Corrigé de l'examen du 1er mars 2016 (durée 3h)

Version du 3 mars : coquilles corrigées dans les solutions de 1.1 et 2.9 ; détails ajoutés dans la remarque 3.0 et les solutions de 3.2, 3.3, 3.5 et 3.6.

Exercice 1. — Soient k un corps, G le k-schéma en groupes $\mathrm{GL}_{2,k}$. On a une action naturelle de G sur l'algèbre de polynômes $k[X,Y]$, par automorphismes d'algèbre, définie comme suit : pour toute k-algèbre R et $g = \left(\begin{smallmatrix} a_0 & b_0 \\ c_0 & d_0 \end{smallmatrix}\right) \in G(R)$, on a dans $R[X,Y]$:

$$g^{-1}X = a_0X + b_0Y, \qquad g^{-1}Y = c_0X + d_0Y.$$

Soit H le stabilisateur dans G de l'élément XY.

(1) Écrire les équations définissant H. Soit A le quotient de $k[G] = k[a,b,c,d,(ad-bc)^{-1}]$ par l'idéal engendré par ces équations.

Solution : Pour tout g comme ci-dessus, on a :

$$g^{-1}XY = (g^{-1}X)(g^{-1}Y) = (a_0X + b_0Y)(c_0X + d_0Y) = a_0c_0X^2 + (a_0d_0 + b_0c_0)XY + b_0d_0Y^2.$$

Donc H est défini par les équations $ac = 0 = bd$ et $ad + bc = 1$. Remarquons que celles-ci entraînent $ab = ab(ad+bc) = a^2(bd) + b^2(ac) = 0$ et, de même, $cd = 0$.

(2) Déterminer dans A deux idempotents e, f non nuls tels que $e + f = 1$ et $ef = 0$. (Par abus, on notera encore a, b, c, d les images de a, b, c, d dans A.)

Solution : Comme $(ad)(bc) = (ac)(bd) = 0$, en multipliant l'égalité $ad + bc = 1$ par ad (resp. bc) on obtient que $e = ad$ et $f = bc$ sont des idempotents tels que $e + f = 1$ et $ef = 0$.

(3) Déterminer les composantes connexes de H et donner une équation définissant la composante neutre H^0.

Solution : Comme $e + f = 1$ et $ef = 0$, G est réunion disjointe des deux sous-schémas ouverts et fermés définis par les équations $f = 0$ et $e = 0$. Montrons que chaque d'eux est connexe. Dans $A/(f)$, les égalités $ad = 1$ et $ac = 0 = bd$ entraînent $c = 0 = b$, donc $A/(f) = k[a, a^{-1}]$. Ceci correspond au sous-groupe des matrices diagonales de déterminant 1, isomorphe à $\mathbb{G}_{m,k}$ donc connexe : c'est la composante connexe H^0.

D'autre part, dans $A/(e)$ les égalités $bc = 1$ et $ac = 0 = bd$ entraînent $a = 0 = d$, donc $A/(e) = k[c, c^{-1}]$. Ceci correspond au sous-schéma ouvert et fermé des matrices de la forme $\left(\begin{smallmatrix} 0 & s^{-1} \\ s & 0 \end{smallmatrix}\right)$, qui est connexe car isomorphe à $\mathbb{G}_{m,k}$ comme k-schéma. C'est la composante connexe de l'élément $\sigma = \left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right)$ de $G(k)$, et c'est l'image de H^0 par la translation, disons à gauche, définie par σ.

Corrigeons au passage une erreur faite dans le polycopié : si R est une k-algèbre ne contenant pas d'idempotents autres que 0 et 1 (i.e. telle que $\mathrm{Spec}(R)$ soit connexe) alors tout morphisme $\mathrm{Spec}(R) \to G$ est à valeurs dans l'une des composantes connexes, i.e. pour tout morphisme $\phi : A \to R$ l'un des idempotents $f = bc$ ou $e = ad$ s'envoie sur 0 (et l'autre sur 1), et donc $G(R)$ est la réunion des R-points $\left(\begin{smallmatrix} t & 0 \\ 0 & t^{-1} \end{smallmatrix}\right)$ et $\left(\begin{smallmatrix} 0 & s^{-1} \\ s & 0 \end{smallmatrix}\right)$, pour $t, s \in R^\times$. Mais ceci est faux si R contient un idempotent $x \neq 0, 1$ car alors, posant $y = 1 - x$, la matrice $\left(\begin{smallmatrix} x & y \\ y & x \end{smallmatrix}\right)$ appartient à $G(R)$.

