Classification des groupes réductifs sur un corps k

Références pour ce chapitre :

[Bl] André Blanchard, Les corps non commutatifs, P.U.F, 1972. (Chap. III-IV)

[BAlg] Nicolas Bourbaki, Algèbre, Chap. 4-7, Masson, 1981 (Chap. V, §§7,10,13) et Chap. 8, Springer-Verlag, 2012. (§§14-19)

[KMRT] M.-A. Knus, A. Merkurjev, M. Rost, J.-P. Tignol, The book of involutions, Amer. Math. Soc. 1998. (§§1,2,29)

[Sch] Winfried Scharlau, Quadratic and hermitian forms, Springer-Verlag, 1985. (Chap. 8 et §§10.1, 10.3)

[Se] Jean-Pierre Serre, Cohomologie galoisienne (5ème édition), Springer-Verlag, 1994. (§§II.5 et III.1)

[SGA3] Schémas en groupes (SGA 3), t. III, nouvelle édition recomposée et annotée, Documents Mathématiques 8, Soc. Math. France, 2011. (Exp. XXI et XXIV)

[Sp] T. A. Springer, Linear algebraic groups (2nd ed.), Birkäuser, 1998. (Chap. 17)

[Ti] Jacques Tits, Liesche Gruppen und Algebren, Springer-Verlag, 1983. (§IV.6)

---

(1) On fixe un corps de base k et une clôture algébrique $\overline{k}$. Soit k_s la clôture séparable de k dans $\overline{k}$, i.e. l'ensemble des $\lambda \in \overline{k}$ dont le polynôme minimal sur k n'a que des racines simples. (On a $k_s = \overline{k}$ si k est parfait, en particulier si $\mathrm{car}(k) = 0$ ou si k est un corps fini.) Alors k_s/k est une extension galoisienne, i.e. posant $\Gamma = \mathrm{Aut}_k(k_s)$, le sous-corps des invariants $k_s^\Gamma = \{x \in k_s \mid \forall \gamma \in \Gamma,\ \gamma(x) = x\}$ égale k. On écrira $\Gamma = \mathrm{Gal}(k_s/k)$. (Pour tout ceci, voir par exemple [BAlg, §V.10].)

Dans toute la suite, « k-groupe algébrique » signifie : « k-schéma en groupes G affine de type fini, géométriquement réduit », i.e. G est donné par une k-algèbre de Hopf $A = k[G]$ de type fini, telle que $A_{\overline{k}} = A \otimes \overline{k}$ est réduite. Si $X = \mathrm{Spec}(B)$ est un k-schéma affine et K un corps contenant k, on notera $X \otimes K$ ou simplement X_K le K-schéma $\mathrm{Spec}(B_K)$, où $B_K = B \otimes K$.

1. k-groupes réductifs

***Définition 1.1* (k-tores).** — Soit S un k-groupe algébrique.

(i) On dit que S est un k-tore de dimension r si $S \otimes \overline{k}$ est isomorphe au produit de r copies de $\mathbb{G}_{m,\overline{k}}$.

(ii) Attention, un k-tore de dimension r n'est **pas nécessairement** isomorphe à $\mathbb{G}_{m,k}^r$, cf. exemples plus bas.

(iii) Si $S \simeq (\mathbb{G}_{m,k})^r$, on dit que S est un tore **déployé** (de dimension r).

Exemple 1.2. — Supposons $\mathrm{car}(k) \neq 2$. Soit δ un élément de k qui n'est pas un carré dans k. Le polynôme $X^2 - \delta$ a deux racines distinctes $\pm\sqrt{\delta}$ dans $\overline{k}$ et elles sont donc dans k_s ; soit $k' = k(\sqrt{\delta})$ l'extension quadratique correspondante. Pour toute k-algèbre R, on a $R \otimes k' = R \oplus R\sqrt{\delta}$ et l'application qui à tout $z = x + y\sqrt{\delta}$ associe $\overline{z} = x - y\sqrt{\delta}$ est un automorphisme de R-algèbre ; par conséquent l'application $z \mapsto N(z) = z\overline{z} = x^2 - \delta y^2$ est un morphisme de groupes $\mathbb{G}_m(R \otimes k') \to k^\times$; notons $S(R)$ son noyau, i.e.

$$S(R) = \{x + y\sqrt{\delta} \in (R \otimes k')^\times \mid x^2 - \delta y^2 = 1\}.$$

(1) Version du 13 avril 2016.

Ceci définit un k-foncteur en groupes, qui est représenté par la k-algèbre (de Hopf) $A = k[X,Y]/(X^2-\delta Y^2-1)$. En faisant dans $k'[X,Y]$ le changement de variables $T = X+\sqrt{\delta}Y$ et $T' = X-\sqrt{\delta}Y$ (c'est bien un changement de variables car $X = (T+T')/2$ et $Y = (T-T')/2\sqrt{\delta}$), on obtient que

$$A_{k'} \simeq k'[T,T']/(TT'-1) = k'[T,T^{-1}]$$

et la loi de groupe est donnée par $t_1 \cdot t_2 = t_1 t_2$, i.e. $S_{k'} \simeq \mathbb{G}_{m,k'}$. Donc S est un k-tore de dimension 1.

Par contre S n'est pas déployé. En effet, S est isomorphe au sous-groupe H de $\mathrm{SL}_{2,k}$ défini par

$$H(R) = \left\{ \begin{pmatrix} x & \delta y \\ y & x \end{pmatrix} \in \mathrm{GL}_2(R) \;\middle|\; x^2 - \delta y^2 = 1 \right\}$$

donc $V = k^2$ est une représentation de S. Si S était isomorphe à $\mathbb{G}_{m,k}$ alors V serait somme d'espaces de poids donc les éléments de $S(k)$ seraient tous diagonaux dans une certaine base de V. Or les valeurs propres (dans k') de la matrice ci-dessus sont $x \pm y\sqrt{\delta}$ et celles-ci ne sont pas dans k (sauf si $y = 0$).

Remarque 1.3. — On peut montrer (voir plus bas) que les classes d'isomorphisme de k-tores de dimension 1 non déployés sont en bijection avec les sous-groupes d'indice 2 de $\Gamma = \mathrm{Gal}(k_s/k)$, i.e. avec les extensions quadratiques de k contenues dans k_s.

En particulier, si $k = \mathbb{R}$ il existe à isomorphisme près un unique $\mathbb{R}$-tore de dimension 1 non déployé ; c'est le groupe $\mathrm{SO}_{2,\mathbb{R}}$, dont les R-points sont :

$$\mathrm{SO}_2(R) = \left\{ \begin{pmatrix} x & -y \\ y & x \end{pmatrix} \in \mathrm{GL}_2(R) \;\middle|\; x^2 + y^2 = 1 \right\}.$$

Terminologie 1.4 **(Données radicielles simplement connexes ou adjointes)**
Soit $\mathscr{R} = (M, M^\vee, R, R^\vee)$ une donnée radicielle réduite.

(i) Son **rang**, noté $\mathrm{rang}(\mathscr{R})$, est le rang des groupes abéliens libres M et $M^\vee = \mathrm{Hom}_{\mathbb{Z}}(M,\mathbb{Z})$.

(ii) Le *rang semi-simple* de $\mathscr{R}$, noté $\mathrm{rang}_{\mathrm{ss}}(\mathscr{R})$, est le rang du sous-groupe $Q(R) = \mathbb{Z}R$ de M. On dit que $\mathscr{R}$ est **semi-simple** si $\mathrm{rang}_{\mathrm{ss}}(\mathscr{R}) = \mathrm{rang}(\mathscr{R})$, ce qui équivaut à dire que R (resp. $R^\vee$) engendre $M \otimes \mathbb{Q}$ (resp. $M^\vee \otimes \mathbb{Q}$) comme $\mathbb{Q}$-espace vectoriel.

(iii) On dit que $\mathscr{R}$ est **simplement connexe**, resp. **adjointe**, si $\mathbb{Z}R = M$, resp. $\mathbb{Z}R^\vee = M^\vee$. (Ceci entraîne bien sûr que $\mathscr{R}$ est semi-simple.)

(iv) Nous dirons que $\mathscr{R}$ est **irréductible** si elle est semi-simple et si le système de racines R est irréductible.

Définition 1.5 **(k-groupes réductifs)**. — Soit G un k-groupe algébrique. On dit que G est un k-groupe réductif si $G \otimes \overline{k}$ est un $\overline{k}$-groupe réductif.

Dans ce cas, tous les tores maximaux de $G \otimes \overline{k}$ sont conjugués par $G(\overline{k})$, leur dimension commune est notée r et s'appelle le *rang réductif* de G ; de plus, si T est l'un d'eux l'ensemble R des poids non nuls de T dans $\mathrm{Lie}(G) \otimes \overline{k}$ est un système de racines et $\mathscr{R} = (X(T), X_*(T), R, R^\vee)$ est une donnée radicielle réduite dont la classe d'isomorphisme ne dépend pas du choix de T. On dira que G est un k-groupe réductif **de type** $\mathscr{R}$; son rang réductif est alors $r = \mathrm{rang}(\mathscr{R})$.

Définition 1.6 **(k-groupes réductifs déployés)**. — Soit G un k-groupe réductif de type $\mathscr{R} = (M, M^\vee, R, R^\vee)$.

(i) On dit que G est **déployé** (sur k) s'il contient un k-tore déployé T de dimension $r = \mathrm{rang}(\mathscr{R})$. Dans ce cas, l'ensemble des poids non nuls de T dans $\mathfrak{g} = \mathrm{Lie}(G)$ est R et l'on a $\mathscr{R} \simeq (X(T), X_*(T), R, R^\vee)$.

(ii) Attention, G n'est **pas nécessairement** déployé, cf. exemple plus bas.

On admet la proposition suivante (cf. [SGA3, Exp. XXIII et XV 1.2] ou [Sp, §16.3]).

***Proposition 1.7* (Unicité des groupes déployés).** — *Soit $\mathscr{R}$ une donnée radicielle réduite. Il existe un k-groupe réductif déployé H de type $\mathscr{R}$, unique à isomorphisme près.*

Exemples 1.8. — 1) $\mathrm{GL}_{n,k}$, $\mathrm{SL}_{n,k}$, $\mathrm{PGL}_{n,k}$ et le groupe symplectique $\mathrm{Sp}_{2n,k}$ sont des k-groupes réductifs déployés. Si $\mathrm{car}(k) \neq 2$ et si J_n désigne l'élément de $\mathrm{GL}_n(k)$ dont tous les coefficients sont nuls sauf ceux de la seconde diagonale qui valent 1 (i.e. $J_{i,j} = 1$ si $i + j = n$ et $= 0$ sinon), il en est de même du groupe spécial orthogonal $\mathrm{SO}(J_n)_k$ défini par $\mathrm{SO}(J_n)(R) = \{A \in \mathrm{SL}_n(R) \mid {}^tAJ_nA = J_n\}$ pour toute k-algèbre R. (On peut aussi définir le groupe orthogonal déployé sur un corps de caractéristique 2, mais la définition est un peu différente.)

2) Le $\mathbb{R}$-groupe $G = \mathrm{SO}(3)_{\mathbb{R}}$, défini par $\mathrm{SO}(3)(R) = \{A \in \mathrm{SL}_n(R) \mid {}^tAA = I_3\}$ pour toute $\mathbb{R}$-algèbre R, est un $\mathbb{R}$-groupe réductif de rang réductif 1 car $G \otimes \mathbb{C}$ est isomorphe à $\mathrm{SO}(J_3)_{\mathbb{C}}$. Mais G ne contient aucun $\mathbb{R}$-tore déployé $T \simeq \mathbb{G}_{m,\mathbb{R}}$, car sinon le T-module $V = \mathbb{R}^3$ serait somme directe d'espaces de poids, donc tous les éléments de $T(\mathbb{R})$ seraient diagonaux dans une certaine base de V. Or tout élément $f \neq \mathrm{id}_V$ de $T(\mathbb{R}) \subset \mathrm{SO}(3)(\mathbb{R})$ est une rotation, si elle est diagonalisable alors sa matrice dans une certaine base orthonormée $\mathscr{B}$ est $\left(\begin{smallmatrix} 1 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & -1 \end{smallmatrix}\right)$; alors un élément diagonalisable g de $T(\mathbb{R})$, commutant à f, ne peut être que l'une des matrices $\left(\begin{smallmatrix} \varepsilon & 0 & 0 \\ 0 & \varepsilon' & 0 \\ 0 & 0 & \varepsilon\varepsilon' \end{smallmatrix}\right)$, où $\varepsilon^2 = 1 = \varepsilon'^2$.

Remarques. — 1) Il existe des données radicielles semi-simples qui ne sont ni simplement connexes ni adjointes ; par exemple celle du groupe $\mathrm{SL}_{n,k}/\mu_{d,k}$, où d est un diviseur strict de n, ou celle du groupe $\mathrm{SO}(J_{2n})$ pour $n \geq 2$.

2) Si $\mathscr{R}$ est une donnée radicielle simplement connexe (resp. adjointe) de système de racines R et si $R = R_1 \times \cdots \times R_n$ est la décomposition de R en produit de systèmes de racines irréductibles, alors $\mathscr{R}$ est isomorphe au produit $\mathscr{R}_1 \times \cdots \times \mathscr{R}_n$, où chaque $\mathscr{R}_i$ est la donnée radicielle simplement connexe (resp. adjointe) de type R_i. Ceci explique l'importance des données radicielles simplement connexes ou adjointes pour les questions de classification, car elles permettent de se ramener au cas d'un système de racines irréductible. En dehors du cas simplement connexe ou adjoint, ceci n'est pas toujours possibe, cf. 3) ci-dessous.

3) La donnée radicielle du k-groupe semi-simple $G = (\mathrm{SL}_{n,k} \times \mathrm{SL}_{n,k})/\mu_{n,k}$, où le centre $\mu_{n,k}$ de $\mathrm{SL}_{n,k}$ est plongé diagonalement dans $\mathrm{SL}_{n,k} \times \mathrm{SL}_{n,k}$ ne se décompose pas comme un produit de deux données radicielles irréductibles.

Tenant pour acquise la classification des données radicielles réduites $\mathscr{R}$, le principe de la classification des k-groupes réductifs est le suivant : on fixe une donnée radicielle réduite $\mathscr{R}$ et, notant H l'unique k-groupe réductif déployé de type $\mathscr{R}$, on va chercher à classifier tous les k-groupes réductifs G de type $\mathscr{R}$, en montrant d'abord que $G \otimes k_s \simeq H \otimes k_s$ puis en procédant par « descente galoisienne » (cf. la section suivante). Pour cela, on aura besoin de la description suivante du groupe d'automorphismes de $H \otimes k_s$ (et, plus généralement, de $H \otimes K$ pour tout corps K contenant k).

