci-dessus, on constate que cet isomomorphisme canonique n'est autre que l'homomorphisme $p \otimes p : \mathrm{A} \otimes_k \mathrm{A} \to \mathrm{B} \otimes_k \mathrm{B}$.)

5. Soit f un élément de A tel que $\Delta(f) \in \mathrm{J} \otimes_k \mathrm{A} + \mathrm{A} \otimes_k \mathrm{J}$. On dispose par hypothèse d'une écriture de $\Delta(f)$ sous la forme $\Delta(f) = \sum_\alpha g_\alpha \otimes h_\alpha$ avec $g_\alpha \in \mathrm{J}$ ou $h_\alpha \in \mathrm{J}$ pour tout α. En vertu de la question 1,

$$\overline{f}(st) = \sum_\alpha \overline{g_\alpha}(s)\overline{h_\alpha}(t)$$

pour tous $s,t \in \mathrm{GL}_n(k)$; appliquant cela avec $s \in \Gamma$ et $t = e$ l'élément neutre de Γ, on en déduit

$$\overline{f}(s) = \overline{f}(se) = \sum_\alpha \overline{g_\alpha}(s)\overline{h_\alpha}(e) = 0$$

puisque $g_\alpha(s) = 0$ ou $h_\alpha(e) = 0$ pour tout α. Ainsi, $\overline{f}$ s'annule identiquement sur Γ.

6. L'unicité de $\overline{\Delta}$ est claire : si deux homomorphismes $u,v : \mathrm{B} \to \mathrm{B} \otimes_k \mathrm{B}$ sont tels que $u \circ p = v \circ p$, alors $u = v$ car p est une application surjective. Pour établir l'existence de $\overline{\Delta}$, il faut vérifier que l'application $(p \otimes p) \circ \Delta$ s'annule identiquement sur l'idéal J ou, de manière équivalente, que $\Delta(\mathrm{J})$ est contenu dans $\mathrm{J} \otimes_k \mathrm{A} + \mathrm{A} \otimes_k \mathrm{J}$.

Soit donc $f \in \mathrm{J}$ et considérons une base $(a_\lambda)_{\lambda \in \Lambda' \cup \Lambda''}$ de A comme k-espace vectoriel telle que $(a_\lambda)_{\lambda \in \Lambda'}$ soit une base du sous-k-espace vectoriel J. Comme $(1 \otimes a_\lambda)_{\lambda \in \Lambda' \cup \Lambda''}$ est une base de $\mathrm{A} \otimes_k \mathrm{A}$, $\Delta(f)$ s'écrit de manière unique sous la forme

$$\Delta(f) = \sum_{\lambda \in \Lambda' \cup \Lambda''} g_\lambda \otimes a_\lambda$$

avec $g_\lambda \in \mathrm{A}$. Quel que soit $s \in \Gamma$, l'élément

$$\sum_{\lambda \in \Lambda' \cup \Lambda''} g_\lambda(s) a_\lambda$$

de A s'annule identiquement sur Γ en vertu de la question 1, donc appartient à J par définition de cet idéal. On en déduit que l'on a $h_\lambda(s) = 0$ pour tout $\lambda \in \Lambda''$ et tout $s \in \Gamma$, d'où $h_\lambda \in \mathrm{J}$ pour tout $\lambda \in \Lambda''$. Ceci prouve que $\Delta(f)$ appartient à l'idéal $\mathrm{J} \otimes_k \mathrm{A} + \mathrm{A} \otimes_k \mathrm{J}$ de $\mathrm{A} \otimes_k \mathrm{A}$, ce qu'il fallait démontrer.

7. En raisonnant comme pour la question 1, on vérifie que l'on a $\overline{\iota(f)}(s) = \overline{f}(s^{-1})$ pour tous $f \in \mathrm{A}$, $s \in \mathrm{GL}_n(k)$. Appliquant ceci avec $f \in \mathrm{J}$ et $s \in \Gamma$, on obtient $\overline{\iota(f)}(s) = 0$ puisque $s^{-1} \in \Gamma$ et donc $\iota(f) \in \mathrm{J}$. L'application $p \circ \iota : \mathrm{A} \to \mathrm{B}$ se factorise donc à travers la projection p et, p étant surjective, il existe un unique homomorphisme $\overline{\iota} : \mathrm{B} \to \mathrm{B}$ tel que le diagramme

$$\begin{tikzcd}
\mathrm{A} \arrow[r, "\iota"] \arrow[d, "p"'] & \mathrm{A} \arrow[d, "p"] \\
\mathrm{B} \arrow[r, "\overline{\iota}"'] & \mathrm{B}
\end{tikzcd}$$

soit commutatif.