(4) Quel est le k-schéma en groupes H^0 ?

Solution : On a vu plus haut que c'est $\mathbb{G}_{m,k}$.

(5) Le k-schéma en groupes H est-il géométriquement réduit ?

Solution : Oui, car d'après la caractérisation en termes de l'algèbre de Lie, ceci ne dépend que de H^0, et $\mathbb{G}_{m,k}$ est géométriquement réduit (i.e. $\overline{k}[a, a^{-1}]$ est réduite). On peut aussi dire directement que $A \otimes \overline{k} \simeq \overline{k}[a, a^{-1}] \oplus \overline{k}[c, c^{-1}]$ est réduite.)

(6) Notons $\det_H$ la restriction à H du déterminant (i.e. l'image dans A de l'élément dét de $k[G]$). Exprimer $\det_H$ en fonction de l'un des idempotents de la question (2), puis calculer $\det_H^2$.

Solution : $\det_H = ad - bc = ad + bc - 2bc = 1 - 2f$. Comme $f^2 = f$ on obtient $\det_H^2 = 1 - 4f + 4f^2 = 1$, donc $\det_H^{-1} = \det_H$.

(7) Il est naturel de poser $H = O(2)_k$ et $H^0 = \mathrm{SO}(2)_k$; noter toutefois que si $\mathrm{car}(k) = 2$, on a $\det_H = 1$. Déduire de la question précédente une équation de $\mathrm{SO}(2)_k$ dans $O_{2,k}$ valable en toute caractéristique.

Solution : $\mathrm{SO}(2)_k$ est défini dans $O(2)_k$ par l'équation $bc = 0$.

On rappelle que $M_2(k)$ est un G-module pour l'action adjointe, donc a fortiori un H-module. Soit E le sous-espace vectoriel de $M_2(k)$ formé des matrices diagonales

(8) Montrer que E est un sous-H-module de $M_2(k)$. (On pourra utiliser la question 5.)

Solution : Comme H est géométriquement réduit, il suffit de montrer que $E_{\overline{k}} = E \otimes \overline{k}$ est stable par $H(\overline{k})$. Or on voit facilement que pour tout $X = \left(\begin{smallmatrix} x_1 & 0 \\ 0 & x_2 \end{smallmatrix}\right)$ dans $E_{\overline{k}}$ et $g \in H(\overline{k})$, on a :

$$gXg^{-1} = \begin{cases} X & \text{si } g \in H^0(\overline{k}) \\ \begin{pmatrix} x_2 & 0 \\ 0 & x_1 \end{pmatrix} & \text{sinon.} \end{cases}$$

Ou bien on peut faire le calcul (plus compliqué) avec la k-algèbre $R = A$ et l'élément $g = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ de $H(A)$; dans ce cas

$$gXg^{-1} = \det(g)^{-1} \begin{pmatrix} ax_1 & bx_2 \\ cx_1 & dx_2 \end{pmatrix} \begin{pmatrix} d & -b \\ -c & a \end{pmatrix} = (1-2f) \begin{pmatrix} ex_1 - fx_2 & ab(x_2 - x_1) \\ cd(x_1 - x_2) & ex_2 - fx_1 \end{pmatrix}.$$

Or on a vu dans la question 1 que $ab = 0 = cd$; d'autre part, comme $fe = 0$ et $f^2 = f$ on a $(1-2f)e = e$ et $(1-2f)f = f$, d'où :

$$gXg^{-1} = \begin{pmatrix} ex_1 + fx_2 & 0 \\ 0 & ex_2 + fx_1 \end{pmatrix} \in E \otimes A.$$

Ceci étant vrai pour l'élément « générique » $g \in H(A)$, on obtient que pour tout $h \in H(R)$ (i.e. h est un morphisme de k-algèbres $A \to R$) on a $hXh^{-1} \in E \otimes R$.