***Rappels 1.9* (Morphismes de données radicielles).** — Soient $\mathscr{R} = (M, M^\vee, R, R^\vee)$ et $\mathscr{R}' = (M', M'^\vee, R', R'^\vee)$ deux données radicielles. Soit $f : M \to M'$ une application $\mathbb{Z}$-linéaire et ${}^tf : M'^\vee \to M^\vee$ sa transposée.

(i) On dit que f est un **morphisme** de $\mathscr{R}$ vers $\mathscr{R}'$ si f induit une bijection de R sur R' et ${}^t f$ une bijection de $R'^\vee$ sur $R^\vee$.

(ii) Un tel morphisme est appelé une **isogénie** si, de plus, f est injectif de conoyau fini.

(iii) On note $\mathrm{Aut}(\mathscr{R})$ le groupe des morphismes bijectifs $f : \mathscr{R} \to \mathscr{R}$; c'est un sous-groupe de $\mathrm{Aut}_{\mathbb{Z}}(M) = \mathrm{GL}(M)$.

***Définitions 1.10* (Données radicielles épinglées).** — Une donnée radicielle réduite **épinglée** est un couple $(\mathscr{R}, \Delta)$, où $\mathscr{R} = (M, M^\vee, R, R^\vee)$ une donnée radicielle réduite et Δ est une base de R. Le groupe d'automorphismes de cette donnée épinglée est :

$$\mathrm{Aut}(\mathscr{R}, \Delta) = \{f \in \mathrm{Aut}(\mathscr{R}) \mid f(\Delta) = \Delta\}.$$

Alors, on a le théorème suivant (cf. [SGA3, §XXIII 6.7 et §XXIV 1]).

Théorème 1.11. — *Soit H un k-groupe réductif déployé de type $\mathscr{R} = (M, M^\vee, R, R^\vee)$, et H_{ad} le quotient de H par son centre. Pour tout corps K contenant k, notons $\mathscr{A}(K)$ le groupe des automorphismes du K-groupe algébrique H_K. Soient Δ une base de R et $\mathscr{D}$ son diagramme de Dynkin.*

(i) *$\mathscr{A}(K)$ est isomorphe*[(2)] *au produit semi-direct $H_{\mathrm{ad}}(K) \rtimes \mathrm{Aut}(\mathscr{R}, \Delta)$.*

(ii) *Si H est semi-simple, on a $\mathrm{Aut}(\mathscr{R}, \Delta) \subset \mathrm{Aut}(\mathscr{D})$, et cette inclusion est une égalité si H est simplement connexe ou bien adjoint.*

Exemple 1.12. — Soit $\mathscr{D}$ le diagramme de Dynkin de type $A_1 \times A_1$, i.e. $\mathscr{D}$ est formé de deux points 1 et 2, sans arête. On a $\mathrm{Aut}(\mathscr{D}) = S_2$. Il y a quatre k-groupes semi-simples déployés dont le diagramme de Dynkin est $\mathscr{D}$:

$$H_{sc} = (\mathrm{SL}_{2,k})^2, \qquad H_1 = H_{sc}/\mu_{2,k}, \qquad H_{\mathrm{ad}} = (\mathrm{PGL}_{2,k})^2, \qquad H_2 = \mathrm{SL}_{2,k} \times \mathrm{PGL}_{2,k},$$

où dans la définition de H_1 le centre $\mu_{2,k}$ de $\mathrm{SL}_{2,k}$ est plongé diagonalement dans $H_{\mathrm{sc}} = \mathrm{SL}_{2,k} \times \mathrm{SL}_{2,k}$. Pour tous ces groupes, le groupe d'automorphisme de H_K contient $H_{\mathrm{ad}}(K) = \mathrm{PGL}_2(K)^2$. Dans les trois premiers cas, l'automorphisme non trivial de $\mathscr{D}$ se relève en un automorphisme de H, qui est l'échange des deux facteurs, donc dans ces trois cas on a $\mathscr{A}(K) \simeq H_{\mathrm{ad}}(K) \rtimes S_2$.[(3)] Par contre, dans le cas de H_2 on ne peut échanger les facteurs $\mathrm{SL}_{2,k}$ et $\mathrm{PGL}_{2,k}$, non isomorphes, et l'on a $\mathscr{A}(K) = H_{\mathrm{ad}}(K)$.

La fin de ce paragraphe peut être omise en première lecture, ceci ne sera utilisé que pour ramener la classification des k-groupes réductifs de type $\mathscr{R}$ au cas où $\mathscr{R}$ est semi-simple et simplement connexe, puis au cas où $\mathscr{R}$ est irréductible.

Définition 1.13. — On dit qu'une donnée radicielle $\mathscr{R} = (M, M^\vee, R, R^\vee)$ est « *triviale* » de rang s si $R = \varnothing$, i.e. si $\mathscr{R}$ est la donnée de deux groupes abéliens de rang s duaux l'un de l'autre $(M, M^\vee)$, i.e. si $\mathscr{R}$ est la donnée radicielle d'un k-tore déployé S de dimension s.

On peut démontrer les résultats suivants (cf. [SGA3], §XXI.6 et §XXIV.1).

Théorème 1.14. — *Soient H un k-groupe réductif déployé de type $\mathscr{R}$, T un k-tore déployé de dimension* $\mathrm{rang}(\mathscr{R})$*, de sorte que $\mathscr{R} \simeq (X(T), X_*(T), R, R^\vee)$. Soit Z la composante connexe du centre de H et soit H_{sc} l'unique k-groupe semi-simple déployé simplement connexe de type R ; notons* $\mathrm{sc}(\mathscr{R})$ *sa donnée radicielle. Soit Δ une base de R et $\mathscr{D}$ son diagramme de Dynkin.*

(i) *Z est le sous-groupe fermé* $\mathrm{Spec}(k\overline{M})$ *de T, où $\overline{M} = X(T)/X(T) \cap \mathbb{Q}R$. On note* $\mathrm{rad}(\mathscr{R})$ *la donnée radicielle triviale* $(\overline{M}, \mathrm{Hom}_{\mathbb{Z}}(\overline{M}, \mathbb{Z}))$.

---

(2) Pour obtenir cet isomorphisme, il faut fixer un « *épinglage* » de H, i.e. un k-tore déployé T de rang $\mathrm{rang}(\mathscr{R})$ et pour tout $\alpha \in \Delta$ un générateur X_α de $\mathrm{Lie}(H)_\alpha$.

(3) Ceci montre que la condition « simplement connexe ou adjoint » est une condition *suffisante*, mais pas nécessaire, pour avoir l'égalité $\mathrm{Aut}(\mathscr{R}, \Delta) = \mathrm{Aut}(\mathscr{D})$.

(ii) *Posons $\widetilde{H} = Z \times H_{\mathrm{sc}}$. Il existe un morphisme surjectif canonique $\pi : \widetilde{H} \to H$, dont le noyau est isomorphe à un sous-schéma en groupes fermé du centre de H_{sc}.*

(iii) *π correspond à un morphisme de données radicielles $\mathscr{R} \to \mathrm{rad}(\mathscr{R}) \times \mathrm{sc}(\mathscr{R})$ et l'on a $\mathrm{Aut}(\mathscr{R}, \Delta) \subset \mathrm{Aut}_{\mathbb{Z}}(\overline{M}) \times \mathrm{Aut}(\mathscr{D})$. Par conséquent, comme $\widetilde{H}$ et H ont le même groupe adjoint associé, on a pour tout corps K contenant k :*

$$\mathrm{Aut}_{K\text{-gpe}}(H_K) \subset \mathrm{Aut}_{K\text{-gpe}}(\widetilde{H}_K).$$

Remarques 1.15. — 1) Le dual de $\overline{M}$ s'identifie à $R^{\perp} = \{\mu \in M^{\vee} \mid (\alpha, \mu) = 0,\ \forall \alpha \in R\}$.

2) Posons $N = (R^{\vee})^{\perp} = \{\chi \in M \mid (\chi, \alpha^{\vee}) = 0, \forall \alpha \in R\}$ et notons π la projection $M \to M/N$. Alors $(M/N, M^{\vee} \cap \mathbb{Q}R^{\vee}, \pi(R), R^{\vee})$ est une donnée radicielle semi-simple, notée dér$(\mathscr{R})$.

3) Posons $P(R^{\vee}) = \{\chi \in (M/N) \otimes \mathbb{Q} \mid (\chi, \alpha^{\vee}) \in \mathbb{Z},\ \forall \alpha \in R\}$. Alors $\mathrm{sc}(\mathscr{R}) = (P(R^{\vee}), \mathbb{Z}R^{\vee}, \pi(R), R^{\vee})$.

2. Descente inséparable

Soient H un k-groupe réductif **déployé** de type $\mathscr{R}$ et G un k-groupe réductif tel que $G \otimes \overline{k} \simeq H \otimes \overline{k}$. Le but de cette courte section est de montrer qu'alors on a déjà $G \otimes k_s \simeq H \otimes k_s$. Si $\mathrm{car}(k) = 0$ alors $k_s = \overline{k}$ et il n'y a rien à montrer. On peut donc supposer que $\mathrm{car}(k) = p > 0$.

D'après un théorème de Grothendieck ([SGA3, t. II, Exp. XIV, Th. 3.20], voir aussi [Sp, Th. 13.3.6]), G contient un k-tore S de dimension $r = \mathrm{rang}(\mathscr{R})$. Posons $A = k[S]$. Alors $S \otimes \overline{k}$ est déployé, et il suffit de montrer que $S \otimes k_s$ est déployé, car ceci entraînera que $G \otimes k_s$ est un k-groupe réductif déployé de type $\mathscr{R}$, donc isomorphe à $H \otimes k_s$ par unicité. Posons $\Lambda = \mathbb{Z}^r$.

Lemme 2.1. — *Il existe un corps L tel que $k_s \subset L \subset \overline{k}$ et $[L : k_s] < \infty$ et un isomorphisme d'algèbres de Hopf $\phi : L\Lambda \xrightarrow{\sim} A \otimes L$.*

Démonstration. — Par hypothèse, il existe un tel isomorphisme $\psi : \overline{k}\Lambda \xrightarrow{\sim} A \otimes \overline{k}$. Notant $(\chi_1, \ldots, \chi_r)$ la base canonique de $\Lambda = \mathbb{Z}^r$ on peut écrire :

$$\psi(\chi_i) = \sum_{j=1}^{N} a_{ij} \otimes \lambda_{ij}$$

avec $a_{ij} \in A$ et $\lambda_{ij} \in \overline{k}$. Le sous-corps L de $\overline{k}$ engendré sur k_s par les λ_{ij} est de degré fini sur k_s et ψ induit un isomorphisme ϕ de $L\Lambda$ sur une sous-L-algèbre de Hopf A' de $A_L = A \otimes L$. Et, comme $A' \otimes_L \overline{k} = \mathrm{Im}(\psi) = A \otimes \overline{k} = A_L \otimes_L \overline{k}$, on a nécessairement $A' = A_L$. □

D'autre part, comme k_s est la clôture séparable de k dans $\overline{k}$ alors tout $x \in L$ est *radiciel* sur k_s, i.e. il existe $n \in \mathbb{N}$ tel que $x^{p^n} \in k_s$. On en déduit qu'il existe une suite de sous-corps

$$k_s = K_0 \subset K_1 \subset \cdots \subset K_m = L$$

telle que chaque K_i soit radiciel d'exposant 1 sur K_{i-1}, c.-à-d. $x^p \in K_{i-1}$ pour tout $x \in K_i$, condition qu'on écrit : $K_i^p \subset K_{i-1}$. (Pour tout ceci, voir [BALg, Chap. V, §5 et §7].) En procédant par récurrence sur m, on voit donc qu'il suffit de démontrer la proposition suivante :

Proposition 2.2. — *Soient $K \subset L$ des corps contenant k_s et tels que $L^p \subset K$. Alors tout isomorphisme de L-algèbres de Hopf $\phi : L\Lambda \xrightarrow{\sim} A \otimes L$ envoie Λ dans $A \otimes K$ donc provient d'un isomorphisme de K-algèbres de Hopf $K\Lambda \xrightarrow{\sim} A \otimes K$.*

Pour démontrer la proposition, on a besoin de la généralisation suivante de la théorie de Galois, due à Nathan Jacobson (cf. [BAlg, §V.13]).

Définition 2.3. — Soit $K \subset L$ une extension de corps. L'ensemble $\mathfrak{g} = \mathrm{Der}_K(L)$ des K-dérivations de L est l'ensemble des applications K-linéaires $\partial : L \to L$ telles que $\partial(ab) = \partial(a)b + a\partial(b)$ pour tout $a, b \in L$.

Noter que cette condition entraîne que $\partial(1) = \partial(1)+\partial(1)$ d'où $\partial(1) = 0$ et donc $\partial(a) = 0$ pour tout $a \in K$ puisque ∂ est K-linéaire. Notant $L^{\mathfrak{g}} = \{x \in L \mid \forall \partial \in \mathfrak{g},\ \partial(x) = 0\}$, on a donc $K \subset L^{\mathfrak{g}}$.

(Si $\partial, \partial' \in \mathfrak{g}$, on vérifie facilement que le crochet $[\partial, \partial'] = \partial \circ \partial' - \partial' \circ \partial$ appartient à $\mathfrak{g}$, donc $\mathfrak{g}$ est une sous-algèbre de Lie de $\mathrm{End}_K(L)$.)

Proposition 2.4. — *Avec les notations précédentes, supposons que* $\mathrm{car}(K) = p$ *et que l'extension* L/K *soit radicielle de hauteur* ≤ 1*, i.e. telle que* $x^p \in K$ *pour tout* $x \in L$*. Alors on a* $L^{\mathfrak{g}} = K$*.*

Conservons les hypothèses de la proposition précédente. Pour tout K-espace vectoriel V, l'espace vectoriel $V_L = V \otimes_K L$ est muni d'une action de $\mathfrak{g}$, définie par $\partial_V(v \otimes x) = x \otimes \partial(x)$, pour tout $v \in V$, $x \in L$ et $\partial \in \mathfrak{g}$. Identifiant V à $V \otimes 1$, on obtient le :

Corollaire 2.5. — V *égale* $V_L^{\mathfrak{g}} = \{w \in V_L \mid \forall \partial \in \mathfrak{g}, \quad \partial(w) = 0\}$.