Enfin, comme $e \in \Gamma$, on a $e^*(f) = \overline{f}(e) = 0$ pour tout $f \in \mathrm{J}$. Il existe donc un unique homomorphisme $\overline{e}^* : \mathrm{B} \to k$ tel que $e^* = \overline{e}^* \circ p$.

8. Montrons que l'homomorphisme $\overline{\Delta}$ est coassociatif. On considère pour cela le diagramme

$$\begin{tikzcd}
\mathrm{A} \arrow[rrr, "\Delta"] \arrow[dr, "p"] \arrow[ddd, "\Delta"'] & & & \mathrm{A} \otimes_k \mathrm{A} \arrow[dl, "p\otimes p"'] \arrow[ddd, "\mathrm{id}_\mathrm{A}\otimes\Delta"] \\
& \mathrm{B} \arrow[r, "\overline{\Delta}"] \arrow[d, "\overline{\Delta}"'] & \mathrm{B} \otimes_k \mathrm{B} \arrow[d, "\mathrm{id}_\mathrm{B}\otimes\overline{\Delta}"] & \\
& \mathrm{B} \otimes_k \mathrm{B} \arrow[r, "\overline{\Delta}\otimes\mathrm{id}_\mathrm{B}"'] & \mathrm{B} \otimes_k \mathrm{B} \otimes_k \mathrm{B} & \\
\mathrm{A} \otimes_k \mathrm{A} \arrow[ur, "p\otimes p"] \arrow[rrr, "\Delta\otimes\mathrm{id}_\mathrm{A}"'] & & & \mathrm{A} \otimes_k \mathrm{A} \otimes_k \mathrm{A} \arrow[ul, "p\otimes p\otimes p"']
\end{tikzcd}$$

Le carré extérieur est commutatif puisque $(\mathrm{A}, \Delta, e^*, \iota)$ est une bigèbre tandis que chacun des quatre trapèzes est commutatif en vertu de la question 6. On en déduit facilement l'identité $(\mathrm{id}_\mathrm{B} \otimes \overline{\Delta}) \circ p = (\overline{\Delta} \circ \mathrm{id}_\mathrm{B}) \circ p$, puis

$$\mathrm{id}_\mathrm{B} \otimes \overline{\Delta} = \overline{\Delta} \circ \mathrm{id}_\mathrm{B}$$

car p est une application *surjective*.

Le raisonnement que l'on vient de faire s'applique à chacun des trois autres diagrammes à considérer (counité à gauche et à droite, coinversion).

9. La k-algèbre $\mathrm{B} = \mathrm{A}/\mathrm{J}$ est de type fini puisque quotient de la k-algèbre de type fini A. Utilisant la structure de bigèbre sur B que l'on vient de construire, on définit un groupe algébrique G muni d'un homomorphisme $i : \mathrm{G} \to \mathrm{GL}_n$ tel que $i^* = p$. Enfin, l'application i_k induit un isomorphisme entre $\mathrm{G}(k) = \mathrm{Hom}_{\mathbf{Alg}_k}(\mathrm{B}, k)$ et le sous-groupe fermé $\Gamma \subset \mathrm{GL}_n(k)$ en vertu de la question 3.

***Seconde partie* — 10.** Quel que soit l'ensemble E, l'application canonique

$$\rho : \mathrm{E} \to \mathrm{Hom}_{\mathbf{Alg}_k}(\mathscr{F}(\mathrm{E}, k), k), \;\; e \mapsto (\varphi \mapsto \varphi(e))$$

est injective. Considérons en effet pour tout $e \in \mathrm{E}$ la fonction caractéristique $\mathbf{1}_e : \mathrm{E} \to k$ de $\{e\}$:

$$\mathbf{1}_e(e') = \begin{cases} 1 & \text{si } e' = e \\ 0 & \text{si } e' \neq e \end{cases}$$

Si $e \neq e'$, alors $\mathbf{1}_e(e) = 1 \neq \mathbf{1}'_e(e)$ et donc e et e' définissent des éléments distincts de $\mathrm{Hom}_{\mathbf{Alg}_k}(\mathscr{F}(\mathrm{E}, k), k)$.