(9) Déterminer le noyau du morphisme $\rho : H \to \mathrm{GL}(E)$ ainsi que son image $\rho(H)$.

Solution : Il résulte de ce qui précède que ρ envoie H^0 sur le groupe trivial $\{\mathrm{id}_E\}$ et envoie la composante non neutre σH^0 sur la matrice $\left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right) = \sigma_E \in \mathrm{GL}(E)$. Ceci montre que $\mathrm{Ker}(\rho) = H^0$ et $\rho(H) = \{\mathrm{id}_E, \sigma_E\}$ est isomorphe au k-schéma en groupes constant $(\mathbb{Z}/2\mathbb{Z})_k = \mathrm{Spec}(B)$ où $B = ke \oplus kf$ (on a $\Delta(e) = e \otimes e + f \otimes f$ et $\Delta(f) = e \otimes f + f \otimes e$).

Remarque. On a $\rho(H) \simeq H/H^0$ et $B = k[H]^{H^0}$.

Exercice 2. — Soient k un corps et n un entier ≥ 1. On munit $V = k^{2n}$ d'une forme symplectique[(1)] $\langle\ ,\ \rangle$; soit G le groupe symplectique associé, i.e. pour toute k-algèbre R,

$$G(R) = \{g \in \mathrm{GL}_{2n}(R) \mid \forall X, Y \in R^{2n}, \quad \langle gX, gY \rangle = \langle X, Y \rangle\}.$$

Le but de l'exercice est de montrer que G est connexe. Soit $\overline{k}$ une clôture algébrique de k.

(1) En citant des résultats du cours, démontrez qu'il suffit de prouver que $G_{\overline{k}} = \mathrm{Spec}(k[G] \otimes \overline{k})$ est connexe.

Solution : On a vu en cours que si $G_{\overline{k}}$ est connexe il en est de même de G (car la projection $G_{\overline{k}} \to G$ est surjective).

[(1)] I.e. une forme bilinéaire alternée non dégénérée.

(2) En citant des résultats du cours, démontrez qu'il suffit de prouver que tout $g \in G_{\overline{k}}(\overline{k})$ appartient à une partie connexe de (l'espace topologique sous-jacent à) $G_{\overline{k}}$ contenant l'élément neutre.

Solution : Soit C une composante connexe de $G_{\overline{k}}$. On a vu en cours que C contient un k-point $g \in G_{\overline{k}}(\overline{k})$ (identifié au point fermé image du morphisme $g : \mathrm{Spec}(\overline{k}) \to G_{\overline{k}}(\overline{k})$). Donc si g appartient à une partie connexe de $G_{\overline{k}}$ contenant l'élément neutre alors $g \in G^0_{\overline{k}}$ donc $C = G^0_{\overline{k}}$. Ceci montre que $G_{\overline{k}}$ est connexe si la condition de l'énoncé est vérifiée.

Pour tout $v \in k^{2n} - \{0\}$, on a un morphisme de k-schémas $\tau_v : \mathbb{G}_{a,k} \to \mathrm{GL}_{2n,k}$ défini comme suit. Pour toute k-algèbre R et $t \in R$, $\tau_v(t)$ est l'élément de $\mathrm{GL}_{2n}(R)$ tel que, pour tout $X \in R^{2n}$:

$$(\star) \qquad \tau_v(t)X = X + t\langle X, v\rangle v.$$

(3) Montrer que $\tau_v(t) \in G(R)$ et que $\tau_v(t)\tau_v(t') = \tau_v(t+t')$. Par conséquent, τ_v est un morphisme de k-schémas en groupes $\mathbb{G}_{a,k} \to G$.

Solution : Comme $\langle v, v\rangle = 0$ on a :

$$\tau_v(t)\tau_v(t')X = \tau_v(t)(X + t'\langle X, v\rangle v) = X + t'\langle X, v\rangle v + t\langle X, v\rangle v = \tau_v(t+t')X$$

d'où $\tau_v(t)\tau_v(t') = \tau_v(t+t')$; en particulier l'inverse de $\tau_v(t)$ est $\tau_v(-t)$. Donc τ_v est bien un morphisme de k-schémas en groupes $\mathbb{G}_{a,k} \to \mathrm{GL}_{2n,k}$. De plus, pour $X, Y \in R^{2n}$ on a :

$$\langle \tau_v(t)X, \tau_v(t)Y\rangle = \langle X + t\langle X, v\rangle v, Y + t\langle Y, v\rangle v\rangle = \langle X, Y\rangle + t\langle Y, v\rangle\langle X, v\rangle + t\langle X, v\rangle\langle v, Y\rangle = \langle X, Y\rangle$$

donc τ_v est bien à valeurs dans G.