Démonstration. — En effet, l'inclusion $\subset$ est claire. Réciproquement, soit $w \in V_L^{\mathfrak{g}}$. On peut écrire $w = \sum_{i=1}^n v_i \otimes a_i$ avec $a_i \in L$ et les $v_i \in V$ linéairement indépendants. Alors l'égalité

$$0 = \partial(w) = \sum_{i=1}^{n} v_i \otimes \partial(a_i)$$

entraîne que $\partial(a_i) = 0$ pour tout $\partial \in \mathfrak{g}$, d'où $a_i \in K$ d'après 2.4 et donc $w \in V$. □

La construction précédente est clairement fonctorielle, i.e. pour toute application K-linéaire $f : U \to V$ on a $\partial_V \circ (f \otimes \mathrm{id}_L) = f \otimes \partial = (f \otimes \mathrm{id}_L) \circ \partial_U$. En particulier, si $V = A$ est une K-algèbre, alors pour tous $a, b \in A$ et $\lambda, \mu \in L$, posant $x = a \otimes \lambda$ et $y = b \otimes \mu$, on a pour tout $\partial \in \mathfrak{g}$:

$$\partial(xy) = \partial(ab \otimes \lambda\mu) = ab \otimes \partial(\lambda\mu) = (a \otimes \partial(\lambda))(b \otimes \mu) + (a \otimes \lambda)(b \otimes \partial(\mu)) = \partial(x)y + x\partial(y),$$

donc ∂_A est une K-dérivation de A.

On peut maintenant démontrer la proposition 2.2 : soit $\chi \in \Lambda$ et $y = \phi(\chi) \in A \otimes L$. Notons Δ_A (resp. Δ) la comultiplication de A (resp. de $L\Lambda$) et soit $\partial \in \mathfrak{g} = \mathrm{Der}_K(L)$. Comme ϕ est un morphisme d'algèbres de Hopf, on a :

$$\Delta_A(\partial_A(y)) = (\Delta_A \circ \partial_A \circ \phi)(\chi) = (\partial_{A\otimes A} \circ \Delta_A \circ \phi)(\chi) = (\partial_{A\otimes A} \circ (\phi \otimes \phi) \circ \Delta)(\chi) = \partial(y \otimes y)$$

et comme $\partial = \partial_{A\otimes A}$ est une dérivation de $A \otimes A$, on a :

$$\partial(y \otimes y) = \partial\Big((y \otimes 1)(1 \otimes y)\Big) = \partial(y) \otimes y + y \otimes \partial(y).$$

Et comme $y^{-1} = \phi(\chi^{-1})$ vérifie $\Delta_A(y^{-1}) = y^{-1} \otimes y^{-1}$, on obtient que $x = y^{-1}\partial(y)$ vérifie

$$\Delta_A(x) = x \otimes 1 + 1 \otimes x.$$

Donc x définit un morphisme de L-algèbres de Hopf $L[\mathbb{G}_{a,L}] \to A \otimes L$, i.e. un morphisme de L-groupes algébriques $S \otimes L \to \mathbb{G}_{a,L}$. Par extension des scalaires, on obtient un morphisme de $\overline{k}$-groupes algébriques de $S \otimes \overline{k} \simeq (\mathbb{G}_{m,\overline{k}})^r$ vers $\mathbb{G}_{a,\overline{k}}$, qui est nécessairement trivial puisque $(\mathbb{G}_{m,\overline{k}})^r$ est diagonalisable et $\mathbb{G}_{a,\overline{k}}$ unipotent. Donc $x = 0$.

Une autre façon de montrer que $x = 0$ est la suivante. Notant $x' = \phi^{-1}(x) \in L\Lambda$, on peut écrire de façon unique $x' = \sum_{\mu\in\Lambda} c_\mu\mu$, avec les c_μ dans L et nuls sauf pour un nombre fini d'indices. L'égalité $\Delta(x') = x' \otimes 1 + 1 \otimes x'$ donne alors :

$$\sum_\mu c_\mu\, \mu \otimes \mu = \sum_\mu c_\mu\mu \otimes 1 + \sum_\mu 1 \otimes c_\mu\mu = (c_1 + \sum_\mu c_\mu\mu) \otimes 1 + \sum_{\mu\neq 1} c_\mu \otimes \mu.$$

Comme les $\mu' \otimes \mu$ sont linéairement indépendants, on en déduit que $c_\mu = 0$ pour $\mu \neq 1$, puis que $c_1 = 0$, d'où $x' = 0$ et donc $x = 0$.

Comme $0 = x = y^{-1}\partial(y)$, on obtient $\partial(y) = 0$ pour tout $\partial \in \mathfrak{g}$, donc $y = \phi(\chi)$ appartient à A d'après 2.5. Il en résulte que $\phi(\Lambda) \subset A$, donc ϕ induit un isomorphisme de $K\Lambda$ sur une sous-K-algèbre A' de A, et comme $A' \otimes_K L = \phi(L\Lambda)$ égale $A \otimes_K L$, on obtient que $A' = A$. Ceci achève la preuve de la proposition 2.2.

Par conséquent, on a obtenu le théorème suivant :

Théorème 2.6. — *Soient H un k-groupe réductif* **déployé** *de type $\mathscr{R}$ et G un k-groupe réductif qui est isomorphe à H sur $\overline{k}$, i.e. tel que $G\otimes\overline{k} \simeq H\otimes\overline{k}$. Alors G est déjà isomorphe à H sur k_s, i.e. on a $G \otimes k_s \simeq H \otimes k_s$.*

3. Descente et cohomologie galoisiennes

Soit K/k une extension galoisienne, de groupe de Galois Γ. (On n'impose pas $[K : k] < \infty$, en particulier on pourra prendre $K = k_s$.)

Définition 3.1 **(Actions continues de Γ)**. — Une action de Γ sur un ensemble X est dite **continue** si, pour tout $x \in X$, il existe une extension galoisienne *finie* L_x/k telle que le sous-groupe $\Delta_x = \mathrm{Gal}(K/L_x) = \{\gamma \in \Gamma \mid \forall\lambda \in L_x,\ \gamma(\lambda) = \lambda\}$ soit contenu dans le stabilisateur Γ_x de x.

Comme $\Gamma/\Delta_x \simeq \mathrm{Gal}(L_x/k)$ est fini, ceci entraîne en particulier que l'orbite Γx est finie.

Remarque 3.2. — La terminologie s'explique comme suit : on munit Γ d'une structure de groupe topologique en déclarant qu'un sous-groupe est ouvert ssi il contient un sous-groupe $\mathrm{Gal}(K/L)$ pour une certaine extension galoisienne *finie* L/k. (Si K/k est elle-même finie, on peut prendre $L = K$ et l'on obtient ainsi la topologie discrète.) Alors, munissant X de la topologie discrète, la condition plus haut équivaut à dire que pour tout $x \in X$ l'application $\Gamma \to X$, $\gamma \mapsto \gamma x$ est continue.

Soit U un k-espace vectoriel et $V = K \otimes U$. L'action de Γ sur V, définie par $\gamma(\lambda \otimes u) = \gamma(\lambda) \otimes u$, vérifie les deux propriétés suivantes :

(1) Elle est **semi-linéaire**, i.e. pour tout $v \in V$ et $\lambda \in K$, on a $\gamma(\lambda v) = \gamma(\lambda)\gamma(v)$.

(2) Elle est **continue** : en effet, soit $v \in V$, on peut écrire $v = \sum_{i=1}^n \lambda_i \otimes u_i$ avec $u_i \in U$ et $\lambda_i \in K$, alors les λ_i sont contenus dans une sous-extension galoisienne L de degré fini sur k et Γ_x contient $\Delta_L = \mathrm{Gal}(K/L)$.

Définition 3.3 **(Actions semi-linéaires de Γ sur un K-ev)**

Soit V un K-ev muni d'une action **continue** de Γ. On dit qu'elle est **semi-linéaire** si elle vérifie la première condition plus haut :

(1) Pour tout $v \in V$ et $\lambda \in K$, on a $\gamma(\lambda v) = \gamma(\lambda)\gamma(v)$.

Ceci, combiné avec l'hypothèse de continuité, entraîne la propriété suivante :

(2′) Pour tout $v \in V$, il existe une extension galoisienne finie L/k et un L-sev $E \subset V$ de dimension finie, contenant v et stable par Γ, tels que l'action de Γ sur E se factorise par le quotient fini $\mathrm{Gal}(L/k) = \Gamma/\Delta$, où $\Delta = \mathrm{Gal}(K/L)$.

En effet, soit L/k une extension galoisienne finie telle que $\Delta_L = \mathrm{Gal}(K/L)$ soit contenu dans Γ_v. L'orbite Γv est finie, notons-la $\Gamma v = \{\gamma_i(v) \mid i = 0, \ldots, n\}$ et soit E le L-sev

de V qu'elle engendre. D'une part Δ_L est distingué dans Γ et contenu dans Γ_v donc dans $\Gamma_{\gamma_i(v)} = \gamma_i\Gamma_v\gamma_i^{-1}$ pour tout i ; d'autre part tout $w \in E$ s'écrit $w = \sum_i \lambda_i\gamma_i(v)$ avec $\lambda_i \in L$, donc pour tout $\gamma \in \Gamma$ on a :

$$\gamma(w) = \sum_i \gamma(\lambda_i)\gamma\gamma_i(v) = \sum_i \gamma(\lambda_i)\gamma_i(v).$$

Ceci montre que E est stable par Γ et que Δ_L y agit trivialement.

Notation. — Si V est un K-ev muni d'une action semi-linéaire continue de Γ, on pose

$$V^\Gamma = \{v \in V \mid \forall\gamma \in \Gamma, \quad \gamma(v) = v\}.$$

C'est un k-sev de V.

Lemme 3.4. — *Soient U un k-ev et $V = K \otimes U$ muni de l'action de Γ définie plus haut. Alors :*

(1) $V^\Gamma = U$.

(2) *Soit W un K-sev de V. Alors : W est Γ-stable $\iff W = K \otimes W^\Gamma$.*

Démonstration. — (1) Soit $v \in V^\Gamma$, écrivons $v = \sum_{i=1}^n \lambda_i \otimes u_i$, avec $\lambda_i \in K$ et les u_i linéairement indépendants dans U. Alors, pour tout $\gamma \in \Gamma$, l'égalité $v = \gamma(v)$ entraîne $\gamma(\lambda_i) = \lambda_i$ pour tout i, donc les λ_i sont dans $K^\Gamma = k$, d'où $v \in U$.

(2) L'implication $\Leftarrow$ est claire, prouvons $\Rightarrow$. D'après ce qui précède, $E = W^\Gamma$ est un k-sev de U ; notons F un supplémentaire de E dans U. Alors on a $V = (K \otimes E) \oplus (K \otimes F)$ et $K \otimes E \subset W$. Si cette inclusion était stricte, il existerait $w \in W - \{0\}$ s'écrivant :

$$(*) \qquad w = \lambda_1 \otimes f_1 + \cdots + \lambda_n \otimes f_n$$

avec $\lambda_i \in K$, les f_i linéairement indépendants dans F, et n *minimal* (d'où $\lambda_i \neq 0$ pour tout i). Remplaçant w par $\lambda_n^{-1}w$, on se ramène au cas où $\lambda_n = 1$. Soit $\gamma \in \Gamma$; comme W est Γ-stable alors

$$\gamma(w) - w = \sum_{i=1}^{n-1}(\gamma(\lambda_i) - \lambda_i) \otimes f_i$$

appartient à W, et par minimalité de n ceci entraîne que $\gamma(w) = w$ pour tout γ, d'où $w \in E$ ce qui contredit $(*)$. Cette contradiction montre que l'inclusion $K \otimes E \subset W$ est une égalité. □

***Proposition 3.5* (Lemme de Dedekind).** — *Soit A, L deux k-algèbres, L étant un corps. L'ensemble $X_k(A, L)$ des morphismes de k-algèbres $A \to L$ est une partie libre du L-espace vectoriel* $\mathrm{Hom}_k(A, L)$.

Démonstration. — Supposons qu'on ait une égalité $\mu_1\chi_1 + \cdots + \mu_n\chi_n = 0$, avec $\mu_i \in L$, les χ_i dans $X_k(A, L)$ deux à deux distincts et n *minimal*. Alors $\mu_i \neq 0$ pour tout i et $n > 1$. Comme $\chi_n \neq \chi_1$, il existe $a \in A$ tel que $\chi_n(a) \neq \chi_1(a)$. Alors, pour tout $b \in A$ on a :

$$\chi_n(a)\sum_i \mu_i\chi_i(b) = 0 = \sum_i \mu_i\chi_i(ab) = \sum_i \mu_i\chi_i(a)\chi_i(b)$$

d'où, par soustraction, $\sum_{i=1}^{n-1} \mu_i\big(\chi_n(a) - \chi_i(a)\big)\chi_i = 0$. Comme le coefficient de χ_1 est non nul, ceci contredit la minimalité de n. □

***Définition 3.6* (k-structures sur un K-ev).** — Soit V un K-ev. On dit qu'un sous-k-ev V_0 de V est une « *k-structure* » sur V si l'application naturelle $K \otimes V_0 \to V$ est un isomorphisme.

***Théorème 3.7* (Descente galoisienne des K-ev).** — *Soit V un K-ev muni d'une action semi-linéaire et continue de $\Gamma = \mathrm{Gal}(K/k)$. Le k-sev V^Γ est une k-structure sur V.*

Démonstration. — Posons $V_0 = V^\Gamma$ et soit ϕ l'application naturelle $K \otimes V_0 \to V$. Pour tout $\gamma \in \Gamma$, notons γ_0 (resp. γ_V) l'automorphisme semi-linéaire de $K \otimes V_0$ (resp. de V) défini par γ. Alors, pour tout $v_0 \in V_0$ et $\lambda \in K$ on a :

$$(\gamma_V \circ \phi)(\lambda \otimes v_0) = \gamma_V(\lambda v_0) = \gamma(\lambda)\gamma_V(v_0) = \gamma(\lambda)v_0 = (\phi \circ \gamma_0)(\lambda \otimes v_0).$$

Par conséquent, on a $\gamma_V \circ \phi = \phi \circ \gamma_0$ et il en résulte que le noyau W de ϕ est stable par l'action de Γ sur $K \otimes V_0$. D'après le lemme 3.4, on a donc $W = K \otimes W_0$ pour un certain k-sev W_0 de V_0. Or pour tout $x = 1 \otimes w_0 \in W_0$, on a $0 = \phi(x) = w_0$, d'où $x = 0$. Donc $W_0 = 0$ et $W = 0$, i.e. ϕ est injective.

Montrons que ϕ est surjective. Soit $v \in V$. Par hypothèse, il existe une sous-extension galoisienne L/k de degré fini et un L-sev E de V de dimension finie contenant v et Γ-stable tels que, notant Δ le sous-groupe distingué $\mathrm{Gal}(K/L)$, l'action de Γ sur E se factorise par $\overline{\Gamma} = \mathrm{Gal}(L/k) = \Gamma/\Delta$.