Lorsque l'ensemble E est supposé fini, l'application ρ est surjective. On a en effet

$$1 = \sum_{e \in \mathrm{E}} \mathbf{1}_e \quad \text{et} \quad \mathbf{1}_e \mathbf{1}'_e = \begin{cases} \mathbf{1}_e & \text{si } e' = e \\ 0 & \text{sinon} \end{cases}$$

donc, pour tout homomorphisme de k-algèbre $u : \mathscr{F}(\mathrm{E}, k) \to k$,

$$1 = \sum_{e \in \mathrm{E}} u(\mathbf{1}_e) \quad \text{et} \quad u(\mathbf{1}_e) u(\mathbf{1}'_e) = \begin{cases} u(\mathbf{1}_e) & \text{si } e' = e \\ 0 & \text{sinon} \end{cases}.$$

L'identité $u(\mathbf{1}_e)^2 = u(\mathbf{1}_e)$ équivaut à $u(\mathbf{1}_e)(u(\mathbf{1}_e) - 1) = 0$ et donc implique $u(\mathbf{1}_e) = 0$ ou $u(\mathbf{1}_e) = 1$ puisque k est un corps. Vu la relation $1 = \sum_{e \in \mathrm{E}} u(\mathbf{1}_e)$, il existe au moins un $e \in \mathrm{E}$ tel que $u(\mathbf{1}_e) = 1$, et on a alors $u(\mathbf{1}_{e'}) = 0$ pour tout $e' \in \mathrm{E} - \{e\}$ puisqu'alors $u(\mathbf{1}_e) u(\mathbf{1}'_e) = 0$.

On obtient finalement $\mathbf{1}'_e(u) = \mathbf{1}'_e(e)$ pour tout $e' \in \mathrm{E}$, donc $u(\varphi) = \varphi(e)$ car les fonctions caractéristiques forment une base du k-espace vectoriel $\mathscr{F}(\mathrm{E}, k)$.

11. Les deux homomorphismes naturels de k-algèbres $\mathscr{F}(\mathrm{E}, k) \to \mathscr{F}(\mathrm{E} \times \mathrm{E}, k)$ respectivement définis par

$$\varphi \mapsto ((e, e') \mapsto \varphi(e)) \quad \text{et} \quad \varphi \mapsto ((e, e') \mapsto \varphi(e'))$$

donnent naissance à un homomorphisme canonique

$$\mathscr{F}(\mathrm{E}, k) \otimes_k \mathscr{F}(\mathrm{E}, k) \to \mathscr{F}(\mathrm{E} \times \mathrm{E}, k), \quad \sum_\alpha \varphi_\alpha \psi_\alpha \mapsto \left((e, e') \mapsto \sum_\alpha \varphi_\alpha(e) \psi_\alpha(e') \right)$$

qui envoie la base $(\mathbf{1}_e \otimes \mathbf{1}_{e'})_{(e,e') \in \mathrm{E} \times \mathrm{E}}$ de $\mathscr{F}(\mathrm{E}, k) \otimes_k \mathscr{F}(\mathrm{E}, k)$ sur la base $(\mathbf{1}_{(e,e')})_{(e,e') \in \mathrm{E} \times \mathrm{E}}$ de $\mathscr{F}(\mathrm{E} \times \mathrm{E}, k)$; il s'agit donc d'un isomorphisme.

12. Étant donnés deux éléments distincts s et t dans $\mathrm{GL}_n(k)$, il existe un élément f de A tel que $\overline{f}(s) = 1$ et $\overline{f}(t) = 0$: en effet, si (i, j) est un indice tel que $s_{ij} \neq t_{ij}$, il suffit de considérer le polynôme $f = (s_{ij} - t_{ij})^{-1}(\mathrm{X}_{ij} - t_{ij})$.