Pour $t \in k$, l'élément $\tau_v(t) \in G(k)$ est appelé une « *transvection symplectique* » (de direction v). Le but de la suite de l'exercice est de montrer que tout élément de $G(k)$ est produit d'au plus $4n$ transvections symplectiques. On dira qu'un couple (u, v) d'éléments de k^{2n} est *hyperbolique* si $\langle u, v\rangle = 1$; dans ce cas, $V = k^{2n}$ est la somme directe de $E = ku \oplus kv$ et de son orthogonal $E^\perp$.

Soient (u, v) et (u', v') deux couples hyperboliques. On veut montrer qu'on peut envoyer (u, v) sur (u', v') par un produit d'au plus quatre transvections symplectiques.

(4) On suppose $\langle u, u'\rangle \neq 0$; posant alors $w = u' - u$ montrer que $\tau_w(t)u = u'$ pour un $t \in k^\times$ bien choisi.

Solution : On a $\tau_w(t)u = u + t\langle u, w\rangle(u' - u)$ et $\langle u, w\rangle = \langle u, u'\rangle \neq 0$ donc en prenant $t = \langle u, w\rangle^{-1}$ on obtient $\tau_w(t)u = u'$. (Et donc $\tau_w(t)$ envoie (u, v) sur le couple hyperbolique (u', v''), où $v'' = \tau_w(t)v$.)

(5) Supposons $\langle u, u'\rangle = 0$. Il existe une forme linéaire $f \in V^*$ telle que $f(u) \neq 0$ et $f(u') \neq 0$ et comme $\langle\ ,\ \rangle$ induit un isomorphisme entre V et V^* il existe donc $u'' \in V$ tel que $\langle u, u''\rangle \neq 0$ et $\langle u', u''\rangle \neq 0$. Déduire de la question précédente qu'on peut toujours envoyer (u, v) sur un couple hyperbolique (u', v''), pour un certain v'', par un produit d'au plus deux transvections symplectiques.

Solution : Comme $\langle u, u''\rangle \neq 0$ et $\langle u', u''\rangle \neq 0$ alors, d'après la question précédente il existe une première transvection symplectique envoyant (u, v) sur un couple hyperbolique (u'', v_1), puis une seconde envoyant (u'', v_1) sur (u', v''), pour un certain v''.

Notant maintenant (u, v) au lieu de (u', v''), il reste à envoyer (u, v) sur (u, v') (en gardant le même u).

(6) On suppose $\langle v, v'\rangle \neq 0$ et l'on pose $w = v' - v$. Montrer que $\langle u, w\rangle = 0$ puis qu'il existe $t \in k$ tel que $\tau_w(t)$ envoie (u, v) sur (u, v').

Solution : Comme (u, v) et (u, v') sont des couples hyperboliques, on a $\langle u, v\rangle = 1 = \langle u, v'\rangle$ et donc $\langle u, w\rangle = 0$. Pour tout $t \in k$ on a donc $\tau_w(t)u = u$ et

$$\tau_w(t)v = v + t\langle v, w\rangle(v' - v)$$

et comme $\langle v, w\rangle = \langle v, v'\rangle \neq 0$, ceci vaut v' si l'on prend $t = \langle v, w\rangle^{-1}$.

(7) On suppose $\langle v, v' \rangle = 0$. Montrer alors que $(u, u+v)$ est un couple hyperbolique et que $\langle u+v, v \rangle = 1 = \langle u+v, v' \rangle$. Conclure.