Alors $E_0 = E^{\overline{\Gamma}} = E^\Gamma \subset V_0$, donc il suffit de montrer que l'application $L \otimes E_0 \to E$ est surjective. Soit $f : E \to L$ une forme linéaire nulle sur E_0 et soit $x \in E$ fixé. Pour tout $\lambda \in L$, l'élément

$$y_\lambda = \sum_{\gamma \in \overline{\Gamma}} \gamma(\lambda x) = \sum_{\gamma \in \overline{\Gamma}} \gamma(\lambda)\gamma(x)$$

appartient à E_0 donc on a :

$$0 = f(y_\lambda) = \sum_{\gamma \in \overline{\Gamma}} f(\gamma(x))\gamma(\lambda) = \Big(\sum_{\gamma \in \overline{\Gamma}} a_\gamma \gamma\Big)(\lambda),$$

où $a_\gamma = f(\gamma(x))$. D'après le lemme de Dedekind, on a $a_\gamma = 0$ pour tout γ, d'où en particulier $0 = a_1 = f(x)$. Ceci montre que toute forme linéaire $f : E \to L$ nulle sur E_0 est nulle, donc E_0 engendre E comme L-espace vectoriel et donc $L \otimes E_0 \to E$ est surjectif. Ceci achève la preuve du théorème. □

Terminologie. — Dans la suite, lorsqu'on parlera d'une « action » de Γ sur un K-espace vectoriel, il sera sous-entendu (sauf mention du contraire) que l'action est semi-linéaire et continue.

Lemme 3.8. — *Soient V_1, V_2 deux K-ev avec une action de Γ. Alors $W_0 = V_1^\Gamma \otimes V_2^\Gamma$ est une k-structure sur $W = V_1 \otimes_K V_2$ et l'on a donc*

$$(V_1 \otimes_K V_2)^\Gamma = V_1^\Gamma \otimes V_2^\Gamma.$$

Démonstration. — D'après le théorème précédent, on a $V_i = K \otimes V_i^\Gamma$ pour $i = 1, 2$. Alors on a un isomorphisme canonique :

$$V_1 \otimes_K V_2 \xrightarrow{\sim} K \otimes V_1^\Gamma \otimes V_2^\Gamma, \qquad (\lambda \otimes v_1) \otimes_K (\mu \otimes v_2) \mapsto \lambda\mu \otimes v_1 \otimes v_2$$

donc W_0 est une k-structure sur W, et via l'identification plus haut on a $W^\Gamma = W_0$. □

Corollaire 3.9. — *Soit A un K-espace vectoriel muni d'une structure algébrique* donnée, *d'un des types ci-dessous :*

(1) *une structure de K-algèbre associative avec unité, de dimension finie sur K,*
(2) *une structure de K-algèbre de Hopf de type fini commutative,*

et munie d'une action de Γ respectant cette structure (à la semi-linéarité près). Alors A^Γ est une k-algèbre du même type et l'on a $A = K \otimes A^\Gamma$.

Démonstration. — Posons $A_0 = A^\Gamma$. D'après le théorème précédent, l'application K-linéaire $K \otimes A_0 \to A$ est bijective, donc il suffit de montrer que A_0 est une sous-k-algèbre (de Hopf) de A.

Soit 1 l'élément unité de A. L'hypothèse que Γ respecte la structure d'algèbre signifie, dans les deux cas, que $\gamma(1) = 1$ et $\gamma(ab) = \gamma(a)\gamma(b)$ pour tout $\gamma \in \Gamma$ et $a, b \in A$. Il en résulte que A_0 contient 1 et est stable par multiplication.

Dans le cas (2), notons $\Delta, \varepsilon, \tau$ la comultiplication, l'augmentation et l'antipode de A. L'hypothèse est que l'on a de plus $(\gamma \otimes \gamma)\Delta = \Delta\gamma$, $\gamma\varepsilon = \varepsilon\gamma$ et $\gamma\tau = \tau\gamma$ pour tout $\gamma \in \Gamma$. Les deux dernières conditions entraînent que $\varepsilon(A_0) \subset K^\Gamma = k$ et $\tau(A_0) \subset A_0$. La première entraîne, en tenant compte du lemme précédent, que $\Delta(A_0) \subset A_0 \otimes A_0$. □

Pour toute k-algèbre A d'un des types (1) ou (2) plus haut, on a les deux définitions suivantes.

***Définition 3.10* (Le foncteur en groupes $\mathscr{A}(L) = \mathrm{Aut}_{L\text{-alg}}(L \otimes A)$)**

Pour tout corps L contenant k, posons $A_L = L \otimes A$; c'est une L-algèbre du même type et l'on notera $\mathscr{A}(L)$ le groupe de ses automorphismes de L-algèbres.

Pour tout k-morphisme $L \to L'$, tout L-automorphisme α de A_L se prolonge de façon unique en un L'-automorphisme α' de $A_{L'} = L' \otimes_L A_L$ (défini par $\alpha'(\lambda' \otimes_L a) = \lambda' \otimes_L \alpha(a)$) et l'on obtient ainsi un morphisme de groupes $\mathscr{A}(L) \to \mathscr{A}(L')$, qui est injectif (car si $\alpha' = \mathrm{id}$ alors $\alpha = \mathrm{id}$).

On obtient ainsi un foncteur en groupes $L \mapsto \mathscr{A}(L)$.

***Définition 3.11* (Action de $\mathrm{Gal}(K/k)$ sur $\mathscr{A}(K)$).** — L'action de $\Gamma = \mathrm{Gal}(K/k)$ sur $A_K = K \otimes A$ est continue. Elle induit une action par conjugaison de Γ sur $\mathscr{A}(K)$: en effet, pour tout $\alpha \in \mathscr{A}(K)$, l'application ${}^\gamma\alpha = \gamma \circ \alpha \circ \gamma^{-1} : A_K \to A_K$ respecte la structure d'algèbre et est K-linéaire, car pour tout $a \in A$ et $\lambda \in K$ on a :

$$({}^\gamma\alpha)(\lambda \otimes a) = (\gamma \circ \alpha)\big(\gamma^{-1}(\lambda) \otimes a\big) \overset{(1)}{=} \gamma\big(\gamma^{-1}(\lambda)\alpha(a)\big) \overset{(2)}{=} \lambda\,(\gamma \circ \alpha)(a) \overset{(3)}{=} \lambda\,{}^\gamma\alpha(a),$$

où l'on a l'égalité (1) car α est K-linéaire, (2) par semi-linéarité de l'action, et (3) car $a = 1 \otimes a$ égale $\gamma^{-1}(a)$.

Ceci est une action *par automorphismes de groupe*, i.e. pour tout $\gamma \in \Gamma$ et $\alpha, \beta \in \mathscr{A}(K)$ on a :

$${}^\gamma(\alpha\beta) = \gamma\alpha\beta\gamma^{-1} = (\gamma\alpha\gamma^{-1})(\gamma\beta\gamma^{-1}) = {}^\gamma\alpha\,{}^\gamma\beta.$$

Comme on a supposé A de type fini sur k, cette action est **continue**. En effet, soit $x_1, \ldots, x_n$ un système de générateurs de A comme k-algèbre, alors tout $\alpha \in \mathscr{A}(K)$ est déterminé par ses valeurs sur les x_i. Fixons $\alpha \in \mathscr{A}(K)$; il existe une extension galoisienne finie L/k telle que les $\alpha(x_i)$ appartiennent tous à $L \otimes A$, alors pour tout $\gamma \in \Delta_L = \mathrm{Gal}(K/L)$, α et ${}^\gamma\alpha$ coïncident sur $x_1, \ldots, x_n$ donc sont égaux. Ceci montre que le stabilisateur Γ_α contient Δ_L.

De même, si $\alpha \in \mathscr{A}(k) \subset \mathscr{A}(K)$, i.e. si α provient d'un automorphisme α_0 de A, alors pour tout $a \in A$ on a $\alpha(a) = \alpha_0(a) \in A$, d'où $\gamma(\alpha(a)) = \alpha(a)$ et donc ${}^\gamma\alpha = \alpha$ pour tout $\gamma \in \Gamma$.

Réciproquement, si $\alpha \in \mathscr{A}(K)$ est invariant par Γ, alors le calcul précédent montre que α envoie A dans A, donc induit un isomorphisme α_0 de A sur une sous-algèbre A' de A, et comme $A' \otimes K = \alpha(A_K)$ égale A_K, on obtient que $A' = A$, i.e. α_0 appartient à $\mathscr{A}(k)$. On a donc obtenu :

$$\mathscr{A}(k) = \mathscr{A}(K)^\Gamma = \{\alpha \in \mathscr{A}(K) \mid \forall \gamma \in \Gamma, \quad {}^\gamma\alpha = \alpha\}.$$

Remarque 3.12. — En fait, les raisonnements plus haut montrent que, A étant de type fini sur k, le groupe $\mathscr{A}(K)$ est la réunion des sous-groupes $\mathscr{A}(L)$, pour L parcourant les extensions galoisiennes finies L/k contenues dans K/k (ce qui entraîne la continuité de l'action de Γ).

Définition 3.13 (**1-cocyles et** $H^1(\Gamma, \mathscr{A})$). — Soit $\mathscr{A}$ un groupe, muni d'une action continue de Γ par automorphismes de groupes.

(i) Un 1-cocycle (de Γ à valeurs dans $\mathscr{A}$) est une application $c : \Gamma \to \mathscr{A}$ vérifiant la condition suivante :

$$(\dagger) \qquad \forall \gamma, \gamma' \in \Gamma, \qquad c(\gamma\gamma') = c(\gamma)\, {}^{\gamma}c(\gamma')$$

et qui est **continue** en un sens qu'on va préciser. Notant e_Γ l'élément neutre de Γ et e celui de $\mathscr{A}$, la condition (†) entraîne $c(e_\Gamma) = e$, et la continuité de c signifie qu'il existe une extension galoisienne finie L/k telle que $c(\gamma\gamma') = c(\gamma)$ pour tout $\gamma' \in \Delta_L = \mathrm{Gal}(K/L)$. On note $Z^1(\Gamma, \mathscr{A})$ l'ensemble des 1-cocycles.

(ii) Pour tout $a \in \mathscr{A}$, l'application $c_a : \gamma \mapsto a^{-1}\, {}^{\gamma}a$ est un 1-cocycle.[(4)] Comme Γ agit par automorphismes de groupe on a $\gamma(e) = e$ pour tout γ, et donc c_e est l'application constante de valeur e, qu'on notera simplement e.

(iii) Deux cocycles c, c' sont dits **équivalents** s'il existe $a \in \mathscr{A}$ tel que $c(\gamma) = a^{-1}c'(\gamma)\, {}^{\gamma}a$ pour tout γ. En particulier, on dit qu'un cocyle c est trivial s'il est équivalent à e, i.e. s'il existe $a \in \mathscr{A}$ tel que $c = c_a$.

(iv) On note $H^1(\Gamma, \mathscr{A})$ l'ensemble des classes d'équivalence de cocycles ; ce n'est pas un groupe en général, mais il est « *pointé* » par la donnée de la classe des cocycles triviaux.

(v) Si l'action de Γ sur $\mathscr{A}$ est *triviale*, un cocycle n'est autre qu'un morphisme de groupes $\Gamma \to \mathscr{A}$ et $H^1(\Gamma, \mathscr{A})$ est l'ensemble de ces morphismes pris à conjugaison près par un élément de $\mathscr{A}$.

Remarque 3.14. — Si $\mathscr{A}$ est **abélien** la condition de cocyle s'écrit $c(\gamma\gamma') = c(\gamma) + {}^{\gamma}c(\gamma')$ et l'on voit que si c, c' sont des cocycles il en est de même de $c - c'$, donc $Z^1(\Gamma, \mathscr{A})$ est un groupe abélien. De plus, l'application $\partial : a \mapsto c_a$ est un morphisme de groupes, de noyau $\mathscr{A}^\Gamma = \{a \in \mathscr{A} \mid \forall \gamma \in \Gamma,\ {}^{\gamma}a = a\}$, et deux cocycles c, c' sont équivalents ssi $c - c' \in \mathrm{Im}(\partial)$. On a donc une suite exacte :

$$0 \longrightarrow \mathscr{A}^\Gamma \longrightarrow \mathscr{A} \xrightarrow{\partial} Z^1(\Gamma, \mathscr{A}) \longrightarrow H^1(\Gamma, \mathscr{A}) \longrightarrow 0.$$

Soit maintenant H un k-groupe réductif déployé, $\mathscr{R}$ sa donnée radicielle, épinglée par le choix d'une base Δ du système de racines, $Z(H)$ le centre de H et $H_{\mathrm{ad}} = H/Z(H)$ le k-groupe semi-simple déployé de type adjoint associé à H. Pour tout corps L contenant k, notons $\mathscr{A}(L) = \mathrm{Aut}_{L\text{-gpe}}(H \otimes L)$. On a vu dans la section 1 que $\mathscr{A}(k)$ contient un sous-groupe isomorphe à $\mathrm{Aut}(\mathscr{R}, \Delta)$ et que l'on a un isomorphisme

$$\mathscr{A}(L) \simeq H_{\mathrm{ad}}(L) \rtimes \mathrm{Aut}(\mathscr{R}, \Delta)$$

pour tout L.

D'autre part, rappelons que $K \subset k_s$ est une extension galoisienne de k, de groupe de Galois Γ.

Définition 3.15 (**k-formes**). — (1) Soit G un k-groupe réductif. On dira que G est une K/k-**forme** de H si les K-groupes algébriques $G \otimes K$ et $H \otimes K$ sont isomorphes ; lorsque $K = k_s$, on dira simplement k-**forme**. Comme $k[H]$ est une k-algèbre de Hopf *de type fini* on voit alors, comme dans la démonstration du lemme 2.1, qu'il existe une extension galoisienne *finie* L/k telle que $G \otimes L \simeq H \otimes L$.

(4) Comme l'action de Γ sur $\mathscr{A}$ est continue, Γ_a contient un certain Δ_L et l'on a bien $c_a(\gamma\gamma') = c_a(\gamma)$ pour tout $\gamma' \in \Delta_L$.

On dit que deux K/k-formes G et G' sont isomorphes s'il existe un k-isomorphisme $G \simeq G'$.

(2) D'autre part, soit A une k-algèbre associative avec unité, de dimension n^2 sur k. On dit que A est une K/k-**forme** de $A_0 = M_n(k)$ si $A \otimes K$ est isomorphe comme K-algèbre à $A_0 \otimes K = M_n(K)$; lorsque $K = k_s$, on dira simplement k-**forme**. Comme plus haut, on voit que toute k-forme de A_0 est une L/k-forme, pour une certaine extension galoisienne *finie* L/k.

(3) Plus généralement, ces définitions valent pour toute espèce de structure algébrique pour laquelle l'extension des scalaires a un sens. Par exemple, si $\mathrm{car}(k) \neq 2$ alors toutes les formes quadratiques non dégénérées sur k^n deviennent isomorphes sur k_s à la forme quadratique déployée Q_0 associée à la matrice J_n de 1.8,[(5)] donc toute forme quadratique non dégénérée sur k^n est une k-forme de Q_0.