Si maintenant E est un sous-ensemble fini de $\mathrm{GL}_n(k)$, on choisit pour tout couple $(e, e') \in \mathrm{E} \times \mathrm{E}$ un élément $f_{(e,e')}$ de A tel que $f_{(e,e')}(e) = 1$ et $f_{(e,e')}(e') = 0$. On pose $f_e = \prod_{e' \in \mathrm{E} - \{e\}} f_{(e,e')} \in \mathrm{A}$ et on constate que la restriction de f_e à E est la fonction caractéristique $\mathbf{1}_e$. Comme les fonctions caractéristiquent engendrent le k-espace vectoriel $\mathscr{F}(\mathrm{E}, k)$, la surjectivité de l'application

$$\mathrm{A} \to \mathscr{F}(\mathrm{E}, k), \quad f \mapsto f_{|\mathrm{E}}$$

en découle immédiatement.

13. Considérons encore un sous-ensemble fini E de $\mathrm{GL}_n(k)$ et soit I l'idéal noyau de l'homomorphisme de k-algèbres $\mathrm{A} \to \mathscr{F}(\mathrm{E}, k), \quad f \mapsto \overline{f}_{|\mathrm{E}}$. L'inclusion

$$\mathrm{E} \subset \{s \in \mathrm{GL}_n(k) \mid \overline{f}(s) = 0 \text{ pour tout } f \in \mathrm{I}\}$$

est évidente. D'autre part, tout élément s de $\mathrm{GL}_n(k)$ définit un homomorphisme de k-algèbres $\underline{s} : \mathrm{A} \to k, \ f \mapsto \overline{f}(s)$. Si $\overline{f}(s) = 0$ pour tout $f \in \mathrm{I}$, alors $\underline{s}$ se factorise à travers la projection $\mathrm{A} \to \mathrm{A}/\mathrm{I} \cong \mathscr{F}(\mathrm{E}, k)$ et donc induit un homomorphisme de k-algèbres $\mathscr{F}(\mathrm{E}, k) \to k$. On invoque alors la question 10 pour obtenir un élément e de E tel que $\overline{f}(e) = \overline{f}(s)$ pour tout $f \in \mathrm{A}$, ce qui implique finalement $e = s$ (cf. argument de la question 10).

14. En faisant agir Γ sur lui-même par translation à gauche, on obtient un homomorphisme injectif $\Gamma \to \mathfrak{S}(\Gamma) \simeq \mathfrak{S}_n$, où $n = |\Gamma|$. On obtient par ailleurs un isomorphisme entre $\mathfrak{S}_n$ et un sous-groupe de $\mathrm{GL}_n(k)$ en considérant l'action suivante de $\mathfrak{S}_n$ sur la base canonique $(e_1, \ldots, e_n)$ de $\mathfrak{S}_n$:

$$\sigma \cdot e_i = e_{\sigma(i)}.$$

Le groupe Γ est par conséquent isomorphe à un sous-groupe de $\mathrm{GL}_n(k)$ avec $n = |\Gamma|$ et, en vertu de la question 9, on en déduit qu'il existe un groupe algébrique G sur k tel que $\mathrm{G}(k) \simeq \Gamma$.

15. Pour toute fonction $f \in \mathscr{F}(\Gamma, k)$, $\overline{\Delta}(f)$ est la fonction sur $\Gamma \times \Gamma$ obtenue en composant la multiplication $\Gamma \times \Gamma \to \Gamma$ par f et donc $\overline{\Delta}(f)(\gamma', \gamma'') = f(\gamma'\gamma'')$. Par suite,

$$\overline{\Delta}(\mathbf{1}_\gamma) = \sum_{\substack{(\gamma', \gamma'') \in \Gamma^2 \\ \gamma'\gamma'' = \gamma}} \mathbf{1}_{\gamma'} \otimes \mathbf{1}_{\gamma''}.$$

On obtient de même

$$\overline{e}^*(\mathbf{1}_\gamma) = \begin{cases} 1 & \text{si } \gamma = e \\ 0 & \text{sinon} \end{cases} \quad \text{et} \quad \overline{\iota}(\mathbf{1}_\gamma) = \mathbf{1}_{\gamma^{-1}}.$$

16. On observe que la structure de bigèbre obtenue à la question précédente ne dépend pas du choix d'un isomorphisme entre Γ et un sous-groupe de $\mathrm{GL}_n(k)$. Il est donc loisible de définir directement une structure de k-bigèbre sur $\mathscr{F}(\Gamma, k)$ en utilisant les identités ci-dessus, ce qui conduit à un groupe algébrique $\underline{\Gamma}$ sur k tel que $\underline{\Gamma}(k) \simeq \Gamma$.