Solution : On a $\langle u, u+v \rangle = \langle u, v \rangle = 1$ donc $(u, u+v)$ est un couple hyperbolique. De plus $\langle v, u+v \rangle = \langle v, u \rangle = -1$ et $\langle u+v, v' \rangle = \langle u, v' \rangle = 1$ donc, d'après la question précédente, il existe une première transvection symplectique envoyant (u, v) sur $(u, u+v)$, puis une seconde envoyant $(u, u+v)$ sur (u, v'). On a ainsi montré que tout couple hyperbolique (u, v) peut être envoyé sur tout autre couple (u', v') par un produit d'au plus quatre transvections symplectiques.

On rappelle que V s'écrit comme somme directe de n plans orthogonaux $E_1, \ldots, E_n$, où chaque E_i admet une base hyperbolique (u_i, v_i). Soit g un élément quelconque de $G(k)$.

(8) Montrer qu'il existe un produit h_n d'au plus quatre transvections symplectiques, tel que $h_n g$ soit l'identité sur E_n.

Solution : (gu_n, gv_n) est un couple hyperbolique donc il existe un produit h_n d'au plus quatre transvections symplectiques tel que $h_n g u_n = u_n$ et $h_n g v_n = v_n$. Alors $h_n g$ est l'identité sur E_n.

(9) Comme $h_n g \in G(k)$, il laisse stable $E_n^\perp = E_1 \oplus \cdots \oplus E_{n-1}$. En procédant par récurrence, montrer qu'il existe un produit $h_1 \cdots h_n$ d'au plus $4n$ transvections symplectiques tel que $h_1 \cdots h_n g = \mathrm{id}_V$.

Solution : Par hypothèse de récurrence, il existe un produit h d'au plus $4(n-1)$ transvections symplectiques $\tau_i = \tau_{x_i}(t_i)$, dont les directions x_i appartiennent à $E_n^\perp$, tel que $h h_n g$ soit l'identité sur $E_n^\perp$. De plus, comme les x_i appartiennent à $E_n^\perp$ alors chaque τ_i est l'identité sur E_n, donc il en est de même de $h h_n g$. Donc $h h_n g = \mathrm{id}_V$ et donc $g = (h h_n)^{-1}$ s'écrit comme un produit d'au plus $4n$-transvections symplectiques.

(10) On suppose dans cette question que $k = \overline{k}$. Pour tout $g \in G(k)$, montrer que g appartient à l'image d'un morphisme de k-schémas $Y \to G$, pour un certain k-schéma irréductible Y. En déduire que G est connexe.

Solution : Soit $g \in G(k)$. D'après la question précédente, il existe un entier $N \leq 4n$ et un morphisme de k-schémas $\mu : \mathbb{G}_{a,k}^N \to G$, $(t_1, \ldots, t_N) \mapsto \tau_{x_1}(t_1) \cdots \tau_{x_N}(t_N)$ tel que g appartient à $\mu(Y)$. Comme Y est irréductible (a fortiori connexe), il en est de même de $\mu(Y)$. D'après la question 2, on en déduit que G est connexe.

(11) On admet que G est géométriquement réduit. Montrer que $G \subset \mathrm{SL}_{2n,k}$, i.e. que le morphisme dét : $G \to \mathbb{G}_{m,k}$ est trivial. (Soit J la matrice de $\langle\ ,\ \rangle$ dans la base canonique de k^{2n} ; écrire l'équation « matricielle » définissant G dans $\mathrm{GL}_{2n,k}$, puis utiliser la question précédente.)

Solution : Pour toute k-algèbre R, on a $G(R) = \{g \in \mathrm{GL}_{2n}(R) \mid {}^t g J g = J\}$, donc G est défini par l'équation « matricielle » ${}^t g J g = J$. Prenant le déterminant, on obtient $\mathrm{dét}(g)^2 \mathrm{dét}(J) = \mathrm{dét}(J)$ et comme $\mathrm{dét}(J) \in k^\times$ on obtient $\mathrm{dét}(g)^2 = 1$. Donc, posant $B = k[T]/(T^2-1)$, le morphisme $\mathrm{dét}_G : G \to \mathbb{G}_{m,k}$ se factorise par le sous-schéma en groupes fermé $\mu_{2,k} = \mathrm{Spec}(B)$ de $\mathbb{G}_{m,k} = \mathrm{Spec}(k[T, T^{-1}])$. De plus, comme G est connexe, $\mathrm{dét}_G$ se factorise par la composante connexe de $\mu_{2,k}$, qui est $\mathrm{Spec}(k) = \mathrm{Spec}(k[T]/(T-1))$ si $\mathrm{car}(k) \neq 2$. Enfin, si $\mathrm{car}(k) = 2$ alors $\mu_{2,k} = \mathrm{Spec}(k[T]/(T-1)^2)$ est connexe mais pas réduit, et comme G est réduit $\mathrm{dét}_G$ se factorise dans ce cas par le sous-schéma réduit $\mathrm{Spec}(k[T]/(T-1)) = \mathrm{Spec}(k)$.