Théorème 3.16. — *Avec les notations précédentes, posons* $\mathscr{A}(K) = \mathrm{Aut}_{K\text{-gpe}}(H_K)$ *et* $\mathscr{A}_0(K) = \mathrm{Aut}_{K\text{-alg}}(M_n(K))$. *Alors on a des bijections :*

$$\left\{ \begin{array}{c} K/k\text{-formes de } H \\ \text{à isomorphisme près} \end{array} \right\} \leftrightarrow \left\{ \begin{array}{c} \text{actions de } \Gamma \text{ sur } K \otimes k[H] \\ \text{par automorphismes de Hopf,} \\ \text{à équivalence près} \end{array} \right\} \leftrightarrow H^1(\Gamma, \mathscr{A}(K))$$

$$\left\{ \begin{array}{c} K/k\text{-formes de } M_n(k) \\ \text{à isomorphisme près} \end{array} \right\} \leftrightarrow \left\{ \begin{array}{c} \text{actions de } \Gamma \text{ sur } M_n(K) \\ \text{par automorphismes d'algèbre,} \\ \text{à équivalence près} \end{array} \right\} \leftrightarrow H^1(\Gamma, \mathscr{A}_0(K)).$$

Démonstration. — Traitons le premier cas, le second étant similaire. Posons $A = k[H]$ et $\mathscr{A} = \mathscr{A}(K)$. Pour abréger, on dira « action » de Γ sur A_K au lieu de « action par automorphismes d'algèbres de Hopf ».

Soit donnée une telle action. Alors les éléments invariants A_K^Γ forment une k-algèbre de Hopf B et, d'après le théorème 3.7, on a $K \otimes B = A_K$. Il est clair que B est géométriquement réduite car $B \otimes \overline{k} = A \otimes \overline{k}$ est réduite. Montrons que B est de type fini sur k. Soit $x_1, \ldots, x_n$ un système fini de générateurs de $A_K = B_K$; écrivons $x_j = \sum_i \lambda_{ij} \otimes b_{ij}$ avec $\lambda_{ij} \in K$, $b_{ij} \in B$ et notons B_0 la sous-k-algèbre de B engendrée par les b_{ij}. Alors $K \otimes B_0$ contient les x_j donc égale $A_K = K \otimes B$ et il en résulte que $B_0 = B$. Par conséquent $G = \mathrm{Spec}(B)$ est une k-forme de H.

On dit que deux actions de Γ sur A_K, notées $*$ et $*'$, sont *équivalentes* s'il existe $\alpha \in \mathscr{A}$ tel que $\alpha(\gamma * a) = \gamma *' \alpha(a)$ pour tout $a \in A_K$ et $\gamma \in \Gamma$. Dans ce cas, α induit un isomorphisme de k-algèbres de Hopf entre B, l'algèbre des invariants pour l'action $*$, et B', celle pour $*'$, et donc les k-formes G et G' obtenues sont k-isomorphes. On obtient ainsi une application dans le sens $\leftarrow$.

Enfin, soit G une k-forme de H et $B = k[G]$. *Choisissons* un isomorphisme de K-algèbres de Hopf $\phi : B_K \xrightarrow{\sim} A_K$. Notant γ_B l'action standard de γ sur $B_K = K \otimes B$ définie par $\gamma_B(\lambda \otimes b) = \gamma(\lambda) \otimes b$, définissons une nouvelle action de Γ sur A_K, notée $*_\phi$, par :

$$\gamma *_\phi (a) = (\phi \circ \gamma_B \circ \phi^{-1})(a).$$

(C'est bien une action semi-linéaire par automorphismes de Hopf, et elle est continue car pour tout $x \in A_K$ le stabilisateur $\Gamma_x = \Gamma_{\phi^{-1}(x)}$ contient un certain $\Delta_L = \mathrm{Gal}(K/L)$.) Cette action dépend du choix de l'isomorphisme ϕ, mais si l'on prend un autre isomorphisme $\psi : B_K \xrightarrow{\sim} A_K$ alors $\alpha = \psi\phi^{-1}$ appartient à $\mathscr{A}$ et pour tout $a \in A_K$ et $\gamma \in \Gamma$ on a $\alpha(\gamma *_\phi (a)) = \gamma *_\psi (\alpha(a))$, i.e. les deux actions $*_\phi$ et $*_\psi$ sont équivalentes. On obtient ainsi une application dans le sens $\rightarrow$. De

(5) Voir 3.25 plus loin.

plus, comme $\phi(\gamma_B(x)) = \gamma *_\phi \phi(x)$ pour tout $x \in B_K$, on voit que ϕ induit un isomorphisme de k-algèbres de Hopf entre B et les invariants dans A_K pour l'action $*_\phi$, donc les deux applications sont inverses l'une de l'autre. Ceci établit la première bijection.

Ensuite, on passe des actions aux cocycles comme suit. Fixant une application $c : \Gamma \to \mathscr{A}$, notons $\rho_c(\gamma)$ l'automorphisme semi-linéaire $c(\gamma) \circ \gamma$ de A_K (où le γ de droite agit sur A_K par l'action standard $\gamma(\lambda \otimes a) = \gamma(\lambda) \otimes a$), alors on a

$$\rho_c(\gamma)\rho_c(\gamma') = c(\gamma)\gamma\, c(\gamma')\gamma' = c(\gamma)\, {}^\gamma c(\gamma')\, \gamma\gamma'$$

et ceci égale $\rho_c(\gamma\gamma')$ si et seulement si c vérifie la condition de cocycle. On obtient ainsi une bijection entre actions de Γ sur A_K et 1-cocycles à valeurs dans $\mathscr{A}$, et elle préserve les relations d'équivalence car pour α fixé dans $\mathscr{A}$, l'égalité

$$c(\gamma)\gamma = \rho_c(\gamma) = \alpha^{-1}\rho'_c(\gamma)\alpha = \alpha^{-1}c'(\gamma)\gamma\alpha$$

équivaut à $c(\gamma) = \alpha^{-1}c'(\gamma)\gamma\alpha\gamma^{-1} = \alpha^{-1}c'(\gamma)\, {}^\gamma\alpha$ i.e. à l'équivalence de c et c'. Ceci achève la preuve du théorème. □

Remarque 3.17. — La notion de 1-cocycle à valeurs dans $\mathscr{A}(K)$ peut sembler plus compliquée que celle d'action semi-linéaire de Γ sur A_K. Mais l'avantage des cocycles est que l'on s'est débarassé de l'objet A_K, en ne conservant que l'action (par conjugaison) de Γ sur $\mathscr{A}(K)$. Par conséquent si l'on trouve, pour un autre type de structure où l'extension des scalaires fait sens, un k-objet S tel que le groupe d'automorphismes de S_K soit $\mathscr{A}(K)$, avec la même action de Γ, alors on aura des bijections :

$$\left\{ \begin{array}{c} K/k\text{-formes de } H \\ \text{à isomorphisme près} \end{array} \right\} \leftrightarrow H^1(\Gamma, \mathscr{A}(K)) \leftrightarrow \left\{ \begin{array}{c} K/k\text{-formes de } S \\ \text{à isomorphisme près} \end{array} \right\}$$

et donc la classification des K/k-formes de H pourra se faire en classifiant les K/k-formes de S. On en verra bien des exemples dans ce qui suit.

Commençons par des exemples où $\mathscr{A}(K) = \mathscr{A}(k) = \mathscr{A}$, auquel cas l'action de Γ sur $\mathscr{A}$ est triviale. Dans ce cas, on a vu que $H^1(\Gamma, \mathscr{A})$ est l'ensemble des classes d'équivalence de morphismes de groupes $\Gamma \to \mathscr{A}$, deux morphismes étant équivalents s'ils sont conjugués par un élément de $\mathscr{A}$.

Définition 3.18 **(Groupes de type multiplicatif)**. — Soient M un groupe abélien de type fini et G un k-schéma en groupes de type fini. On dit que G est un k-groupe *de type multiplicatif* de type M si $G \otimes \overline{k} \simeq D(M)_{\overline{k}} = \mathrm{Spec}(\overline{k}M)$. (Si $M = \mathbb{Z}^r$, ceci signifie que G est un k-tore de dimension r.)

Comme dans la proposition 2.2, on peut montrer qu'alors on a déjà $G \otimes k_s \simeq D(M)_{k_s} = \mathrm{Spec}(k_sM)$, donc G est une k-forme de $H = \mathrm{Spec}(kM)$. Comme $\mathrm{Aut}_{L\text{-gpe}}(H_L) = \mathrm{Aut}_{\mathbb{Z}}(M)$ pour tout corps L, on obtient la proposition suivante.

Proposition 3.19. — *Soit M un groupe abélien de type fini, $H = \mathrm{Spec}(kM)$, $\Gamma = \mathrm{Gal}(k_s/k)$.*

(i) *Les classes d'isomorphisme de k-formes de H sont en bijection avec les morphismes de groupes $\Gamma \to \mathrm{Aut}_{\mathbb{Z}}(M)$, pris à conjugaison près.*

(ii) *En particulier les classes d'isomorphisme de k-tores de dimension r sont en bijection avec les morphismes de groupes $\Gamma \to \mathrm{GL}_r(\mathbb{Z})$, pris à conjugaison près.*

(iii) *En particulier, les classes d'isomorphisme de k-tores non déployés de dimension 1 sont en bijection avec les extensions L/k de degré 2 contenues dans k_s.*

Démonstration. — (i) découle de ce qui précède et (ii) en est un cas particulier. Prouvons (iii). Comme $\mathrm{GL}_1(\mathbb{Z}) = \{\pm 1\}$ est commutatif, les k-formes de $\mathbb{G}_{m,k}$, à isomorphisme près, sont en bijection avec les morphismes de groupe $\Gamma \to \{\pm 1\}$; le morphisme trivial correspond à $\mathbb{G}_{m,k}$ et chaque morphisme non trivial est déterminé par son noyau Δ, car il y a alors

un unique isomorphisme $\Gamma/\Delta \xrightarrow{\sim} \{\pm 1\}$. Or, d'après la théorie de Galois, les sous-groupes $\Delta \subset \Gamma$ d'indice 2 sont en bijection, via $\Delta \mapsto k_s^{\Delta}$, avec les extensions L/k de degré 2 contenues dans k_s. □

***Définition 3.20* (Action de $\mathrm{Gal}(K/k)$ sur les K-points d'un k-groupe G)**

Soit A une k-algèbre de type fini, $X = \mathrm{Spec}(A)$. L'action naturelle de Γ sur $A_K = K \otimes A$ induit une action de Γ sur $X(K) = \mathrm{Hom}_{K\text{-alg}}(A_K, K)$, définie par $\gamma \cdot x = \gamma_K \circ x \circ \gamma_{A_K}^{-1}$.

Si l'on choisit un système de générateurs de A, i.e. une surjection $k[X_1, \ldots, X_n] \to A$, i.e. une immersion fermée de X dans un espace affine $\mathbb{A}_k^n$, alors pour tout $x = (x_1, \ldots, x_n) \in X(K)$ on a simplement $\gamma \cdot x = (\gamma(x_1), \ldots, \gamma(x_n))$. En effet, on a :

$$(\gamma \cdot x)(1 \otimes X_i) = \gamma_K\big(x(1 \otimes X_i)\big) = \gamma(x_i).$$

Ceci montre que l'action sur $X(K)$ est **continue**, car pour chaque x ses coordonnées x_i appartiennent à une extension galoisienne finie L/k, donc le stabilisateur Γ_x contient Δ_L.

Évidemment, cette action de Γ est « fonctorielle », i.e. si $B \to A$ est un morphisme de k-algèbres, correspondant à un morphisme π de X vers $\mathrm{Spec}(B)$, alors pour tout $x \in X(K)$ et $\gamma \in \Gamma$, on a $\pi(\gamma(x)) = \gamma(\pi(x))$.

Maintenant, si G est un k-groupe algébrique et $A = k[G]$, Γ agit sur A_K par automorphismes d'algèbre de Hopf, donc agit sur $G(K)$ par automorphismes de groupes. Si l'on considère G comme sous-groupe fermé d'un certain $\mathrm{GL}_{N,k}$, alors pour tout $g = \big(g_{ij}\big)_{1 \le i,j \le N}$ on a simplement $\gamma \cdot g = \big(\gamma(g_{ij})\big)_{1 \le i,j \le N}$. En effet, $k[GL_{N,k}] = k[X_{ij}, \det^{-1}]$ et pour tout $g \in \mathrm{GL}_N(K)$ on a $(\gamma \cdot g)(1 \otimes X_{ij}) = \gamma_K\Big(g(1 \otimes X_{ij})\Big) = \gamma(g_{ij})$. Enfin, si $\pi : G \to G'$ est un morphisme de k-groupes algébriques alors pour tout $g \in G(K)$ et $\gamma \in \Gamma$ on a $\pi(\gamma(g)) = \gamma(\pi(g))$.

Remarque 3.21. — Attention, l'action de Γ sur $G(K)$ dépend du k-groupe G, et pas seulement du K-groupe G_K. Par exemple, soit G le $\mathbb{R}$-groupe $\mathrm{SU}_{2,\mathbb{R}}$ défini par

$$G(R) = \left\{ \begin{pmatrix} a+ib & -c+id \\ c+id & a-ib \end{pmatrix} \in \mathrm{GL}_2(R \otimes_{\mathbb{R}} \mathbb{C}) \;\middle|\; a^2+b^2+c^2+d^2 = 1 \right\}$$

pour toute $\mathbb{R}$-algèbre R. Alors $G(\mathbb{R}) = \mathrm{SU}(2)$ et l'on peut montrer que $G_{\mathbb{C}} \simeq \mathrm{SL}_{2,\mathbb{C}}$ donc $G(\mathbb{C}) \simeq \mathrm{SL}_2(\mathbb{C})$, mais que l'action de $\mathrm{Gal}(\mathbb{C}/\mathbb{R}) = \{\mathrm{id}, \sigma\}$ sur $\mathrm{SL}_2(\mathbb{C})$ provenant de l'action sur $\mathbb{C} \otimes_{\mathbb{R}} \mathbb{R}[G]$ est donnée par $\sigma(g) = {}^t\overline{g}^{-1}$, pour tout $g \in \mathrm{SL}_2(\mathbb{C})$.

***Théorème 3.22* (90 de Hilbert)**. — *On a* $H^1(\Gamma, \mathrm{GL}_n(K)) = \{1\}$.

Démonstration. — Ici, $\mathrm{GL}_n(K)$ est muni de l'action considérée plus haut, i.e. $\gamma \cdot (g_{ij}) = \big(\gamma(g_{ij})\big)$. D'autre part, Γ agit de façon naturelle sur K^n, et l'action sur $\mathrm{GL}_n(K)$ par conjugaison coïncide avec l'action précédente car pour tout $A \in M_n(K)$ et $X \in K^n$ on a : $\gamma(AX) = \gamma(A)\gamma(X)$ et donc, pour tout $g \in \mathrm{GL}_n(K)$:

$$(\gamma g \gamma^{-1})(X) = \gamma\big(g\gamma^{-1}(X)\big) = \gamma(g)X.$$

Soit maintenant $c : \Gamma \to \mathrm{GL}_n(K)$ un 1-cocycle. On définit une nouvelle action de Γ sur K^n en posant $\gamma * X = c(\gamma)\gamma X$; c'est bien une action car

$$\gamma * (\gamma' * X) = c(\gamma)\gamma c(\gamma')\gamma^{-1}\gamma\gamma' X = c(\gamma)\,{}^{\gamma}c(\gamma')\gamma\gamma' X = c(\gamma\gamma')\gamma\gamma' X = (\gamma\gamma') * X.$$

Notons V_0 le k-sev des invariants pour cette action. D'après le théorème 3.7, on a $K \otimes V_0 = K^n$ donc il existe une base $\mathscr{B}_0 = (v_1, \ldots, v_n)$ de K^n formée d'éléments de V_0. Notons $B = \mathrm{Mat}_{\mathrm{can}}(v_1, \ldots, v_n)$ la matrice exprimant les v_i dans la base canonique de K^n. Alors, comme $\gamma * v_i = v_i$ pour tout $\gamma \in \Gamma$, on a :

$$c(\gamma)\gamma(B) = \mathrm{Mat}_{\mathrm{can}}(\gamma * v_1, \ldots, \gamma * v_n) = B$$

et donc $c(\gamma) = B\gamma(B^{-1})$, ce qui prouve que c est équivalent au cocyle constant 1. □

Une conséquence très importante du « théorème 90 » est que l'on va pouvoir étendre le théorème 3.16 à tout sous-groupe fermé G de $\mathrm{GL}_{n,k}$ qui est le stabilisateur d'un certain tenseur $x \in T^{p,q}(V) = V^{\otimes p} \otimes (V^*)^{\otimes q}$, par exemple un groupe orthogonal ou symplectique (stabilisateur d'une forme bilinéaire non dégénérée, symétrique ou alternée).

Définition 3.23. — Soient $V = k^n$ et $x \in T^{p,q}(V)$. Pour tout corps L contenant k, tout $f \in \mathrm{GL}_n(L)$ induit un automorphisme $T^{p,q}(f)$ de $T^{p,q}(V_L) \simeq L \otimes T^{p,q}(V)$.

Une K/k-**forme** du couple (V, x) est un couple (V, x') isomorphe à (V, x) sur K, i.e. tel qu'il existe $f \in \mathrm{GL}_n(K)$ vérifiant $T^{p,q}(f)(1 \otimes x) = 1 \otimes x'$. On dit que (V, x') est isomorphe (sur k) à (V, x) s'il existe un tel f dans $\mathrm{GL}_n(k)$. Si $K = k_s$ on dira « k-formes » au lieu de « k_s/k-formes ».

Soit G le stabilisateur de x dans $\mathrm{GL}(V)$, i.e. pour toute k-algèbre R,

$$G(R) = \{g \in \mathrm{GL}_n(R) \mid T^{p,q}(g)(x \otimes 1) = x \otimes 1\}.$$

L'action de $\Gamma = \mathrm{Gal}(K/k)$ sur K^n induit une action par conjugaison de Γ sur $G(K)$. En effet, pour tout $\gamma \in \Gamma$ et $g \in G(K)$ on a :

$$\gamma g \gamma^{-1}(1 \otimes x) = \gamma g(1 \otimes x) = \gamma(1 \otimes x) = 1 \otimes x.$$

Théorème 3.24. — *L'ensemble $E(K/k)$ des classes d'isomorphisme de K/k-formes de (V, x) est en bijection avec $H^1(\Gamma, G(K))$.*

Démonstration. — Soit (V, x') une K/k-forme et soit $f \in \mathrm{GL}_n(K)$ tel que $T^{p,q}(f)(1 \otimes x) = 1 \otimes x'$. On définit une application $c_f : \Gamma \to G(K)$ en posant

$$c_f(\gamma) = f^{-1} \circ \gamma \circ f \circ \gamma^{-1} = f^{-1} \circ {}^{\gamma}f;$$

on vérifie facilement que c_f est un 1-cocycle, et si f' est un autre K-isomorphisme de (V, x) sur (V, x') alors $f' = f \circ \alpha$ avec $\alpha \in G(K)$ et donc $c_{f'}$ est équivalent à c_f. On obtient ainsi une application $E(K/k) \to H^1(\Gamma, G(K))$.

Montrons qu'elle est injective. Soient (V, x_1) et (V, x_2) deux k-formes donnant des cocycles équivalents ; il existe donc $\alpha \in G(K)$ tel que pour tout $\gamma \in \Gamma$ on ait $c_1(\gamma) = \alpha^{-1} c_2(\gamma)\, {}^{\gamma}\alpha$, c.-à-d. :

$$f_1^{-1} \circ \gamma \circ f_1 \circ \gamma^{-1} = \alpha^{-1} \circ f_2^{-1} \circ \gamma \circ f_2 \circ \alpha \circ \gamma^{-1}$$

et donc $h = f_2 \circ \alpha \circ f_1^{-1} \in \mathrm{GL}_n(K)$ est Γ-invariant donc appartient à $\mathrm{GL}_n(k)$. De plus,

$$T^{p,q}(h)(1 \otimes x_1) = T^{p,q}(f_2)T^{p,q}(\alpha)(1 \otimes x) = T^{p,q}(f_2)(1 \otimes x) = 1 \otimes x_2$$

donc h est un k-isomorphisme $(V, x_1) \xrightarrow{\sim} (V, x_2)$. Ceci prouve l'injectivité.

Prouvons la surjectivité. Soit $c : \Gamma \to G(K)$ un 1-cocyle. Comme $G(K) \subset \mathrm{GL}_n(K)$ et $H^1(\Gamma, \mathrm{GL}_n(K)) = \{1\}$, il existe $f \in \mathrm{GL}_n(K)$ tel que

$$c(\gamma) = f^{-1} \circ {}^{\gamma}f = f^{-1} \circ \gamma \circ f \circ \gamma^{-1}$$

pour tout γ. Posons $x' = T^{p,q}(f)(1 \otimes x)$; c'est un élément de $T^{p,q}(V_K) = K \otimes T^{p,q}(V)$. Pour montrer qu'il appartient à $T^{p,q}(V)$ il suffit de montrer qu'il est fixé par tout $\gamma \in \Gamma$. Pour alléger la notation, notons simplement f au lieu de $T^{p,q}(f)$. Alors on a :

$$\gamma(x') = \gamma f \gamma^{-1}(1 \otimes x) = f \circ c(\gamma)(1 \otimes x) = f(1 \otimes x) = x'$$

(la 1ère égalité car $1 \otimes x$ est Γ-invariant, la 3ème car $c(\gamma) \in G(K)$). Donc $x' \in T^{p,q}(V)$ et donc (V, x') est une K/k-forme de (V, x), pour laquelle f est un K-isomorphisme. Alors le cocycle c_f associé est précisément c. Ceci prouve la surjectivité. □

Corollaire 3.25. — a) *On a* $H^1(\mathrm{Gal}(K/k), \mathrm{Sp}_{2n}(K)) = \{1\}$.

b) *Supposons* $\mathrm{car}(k) \neq 2$ *et soit* $O(J_n)_k$ *le groupe orthogonal défini en 1.8. Alors* $H^1(\mathrm{Gal}(k_s/k), O(J_n)(k_s))$ *est en bijection avec les classes d'isomorphisme de formes quadratiques non dégénérées sur* k^n.

Démonstration. — a) On sait que pour tout corps L, toutes les formes symplectiques sur L^{2n} sont équivalentes. Donc, si ψ est une forme symplectique sur k^{2n}, son stabilisateur est isomorphe à Sp_{2n} et le H^1 en question est en bijection avec les classes d'isomorphisme de k-formes de ψ. Et comme elles sont toutes équivalentes, on a $H^1 = \{1\}$.

b) Comme $\mathrm{car}(k) \neq 2$, toutes les formes quadratiques q non dégénérées sur k_s^n sont équivalentes. En effet, q possède une base orthogonale $(e_1, \ldots, e_n)$; comme pour tout $a \neq 0$ le polynôme $X^2 - a$ est séparable, chaque $q(e_i)$ possède une racine carrée μ_i dans k_s et remplaçant e_i par $\mu_i^{-1} e_i$ on obtient une base orthonormée. Comme $O(J_n)_k$ est le stabilisateur de la forme quadratique définie par J_n, alors $H^1(\mathrm{Gal}(k_s/k), O(J_n)(k_s))$ est en bijection avec les classes d'isomorphisme de formes quadratiques non dégénérées sur k^n. □

Théorème 3.26. — *Soit* $1 \to H \to G \to \overline{G} \to 1$ *une suite exacte de* k*-groupes algébriques.* [6] *On a une suite exacte d'ensembles pointés :*

$$1 \longrightarrow H(k) \longrightarrow G(k) \xrightarrow{\pi} \overline{G}(k) \xrightarrow{h} H^1(\Gamma, H) \xrightarrow{g} H^1(\Gamma, G) \xrightarrow{f} H^1(\Gamma, \overline{G})$$

où $\Gamma = \mathrm{Gal}(k_s/k)$ *et* $H^1(\Gamma, H)$ *désigne* $H^1(\Gamma, H(k_s))$*, et où la notion de suite exacte d'ensembles pointés signifie :*

a) $H(k) = \mathrm{Ker}(\pi)$
b) $h^{-1}(e) = \mathrm{Im}(\pi)$
c) $g^{-1}(e) = \mathrm{Im}(h)$
d) $f^{-1}(e) = \mathrm{Im}(g)$

où e *désigne l'image dans chaque* H^1 *du cocyle trivial. En particulier,* π *est surjectif ssi* $\mathrm{Im}(h) = \{e\}$ *ssi* $g^{-1}(e) = \{e\}$.

Démonstration. — Voir [Se, §II.5]. □

Corollaire 3.27. — *Le morphisme* $\mathrm{GL}_n(k) \to \mathrm{PGL}_n(k)$ *est surjectif, donc* $\mathrm{PGL}_n(k) \simeq \mathrm{GL}_n(k)/k^\times$.

Démonstration. — Ceci résulte de $H^1(\Gamma, \mathbb{G}_m) = \{e\}$ (Hilbert 90). □

Revenons aux k-formes d'un k-groupe réductif déployé H. On a traité plus haut le cas d'un tore. La proposition suivante permet de se ramener au cas où H est semi-simple et simplement connexe. Rappelons (cf. 1.14) qu'il existe un morphisme surjectif canonique :

$$\widetilde{H} = Z \times H_{\mathrm{sc}} \xrightarrow{\pi} H,$$

où Z est la composante connexe du centre de H, H_{sc} est l'unique k-groupe semi-simple déployé simplement connexe ayant même système de racines que H, et $\mathrm{Ker}(\pi)$ est isomorphe à un sous-schéma en groupes fermé du centre de H_{sc}.

Proposition 3.28. — *Soit* G *une* K/k*-forme de* H*. Alors il existe, à isomorphisme près, une unique* K/k*-forme* $\widetilde{G}$ *de* $\widetilde{H}$ *et un morphisme surjectif* $\phi : \widetilde{G} \to G$ *tel que* $\phi \otimes K = \pi \otimes K$*. En particulier,* $\mathrm{Ker}(\phi)$ *est une* K/k*-forme de* $\mathrm{Ker}(\pi)$.

[6] Rappelons que ceci signifie que ce sont des k-schémas en groupes affines et *lisses*.

Esquisse de démonstration. — Soit G une K/k-forme de H, elle est donnée par un cocycle $c : \Gamma \to \mathrm{Aut}_{K\text{-gpe}}(H_K)$. Le morphisme surjectif $\pi : \widetilde{H} \to H$ induit une inclusion $k[H] \subset k[\widetilde{H}]$ et, d'après 1.14, on a

$$\mathrm{Aut}_{K\text{-gpe}}(H_K) \subset \mathrm{Aut}_{K\text{-gpe}}(\widetilde{H}_K)$$

donc l'action $*_c$ de Γ sur $K \otimes k[H]$ se prolonge en une action sur $K \otimes k[\widetilde{H}]$, pour laquelle la sous-algèbre des Γ-invariants définit une K/k-forme $\widetilde{G}$ de $\widetilde{H}$.

Alors l'inclusion $k[G] \subset k[\widetilde{G}]$ correspond à un morphisme surjectif $\phi : \widetilde{G} \to G$, tel que $\phi \otimes K = \pi \otimes K$. Alors, $\mathrm{Ker}(\phi) \otimes K = \mathrm{Ker}(\pi) \otimes K$, i.e. $\mathrm{Ker}(\phi)$ est une K/k-forme de $\mathrm{Ker}(\pi)$. □

Afin de faire une réduction supplémentaire, introduisons la définition suivante.

***Définition 3.29* (k-groupes géométriquement quasi-simples)**

Soit G un k-groupe semi-simple, de type $\mathscr{R}$.

(i) On dit que G est *quasi-simple* s'il n'a pas de sous-groupe fermé distingué $\neq G$ de dimension > 0.

(ii) Si $k = k_s$, on peut montrer que G est quasi-simple ssi $\mathscr{R}$ est irréductible, i.e. ssi le diagramme de Dynkin de $\mathscr{R}$ est connexe.

(iii) Revenant à notre corps de base k, on dit que G est *géométriquement quasi-simple* [7] si $G \otimes k_s$ est quasi-simple, i.e. si $\mathscr{R}$ est irréductible. Évidemment, dans ce cas G est quasi-simple.

(iv) Attention, la réciproque est fausse : si L/k est une extension séparable de degré $n > 1$ et si G_1 est un L-groupe semi-simple de type $\mathscr{R}$, où $\mathscr{R}$ est irréductible, on verra que le k-groupe $G = \mathrm{Res}_{L/k}(G_1)$ obtenu par « restriction des scalaires » est quasi-simple, mais sa donnée radicielle est $\mathscr{R} \times \cdots \times \mathscr{R}$ (n copies), donc G n'est pas géométriquement quasi-simple.