Une façon équivalente de dire la même chose est la suivante. Le morphisme $\mathrm{dét}_G : G \to \mathbb{G}_{m,k}$ correspond au morphisme d'algèbres de Hopf $\eta : k[T, T^{-1}] \to k[G]$ qui envoie T sur l'image de dét $\in k[\mathrm{GL}_{2n,k}]$ dans $k[G]$, notée $\mathrm{dét}_G$. On a vu que pour tout morphisme de k-algèbres $g : k[G] \to R$, l'élément $\mathrm{dét}_G(g) = (g \circ \eta)(T)$ de $R^\times$ vérifie $\mathrm{dét}_G(g)^2 = 1$, donc $g \circ \eta$ se factorise à travers le quotient $k[T]/(T^2-1)$. Appliquant ceci à $R = k[G]$ et au morphisme id_R, on obtient que η se factorise à travers $B = k[T]/(T^2-1)$.

Si $\mathrm{car}(k) \neq 2$ alors B contient les idempotents $e = (1+T)/2$ et $f = (1-T)/2$ et comme $k[G]$ ne contient pas d'idempotents autres que 0 et 1 (car G est connexe), alors η se factorise à travers $B/(f) = k[T]/(T-1)$.

Enfin, si $\mathrm{car}(k) = 2$ alors $B \simeq k[T]/(T-1)^2$ n'est pas réduite, et comme $k[G]$ est réduite, η se factorise à travers $B/\sqrt{0} = k[T]/(T-1)$.

Exercice 3. — Soient k un corps non parfait de caractéristique 2 et a un élément de k qui n'est pas un carré. [(2)] Soit G le k-schéma en groupes défini comme suit : pour toute k-algèbre R,

$$G(R) = \{(x, y) \in R^2 \mid x^2 - ay^2 = 1\}$$

avec la loi de groupe (commutative) : $(x, y)(x', y') = (xx' + ayy', xy' + yx')$.

Remarque : En fait, soit k' l'extension quadratique $k(\sqrt{a})$. Pour toute k-algèbre R, posant $R_{k'} = R \otimes k' = R \oplus R\sqrt{a}$ on a :

$$\begin{aligned} G(R) = \mu_2(R_{k'}) &= \{(x, y) \in R^2 \mid x + y\sqrt{a} \in \mu_2(R_{k'})\} \\ &= \{(x, y) \in R^2 \mid x^2 + ay^2 = 1\}. \end{aligned}$$

(Comme $\mathrm{car}(k) = 2$ on peut écrire $-$ au lieu de $+$, i.e. ceci coïncide avec la définition plus haut.) Ceci définit un *foncteur* en groupes, et comme

$$(x + y\sqrt{a})(x' + y'\sqrt{a}) = (xx' + ayy') + (xy' + yx')\sqrt{a}$$

la loi de groupe (commutative !) est celle donnée plus haut. Enfin, il est clair que le foncteur $R \mapsto G(R)$ (à valeurs dans la catégorie des ensembles) est représenté par la k-algèbre $A = k[X, Y]/(X^2 - aY^2 - 1)$. Donc celle-ci est automatiquement une k-algèbre de Hopf et donc $G = \mathrm{Spec}(A)$ est bien un k-schéma en groupes.

D'autre part, pour toute k-algèbre B de type fini, on notera $\mathrm{Dim}(B)$ sa dimension de Krull, i.e. la dimension du k-schéma $\mathrm{Spec}(B)$. On « rappelle » que si $\mathrm{Dim}(B) = 0$ alors B est de dimension finie sur k (comme k-espace vectoriel), et si B est *intègre* alors $\mathrm{Dim}(B/I) < \mathrm{Dim}(B)$ pour tout idéal $I \neq (0)$.