Remarque 3.30. — Avant de donner ci-dessous la définition de la restriction des scalaires en général, signalons que c'est la généralisation du fait suivant. Soit X une sous-variété fermée de $\mathbb{C}^N$, définie par des équations $P_\ell(z_1, \ldots, z_N) = 0$, pour $\ell = 1, \ldots, r$, avec $P_\ell \in A = \mathbb{C}[Z_1, \ldots, Z_N]$ et soit $d = \dim(X) =$ la dimension de Krull de la $\mathbb{C}$-algèbre $\overline{A} = A/(P_1, \ldots, P_r)$. Écrivons $z_j = x_j + iy_j$ avec $x_j, y_j \in \mathbb{R}$, alors pour tout $\ell = 1, \ldots, r$ on peut écrire

$$P_\ell(z_1, \ldots, z_n) = Q_\ell(x_j, y_j) + iR_\ell(x_j, y_j)$$

pour certains polynômes $Q_\ell, R_\ell \in B = \mathbb{R}[X_1, Y_1, \ldots, X_N, Y_N]$, uniquement déterminés. Posons $Y = \mathrm{Spec}(\overline{B})$, où $\overline{B}$ est le quotient de B par l'idéal engendré par les Q_ℓ et R_ℓ. Alors $Y(\mathbb{R}) = X(\mathbb{C})$ et l'on dit que Y est la variété réelle obtenue à partir de X par restriction des scalaires. On peut montrer que $\mathrm{Dim}(\overline{B}) = 2d$, i.e. Y est de dimension $2d$. De plus, pour toute $\mathbb{R}$-algèbre R, on a une bijection fonctorielle

$$\mathrm{Hom}_{\mathbb{R}\text{-alg}}(\overline{B}, R) = Y(R) \xrightarrow{\sim} X(R) = \mathrm{Hom}_{\mathbb{C}\text{-alg}}(\overline{A}, R \otimes \mathbb{C})$$

qui à tout $(x_1, y_1, \ldots x_N, y_N) \in Y(R)$ associe le point $(x_1 + iy_1, \ldots, x_N + iy_N)$ de $X(R \otimes \mathbb{C})$.

***Définition 3.31* (Restriction des scalaires à la Weil).** — Soit L/k une extension de corps de degré fini et soit $X = \mathrm{Spec}(A)$, où A est une L-algèbre de type fini. Le foncteur $Y = \mathrm{Res}_{L/k}(X)$, qui à toute k-algèbre R associe $X(R \otimes L)$, s'appelle la restriction des scalaires (de L à k) de X. On peut montrer, comme ci-dessus, que Y est représentable par un k-schéma affine X de type fini. [8]

---

[7] Hélas, l'ancienne terminologie « absolument quasi-simple » persiste dans la littérature.

[8] On peut montrer que si X est réduit et L/k *séparable* alors Y est réduit, mais nous n'aurons pas besoin de cela dans la suite.

On peut démontrer le théorème suivant (cf. [KMRT, Th. 26.8]).

Théorème 3.32. — *Soit G un k-groupe semi-simple simplement connexe (ou bien adjoint), soit $\mathscr{D}$ le diagramme de Dynkin de $G \otimes k_s$, $\mathscr{C}$ l'ensemble de ses composantes connexes et $\overline{\mathscr{C}} = \{\mathscr{O}_1, \ldots, \mathscr{O}_r\}$ l'ensemble des orbites de Γ dans $\mathscr{C}$. Pour $i = 1, \ldots, r$, tous les éléments de $\mathscr{O}_i$ sont des diagrammes de Dynkin de même type, disons D_i.*

Alors il existe des couples (L_i, G_i) pour $i = 1, \ldots, r$, où L_i/k est une extension séparable de degré $|\mathscr{O}_i|$ et G_i un L_i-groupe semi-simple simplement connexe de type D_i (donc géométriquement quasi-simple), uniques à isomorphisme près, tels que

$$G \simeq \mathrm{Res}_{L_1/k}(G_1) \times \cdots \times \mathrm{Res}_{L_r/k}(G_r).$$

De plus, chaque $\mathrm{Res}_{L_1/k}(G_1)$ est quasi-simple.

Démonstration. — à compléter □

Par conséquent, la classification des k-groupes semi-simples simplement connexes (ou bien adjoints) se ramène à celle des L-groupes géométriquement quasi-simples et simplement connexes (ou adjoints) sur une extension séparable L de k.

Exemple 3.33. — Prenons $k = \mathbb{R}$. La seule extension de $\mathbb{R}$ est $\mathbb{C}$, qui est algébriquement clos. Donc tout $\mathbb{R}$-groupe semi-simple simplement connexe est un produit de $\mathbb{R}$-groupes semi-simples de l'un des types suivants :

(1) $G = \mathrm{Res}_{\mathbb{C}/\mathbb{R}}(H)$, où H est un $\mathbb{C}$-groupe simplement connexe de type A_n, B_n, C_n, D_n, G_2, F_4, E_6, E_7 ou E_8. (Ceux-ci ont déjà été classifiés.)

(2) $G =$ une $\mathbb{R}$-forme d'un des groupes H précédents. (Celles-ci seront classifiées dans la section suivante, pour les types A, B, C, D.)

4. k-algèbres centrales simples

Dans cette section, on présente quelques résultats fondamentaux sur les k-algèbres centrales simples, qui seront utilisés dans la section suivante. Dans la suite, toutes les k-algèbres A considérées sont supposés *associatives et munies d'un élément unité.*

Définition 4.1 **(k-algèbres centrales simples)**. — Soit A une k-algèbre.

(1) Un idéal bilatère de A est un k-sev J tel que $J = AJA$, ie tel que $axb \in J$ pour tout $x \in J$ et $a, b \in A$.

(2) Un élément a de A est dit *central* si $ab = ba$ pour tout $b \in A$; l'ensemble de ces élements forme un sous-anneau (évidemment commutatif) appelé le *centre* de A et noté $Z(A)$.

(3) On dit que A est **simple** si elle n'a pas d'idéaux bilatères autres que A et (0). Dans ce cas $Z(A)$ est un *corps* K contenant k : en effet, pour tout $z \neq 0$ dans K, l'image de $\ell_z : a \mapsto za = az$ est un idéal bilatère non nul de A donc il existe $a \in A$ tel que $az = za = 1$, d'où $a = z^{-1}$; de plus pour tout $b \in A$ l'égalité $bz = zb$ entraîne $z^{-1}b = bz^{-1}$ d'où $z^{-1} \in K$.

(4) On dit que A est une k-algèbre « centrale simple » si elle est simple, *de dimension finie* sur k et de centre k. Par exemple, $M_n(k)$ est une k-algèbre centrale simple.

Pour établir le théorème 4.11 sur la structure d'une k-algèbre centrale simple A, il sera utile de considérer A comme A-module *à droite*. Pour cette raison, on considère au début des A-modules à gauche ou à droite. Par contre, on adopte la convention suivante.

Définition 4.2 **(Endomorphismes d'un A-module)**. — Pour tout A-module M on note $\mathrm{End}_A(M)$ l'anneau de ses endomorphismes, agissant **à gauche** sur M, i.e. si M est un A-module à gauche (resp. à droite) alors $\mathrm{End}_A(M)$ est l'ensemble des $f \in \mathrm{End}_k(M)$

tels que $f(am) = af(m)$ (resp. $f(ma) = f(m)a$) pour tout $a \in A$, $m \in M$, et l'on a $g(f(m)) = (g \circ f)(m)$ dans tous les cas.

***Définition 4.3* (Modules semi-simples)**. — Soient A une k-algèbre et M un A-module à gauche ou à droite non nul. On dit que M est **semi-simple** s'il est somme directe de sous-modules simples. Si de plus M est de type fini (i.e. engendré par un nombre fini d'éléments), il est somme directe d'un nombre fini de sous-modules simples, et l'on peut écrire :

$$M \simeq S_1^{n_1} \oplus \cdots \oplus S_r^{n_r}$$

où les S_i sont des modules simples deux-à-deux non isomorphes, uniquement déterminés ainsi que les n_i. On dit que M est *isotypique* si $r = 1$, i.e. si M est non nul et somme directe de modules simples tous isomorphes.

***Lemme 4.4* (de Schur)**. — *Soit S un A-module à gauche ou à droite simple.*

(i) *Son anneau d'endomorphismes* $\mathrm{End}_A(S)$ *est un corps D, éventuellement non commutatif, contenant k.*

(ii) *Si* $\dim_k(M) < \infty$ *alors D est un k-ev de dimension finie.*

Démonstration. — (i) Il est clair que $k \subset D$. Soit $f \in D - \{0\}$. Alors $\mathrm{Ker}(f)$ et $f(S)$ sont des sous-A-modules de S ; comme S est simple et $f \neq 0$ on obtient $\mathrm{Ker}(f) = \{0\}$ et $f(M) = M$, donc f est bijectif, d'où (i).

Si de plus $\dim_k(M) = n$ alors, comme $D \subset \mathrm{End}_k(M)$, on a $\dim_k(D) \leq n^2$. □

Du lemme précédent on déduit le :

Corollaire 4.5. — *Soient $S_1, \ldots, S_r$ des A-modules simples deux-à-deux distincts, D_i le corps* $\mathrm{End}_A(S_i)$ *et*

$$M = S_1^{n_1} \oplus \cdots \oplus S_r^{n_r}.$$

Alors $\mathrm{End}_A(M) \simeq M_{n_1}(D_1) \times \cdots \times M_{n_r}(D_r)$.

Démonstration. — Laissée au lecteur. Ou bien voir [Bl, Prop. II.5-6]. □

Définition 4.6. — Soit A une k-algèbre. On note A^{op} la k-algèbre *opposée* à A : elle a même espace vectoriel sous-jacent, mais le produit est défini par $a * b = ba$. Pour $a \in A$ on notera parfois a^{op} l'élément correspondant de A^{op}.

Alors, si M est un A-module à droite, c'est aussi un A^{op}-module à gauche pour l'action défini par $a^{\mathrm{op}} * m = ma$. En effet, on a bien :

$$b^{\mathrm{op}} * (a^{\mathrm{op}} * m) = (ma)b = m(ab) = (ab)^{\mathrm{op}} * m = (b^{\mathrm{op}} * a^{\mathrm{op}}) * m.$$

Lemme 4.7. — *Soit D un corps, non nécessairement commutatif, contenant k.*

(i) *La k-algèbre $A = M_n(D)$ est simple.*

(ii) *L'ensemble V' des vecteurs lignes à n éléments de D est un A-module à droite simple et* $\mathrm{End}_A(V') = D$, *i.e. V' est de façon naturelle un D-ev à gauche, sur lequel A agit à droite.*

(iii) *De même, l'ensemble V des vecteurs colonnes à n éléments de D est un A-module à gauche simple et* $\mathrm{End}_A(V) = D^{\mathrm{op}}$, *i.e. V est de façon naturelle un D-ev à droite, sur lequel A agit à gauche.*

Démonstration. — (i) Soit $a = (a_{ij})$ un élément non nul de A, il existe donc un couple (i_0, j_0) tel que $a_{i_0 j_0} \neq 0$. Désignant par E_{ij} la matrice élémentaire dont tous les coefficients sont nuls sauf celui d'indice (i, j) qui vaut 1, on a :

$$a_{i_0 j_0}^{-1} E_{i i_0} a E_{j_0 j} = E_{ij}.$$

On en déduit que l'idéal bilatère engendré par a égale A. La démonstration de (ii) et (iii) est laissée au lecteur. □

Proposition 4.8. — *Soit A une k-algèbre simple de dimension finie. Alors A est somme directe d'idéaux à droite simples.*

Démonstration. — Commençons par remarquer que tout idéal à droite non nul contient un sous-idéal non nul *de dimension minimale*, qui est donc un idéal à droite simple. Soit donc J un idéal à droite simple. Alors AJ est un idéal bilatère non nul, donc égal à A, donc $A = (AJ)^2 = AJAJ = AJ^2$, donc $J^2 \neq 0$.

Donc il existe $a \in J$ tel que le morphisme de A-modules à droite $\ell_a : J \to J$, $x \mapsto ax$ soit non nul. Comme J est simple, $\mathrm{Ker}(\ell_a) = 0$ et $\ell_a(J) = J$, donc il existe un *unique* $e \in J$ tel que $ae = a$. Alors $ae^2 = ae = a$ donc $e^2 = e$, i.e. e est *idempotent*. Comme J est simple, il est engendré par e, i.e. $J = eA$. Soit $f = 1 - e$, alors $f^2 = 1 + e^2 - 2e = 1 - e = f$, donc f est aussi idempotent, et comme $1 = e + f$ et $ef = fe = 0$, on a $A = eA \oplus fA$.

Supposons avoir trouvé des idempotents $e_1, \ldots, e_r$ deux-à-deux orthogonaux, i.e. tels que $e_i e_j = 0$ pour $i \neq j$, et tels que chaque idéal $e_i A$ soit simple. Alors $e = e_1 + \cdots + e_r$ est un idempotent, et posant $f = 1 - e$ on obtient comme plus haut que

$$A = eA \oplus fA \qquad \text{et} \qquad eA = \bigoplus_{i=1}^{r} e_i A$$

(comme $e_i e_j = 0$ pour $j \neq i$ on a $e_i = e e_i$ d'où $e_i A \subset eA$ et donc $eA = \sum_i e_i A$, de plus la somme est directe car si $e_i a = \sum_{j \neq i} e_j b_j$ alors $e_i a = e_i^2 a = 0$). Si $f = 0$ on a fini. Sinon, l'idéal fA contient un idéal à droite simple S, qui d'après le 1er paragraphe égale εA pour un certain idempotent ε. Comme $\varepsilon \in fA$ alors $\varepsilon = f\varepsilon$. Posons $e_{r+1} = \varepsilon f = f\varepsilon f$. Alors :

(1) $e_{r+1} \neq 0$ car $e_{r+1}\varepsilon = \varepsilon f \varepsilon = \varepsilon^2 = \varepsilon \neq 0$.

(2) $e_{r+1}^2 = \varepsilon f \varepsilon f = \varepsilon^2 f = \varepsilon f = e_{r+1}$ donc e_{r+1} est un idempotent.

(3) Pour tout $i = 1, \ldots, r$ on a $e_i = e e_i e$ d'où $e_i f = 0$ et $f e_i = 0$ et donc $e_i e_{r+1} = 0 = e_{r+1} e_i$.

Il en résulte que $A = \bigoplus_{i=1}^{r+1} e_i A \oplus f'A$, où $f' = f - e_{r+1}$. Comme $\dim_k(A) < \infty$, ce processus se termine après un nombre fini d'étapes et l'on obtient ainsi que

$$A = \bigoplus_{i=1}^{p} e_i A$$

pour des idempotents e_i deux-à-deux orthogonaux tels que chaque idéal $e_i A$ soit simple. □

Exemple 4.9. — Si $A = M_n(D)$, les matrices élémentaires E_{ii}, pour $i = 1, \ldots, n$, sont des idempotents deux-à-deux orthogonaux de somme 1, tels que chaque idéal à droite $E_{ii}A$ soit simple (c'est l'idéal à droite formé des matrices dont toutes les lignes sont nulles sauf la i-ème), et l'on a $A = \bigoplus_{i=1}^{n} E_{i,i} A$.