Comme $k[X, Y]$ est intègre de dimension 2 et comme $\dim_k(k[G]) = \infty$, on a $0 < \mathrm{Dim}(k[G]) < 2$ et donc $\dim(G) = \mathrm{Dim}(k[G]) = 1$.

(1) Montrer que $H = \mu_{2,k}$ est un sous-schéma en groupes fermé de G.

Solution : Considérons la structure d'algèbre de Hopf de A ; on a :

$$\Delta(X) = X \otimes X + aY \otimes Y, \qquad \Delta(Y) = X \otimes Y + Y \otimes X, \qquad \varepsilon(X) = 1, \qquad \varepsilon(Y) = 0.$$

Par conséquent, l'idéal $J = (Y)$ est contenu dans $\mathrm{Ker}(\varepsilon)$ et vérifie $\Delta(J) \subset J \otimes A + A \otimes J$, donc c'est un idéal de Hopf. On a donc un morphisme surjectif d'algèbres de Hopf $A \to A/J = k[X]/(X^2 - 1)$ et ceci montre que $\mu_{2,k}$ est un sous-schéma en groupes fermé de G. Le morphisme de schémas en groupes correspondant $\tau : \mu_{2,k} \to G$ est défini par : pour toute k-algèbre R et $x \in \mu_2(R)$, $\tau(x) = (x, 0)$.

(2) Montrer que $A = k[Y] \oplus k[Y]X$ comme k-espace vectoriel (en notant encore X et Y les images de X et Y dans A).

Solution : C'est clair, puisque $X^2 = aY^2 + 1$ et que c'est la seule équation. De façon plus détaillée, on peut faire la division euclidienne par le polynôme unitaire $D = X^2 - aY^2 - 1$: tout $P \in k[X, Y]$ s'écrit de façon unique $P = QD + S$ avec $\deg_X(S) \leq 1$, i.e. $S \in k[Y] + k[Y]X$.

(3) On rappelle que la sous-algèbre $B = A^H$ est formée des $\phi \in A$ tels que pour tout morphisme de k-algèbres $R \to R'$, $h \in H(R)$ et $g \in G(R')$ on ait $\phi(gh) = \phi(g)$. Montrer que A^H est une k-algèbre $k[u, v]$ avec une relation $u^2 = P(v)$ pour un certain polynôme P de degré 2.

Solution : Soit $\phi \in A$. Soient $R = k[t] = k[T]/(T^2 - 1)$, h l'isomorphisme $k[H] \simeq R$ envoyant X sur t. Alors l'élément h de $H(R)$ agit sur $A \otimes R = R[X, Y]/(X^2 - aY^2 - 1)$ par $hX = tX$ et $hY = tY$. On en déduit que si $\phi \in A^H$ alors on a dans $A \otimes R$ l'égalité $\phi(tX, tY) = \phi(X, Y)$, et ceci entraîne que ϕ est un polynôme en Y^2 et XY (et aussi X^2, mais $X^2 = 1 + aY^2$). Réciproquement, on voit que tout tel polynôme est invariant par H. Par conséquent, B est la sous-algèbre de A

[(2)] Par exemple, $k = \mathbb{F}_2(t)$ et $a = t$.

engendrée par les éléments $u = XY$ et $v = Y^2$; de plus, on a $u^2 = X^2Y^2 = Y^2 + aY^4 = v + av^2$, donc B est un quotient de $C = k[U,V]/(U^2 + V + aV^2)$, qui est de dimension 1.

Par ailleurs, d'après le rappel sur la dimension de Krull fait plus haut, on sait que $\mathrm{Dim}(B) = 1$. (Ceci découle aussi de la question suivante.)

Or le polynôme $P(U,V) = U^2 + V + aV^2$ est irréductible : en effet une factorisation serait nécessairement de la forme $P = (aV + Q(U))(V + R(U))$ avec $Q, R \neq 0$ et $\deg(QR) = 2$; comme P ne contient pas de terme VU^2, on aurait nécessairement $\deg(Q) = 1 = \deg(R)$ et comme le coefficient de U^2 dans P est 1 on aurait

$$P(U,V) = (aV + \alpha U + \beta)(V + \alpha^{-1}U + \gamma)$$

avec $\alpha, \beta, \gamma \in k^\times$; alors le coefficient de UV serait $\alpha + \alpha^{-1}a$ et ceci est non nul car sinon on aurait $a = \alpha^2$. Donc C est intègre, de dimension 1 ; si B était un quotient strict de C, on aurait $\mathrm{Dim}(B) < 1$, ce qui n'est pas le cas. Donc la surjection $C \to B$ est un isomorphisme.

(4) Soit $\overline{G} = G/H = \mathrm{Spec}(B)$. Quelle est la dimension de $\overline{G}$?

Solution : D'après le cours, on sait que $\dim(\overline{G}) = \dim(G) - \dim(H) = 1 - 0 = 1$.

(5) Déterminer les k-points $G(k)$ et montrer que $\overline{G}(k) \neq \{e\}$.

Solution : Soit $(x,y) \in G(k)$, i.e. $(x,y) \in k^2$ et $ay^2 = x^2 + 1$. On a nécessairement $y = 0$ car sinon aurait $a = y^{-2}(x+1)^2$. Donc $y = 0$ et $x^2 = 1$ d'où $x = 1$. Ceci montre que le seul k-point de G est l'élément neutre $e = (1,0)$.

Par contre, $\overline{G}(k)$ contient au moins deux points, car pour $u = 0$ l'équation $0 = v + av^2 = v(1 + av)$ admet les solutions $v = 0$ et $v = a^{-1}$; le point $(0,0)$ étant l'élément neutre de $\overline{G}(k)$.

(En fait, comme l'équation de $\overline{G}(k)$, homogénéisée en $u^2 = vw + av^2$ est celle d'une conique $\mathscr{C}$ du plan projectif $\mathbb{P}^2(k)$ contenant le k-point $p = [0:0:1] = [e_3]$, où (e_1, e_2, e_3) désigne la base canonique de k^3, on peut montrer que les k-points de $\overline{G}$ sont en bijection avec $\mathbb{P}^1(k) \simeq \mathbb{P}(k^3/ke_3)$, car la droite projective d'équation $v = 0$ est la tangente à $\mathscr{C}$ en p, et pour tout $t \in k$ la droite projective d'équation $u = tv$ coupe $\mathscr{C}$ en un unique point $q_t \neq p$ et l'on obtient ainsi une bijection de k sur $\mathscr{C} - \{p\} = \overline{G}(k) - \{e\}$.)

(6) Soient k' l'extension quadratique $k(\sqrt{a})$ et $G' = \mathrm{Spec}(A \otimes k')$. Posant $b = \sqrt{a}$, montrer que le morphisme de k'-schémas $G' \to \mu_{2,k'} \times \mathbb{G}_{a,k'}$ défini par $(x,y) \mapsto (z = x - by, zy)$ est un isomorphisme de k'-schémas en groupes. (Commencer par écrire la loi de groupe de G' dans les « coordonnées » (z,y).)

Solution : Il est clair que l'application $G' \to \mu_{2,k'} \times \mathbb{G}_{a,k'}$ définie par $(x,y) \mapsto (z = x - by, y)$ est un isomorphisme de k'-schémas, d'inverse $(z,y) \mapsto (x = z + by, y)$. Identifiant G' à $\mu_{2,k'} \times \mathbb{G}_{a,k'}$ via cet isomorphisme, un calcul facile, utilisant l'égalité $xy' + x'y = (x - by)y' + (x' - by')y$, montre que dans les « coordonnées » (z,y), la loi de groupe de G' est donnée par :

$$(z,y)(z',y') = (zz', z'y + zy').$$

Comme z appartient à $\mu_2(R)$, on voit alors que le morphisme $\eta : G' \to \mu_{2,k'} \times \mathbb{G}_{a,k'}$ défini par $(z,y) \mapsto (z, zy)$ est un isomorphisme (d'inverse $(z,y') \mapsto (z, zy')$) et aussi un morphisme de k'-schémas en groupes, puisque

$$\eta\big((z,y)(z',y')\big) = (zz', zy + z'y') = \eta(z,y)\eta(z',y').$$