Terminologie 4.10. — Un corps D, éventuellement non commutatif, contenant k et de **dimension finie** sur k sera appelé un « *corps gauche* » sur k.

Théorème 4.11. — *Soit A une k-algèbre centrale simple de dimension finie. Il existe un corps gauche D de centre k, unique à isomorphisme près, et un entier $m \geq 1$ unique tels que $A \simeq M_m(D)$.*

Démonstration. — A est l'anneau des endomorphismes du A-module à droite A, et d'après la proposition précédente, celui-ci est somme directe de sous-modules simples. Donc d'après le corollaire 4.5 A est un produit direct d'algèbres, et comme A est simple il n'y a qu'un seul terme dans le produit (en effet, si $A \simeq A_1 \times A_2$ alors A_1, A_2 sont des idéaux bilatères non nuls) donc $A \simeq M_m(D)$, où D est un corps gauche contenant k. Alors $Z(A) = Z(D)$ donc $Z(D) = k$.

De plus, d'après 4.5, A est isotypique comme A-module à droite, i.e. tous ses idéaux à droite simples sont isomorphes. Si S désigne l'un d'eux, alors $D = \mathrm{End}_A(S)$. L'unicité de D à isomorphisme près en résulte, car si $A \simeq M_p(D')$ alors l'espace V' des matrices lignes à p éléments de D' est un A-module à droite simple et $D' = \mathrm{End}_A(V')$ d'après 4.7, d'où $D' \simeq D$. Enfin l'unicité de m en résulte car on a $\dim_k(A) = m^2 \dim_k(D)$.[9] □

Lemme 4.12. — *Soient A, B deux k-algèbres.*

(i) *L'application naturelle $M_n(k) \otimes A \to M_n(A)$ est un isomorphisme.*
(ii) *Prenant $A = M_p(k)$, on a un isomorphisme $M_n(k) \otimes M_p(k) \simeq M_n\big(M_p(k)\big) \simeq M_{np}(k)$.*
(iii) *On a un isomorphisme $M_n(A) \otimes M_p(B) \simeq M_{np}(k) \otimes A \otimes B \simeq M_{np}(A \otimes B)$.*

Démonstration. — Laissée au lecteur. Ou bien voir [Bl, Prop. II.13-14]. □

Remarque 4.13. — Tout corps gauche D sur $\overline{k}$ égale $\overline{k}$. En effet, soit $x \in D$, alors $\overline{k}[x]$ est une $\overline{k}$-algèbre commutative intègre de dimension finie sur $\overline{k}$, donc un corps de degré fini sur $\overline{k}$, donc égale $\overline{k}$.

Théorème 4.14. — *Soit A une k-algèbre centrale simple.*

(i) *Pour tout corps L commutatif contenant k, $A \otimes L$ est une L-algèbre centrale simple.*
(ii) *Il existe un unique entier n tel que $A \otimes \overline{k} \simeq M_n(\overline{k})$. On pose $n = \deg(A)$; alors $\dim_k(A) = \deg(A)^2$.*
(iii) *Pour toute k-algèbre centrale simple B, $A \otimes B$ est centrale simple.*

Démonstration. — Pour (i), on renvoie à [BAlg, §VIII.14]. Le point (ii) en découle, car $A_{\overline{k}} \simeq M_n(D)$ pour un certain entier n et D un corps gauche de centre $\overline{k}$. D'après la remarque plus haut, on a $D = \overline{k}$ et donc $\dim_k(A) = \dim_{\overline{k}}(A_{\overline{k}}) = n^2$.

Prouvons (iii). On a :

$$A \otimes B \otimes \overline{k} \simeq A_{\overline{k}} \otimes_{\overline{k}} B_{\overline{k}} \simeq M_n(\overline{k}) \otimes_{\overline{k}} M_p(\overline{k}) \simeq M_{np}(\overline{k})$$

donc $A \otimes B \otimes \overline{k}$ est simple et de centre $\overline{k}$. Ceci entraine facilement que $A \otimes B$ est simple et de centre k. □

Remarque 4.15. — Soit A une k-algèbre centrale simple, $n = \deg(A)$. Alors $A \simeq M_m(D)$ pour un unique corps gauche D de centre k (donc non commutatif si $D \neq k$). D'après le point (ii) plus haut, appliqué à D, on sait que $\dim_k(D) = \deg(D)^2$. Comme $n^2 = \dim_k(A) = m^2 \dim_k(D)$, on en déduit que $m = n/\deg(D)$.

Terminologie 4.16. — Une k-algèbre centrale simple A telle que $\deg(A) = 2$ est appelée une *algèbre de quaternions* : c'est soit $M_2(k)$ soit un corps gauche D de centre k, qu'on appelle un **corps de quaternions** sur k.

Si $k = \mathbb{R}$ il n'en existe qu'un à isomorphisme près, noté $\mathbb{H}$. Il a pour base $\{1, i, j, k\}$, où $i^2 = -1 = j^2 = k^2$ et $ij = k = -ji$. Il est muni d'un anti-automorphisme $q \mapsto \overline{q}$, où $\overline{q} = x1 - yi - zj - tk$ si $q = x1 + yi + zj + tk$; on a $\overline{q_1 q_2} = \overline{q_2}\,\overline{q_1}$ et $q\overline{q} = \overline{q}q = x^2 + y^2 + z^2 + t^2$.

Un résultat fondamental de la théorie des k-algèbres centrales simples est le théorème suivant (cf. [BAlg, §VIII.14.3] ou [Bl, Th. III-4]).

***Théorème 4.17* (de Skolem-Noether)**. — *Soient A une k-algèbre centrale simple et B une sous-algèbre simple de A, pas nécessairement de centre k.*[10]

[9] On peut aussi dire que m est déterminé par le fait que $A \simeq S^m$ comme A-modules à droite.
[10] Par exemple, B peut être un sous-corps commutatif de A, par exemple $B = \mathbb{C} \subset A = \mathbb{H}$, où $\mathbb{H}$ est le corps des quaternions, de centre $k = \mathbb{R}$.

(i) *Soit f un k-isomorphisme de B sur une sous-algèbre B' de A. Il existe $a \in A^\times$ tel que $f(b) = aba^{-1}$ pour tout $b \in B$.*

(ii) *En particulier, tout k-automorphisme α de A est* **intérieur** *: il existe $a \in A$ tel que $\alpha = \mathrm{Int}(a)$, i.e. $\alpha(b) = aba^{-1}$ pour tout $b \in A$. Comme $\mathrm{Int}(a') = \mathrm{Int}(a)$ ssi $a' = az$ avec $z \in Z(A)^\times = k^\times$, on obtient un isomorphisme $\mathrm{Aut}_{k\text{-alg}}(A) \simeq A^\times/k^\times$.*

(iii) *En particulier, pour $A = M_n(k)$ on a $\mathrm{Aut}_{k\text{-alg}}(M_n(k)) = \mathrm{GL}_n(k)/k^\times = \mathrm{PGL}_n(k)$.* [(11)]

Définition 4.18. — Soit A une k-algèbre centrale simple, $n = \deg(A)$. On dit qu'une extension algébrique L/k **déploie** A (ou que A est **déployée** sur L) si $A \otimes L \simeq M_n(L)$. Si $L \subset L'$ alors A est déployée sur L' car $M_n(L) \otimes_L L' \simeq M_n(L')$.

On a le résultat suivant (cf. [BAlg, §VIII.14, Th. 1] ou [Bl, Th. III.6 & Prop. III.3]).

Théorème 4.19. — *Soit A une k-algèbre centrale simple, $n = \deg(A)$.*

(i) *$A \otimes k_s \simeq M_n(k_s)$, i.e. A est déployée sur k_s.*

(ii) *Il existe une extension galoisienne K/k de degré fini qui déploie A.*

On en déduit que les k-algèbres centrales simples de degré n sont les k-**formes** de $M_n(k)$. Comme $\mathrm{Aut}_{k_s\text{-alg}}(M_n(k_s)) = \mathrm{PGL}_n(k_s)$ on en déduit que les classes d'isomorphisme de k-algèbres centrales simples de degré n sont en bijection avec $H^1(\Gamma, \mathrm{PGL}_n)$, où $\Gamma = \mathrm{Gal}(k_s/k)$.

Corollaire 4.20. — *Soit K/k une extension galoisienne de groupe de Galois Γ. Comme $\mathrm{Aut}_{K\text{-gpe}}(\mathrm{SL}_{2,K}) = \mathrm{PGL}_2(K)$, les K/k-formes de $\mathrm{SL}_{2,k}$ déployées sur K sont en bijection avec les k-algèbres de quaternions qui se déploient sur K.*

En particulier, si $k = \mathbb{R}$, l'unique forme non déployée est le groupe S^3 des quaternions de norme 1, i.e. pour tout $\mathbb{R}$-algèbre R :

$$S^3(R) = \{(x,y,z,t) \in R^4 = R \otimes \mathbb{H} \mid x^2 + y^2 + z^2 + t^2 = 1\} = \{u \in R \otimes \mathbb{H} \mid u\overline{u} = 1\}.$$

Définition 4.21 **(Norme)**. — Soit Λ un anneau commutatif, A une Λ-algèbre associative avec unité, V un A-module qui est un Λ-module libre de rang fini n. Pour tout $a \in A$, soit $\ell_V(a)$ le Λ-endomorphisme $x \mapsto ax$ de V et soit $P_V(a, X)$ son polynôme caractéristique ; c'est un polynôme unitaire de degré n. Son coefficient constant, égal à $\det(\ell_V(a))$ est noté $N_V(a)$ et appelé la *norme* de a relativement à V. Si V' est un second A-module vérifiant les mêmes hypothèses, on a

$$P_{V\oplus V'}(a,X) = P_V(a,X)P_{V'}(a,X) \qquad \text{et} \qquad N_{V\oplus V'}(a) = N_V(a)N_{V'}(a).$$

En particulier, si A elle-même est un Λ-module libre de rang fini n, on peut prendre $V = A$ et dans ce cas le polynôme caractéristique et la norme de a sont notés $P_{A/\Lambda}(a, X)$ et $N_{A/\Lambda}(a)$.

Proposition 4.22 **(Norme réduite)**. — *Soit A une k-algèbre centrale simple, $n = \deg(A)$.*

(i) *Pour tout $a \in A$, il existe un unique polynôme $Q(a, X) \in k[X]$ unitaire de degré n tel que $Q(a, X)^n = P_{A/k}(a, X)$. Le coefficient constant de $Q(a, X)$ s'appelle la* norme réduite *de a (relativement à A/k) et se note $\mathrm{Nrd}_{A/k}(a)$ ou simplement $\mathrm{Nrd}(a)$. On a $\mathrm{Nrd}(a)^n = N_{A/k}(a)$.*

(ii) *On obtient ainsi un morphisme de groupes $\mathrm{Nrd} : A^\times \to k^\times$.*

(iii) *Mieux : pour toute k-algèbre R, on a un morphisme de groupes $(A \otimes R)^\times \to R^\times$, fonctoriel en R.*

[(11)] Cf. 3.27.

Démonstration. — Soit L/k une extension galoisienne, de groupe de Galois Γ, telle que $A_L = A \otimes L \simeq M_n(L)$; alors A_L est somme directe de n modules simples tous isomorphes à L^n.

Soit $a \in A$ et $P = P_{A/k}(a, X) \in k[X]$ son polynôme caractéristique ; il est unitaire de degré n^2. Soit a' l'élément $a \otimes 1$ de A_L, alors P est aussi le polynôme caractéristique de a' relativement à A_L/L. Comme $A_L \simeq M_n(L)$ est somme directe de n modules simples tous isomorphes à $V = L^n$, on obtient que

$$(*) \qquad P = Q^n$$

où $Q = P_V(a', X)$ n'est autre que le polynôme caractéristique de la matrice $a' \in M_n(L)$. En utilisant la décomposition de P et Q en facteurs irréductibles, on voit que Q est l'unique polynôme unitaire de degré n vérifiant $(*)$. Comme $P \in k[X]$, on a $P = \gamma(P) = \gamma(Q)^n$ pour tout $\gamma \in \Gamma$, donc par unicité $\gamma(Q) = Q$, d'où $Q \in k[X]$. Notons $\mathrm{Nrd}(a) \in k$ le terme constant de Q, alors on a $\mathrm{Nrd}(a)^n = N_{A/k}(a)$, d'où (i).

D'autre part, pour tout $a, b \in A$ on a $\ell_V(ab) = \ell_V(a)\ell_V(b)$ donc Nrd est multiplicative, i.e. $\mathrm{Nrd}(ab) = \mathrm{Nrd}(a)\mathrm{Nrd}(b)$; de plus $\mathrm{Nrd}(1) = 1$ puisque $\ell_V(1) = \mathrm{id}_V$. Il en résulte que Nrd induit un morphisme de groupes $A^\times \to k^\times$, d'où (ii).

Prouvons (iii). Posons $N = n^2$ et soit $(e_1, \ldots, e_N)$ une base de A sur k. Soit Λ l'anneau de polynômes $k[X_1, \ldots, X_N]$, K son corps des fractions et $P \in \Lambda[X]$ le polynôme caractéristique de l'élément « générique » $\alpha = \sum_{i=1}^N X_i e_i$ de A_Λ. On obtient comme plus haut qu'il existe un unique polynôme $Q \in K[X]$ unitaire de degré n, tel que $Q^n = P$. Comme Λ est factoriel, on obtient en travaillant un peu que $Q \in \Lambda[X]$. Alors, pour toute k-algèbre R et $a = \sum_{i=1}^n r_i e_i \in A_R$, $P_{A_R/R}(a, X)$ est la spécialisation de P en $X_i = r_i$ pour $i = 1, \ldots, n$ et de même pour $Q(a, X)$. Le résultat voulu en découle. □

Exemple 4.23. — Prenons $k = \mathbb{R}$ et $A = \mathbb{H}$. Déterminons la norme réduite d'un quaternion q. On peut montrer que tout quaternion est conjugué à un élément de $\mathbb{C} = \mathbb{R} \oplus \mathbb{R}i$ (ceci résulte du théorème de Skolem-Noether 4.17), donc on va se limiter à faire le calcul pour $q = a + ib$, avec $a, b \in \mathbb{R}$. Dans ce cas, la matrice de ℓ_q dans la base $(1, i, j, k)$ est

$$\begin{pmatrix} a & -b & 0 & 0 \\ b & a & 0 & 0 \\ 0 & 0 & a & -b \\ 0 & 0 & b & a \end{pmatrix}$$

et son déterminant est $(a^2 + b^2)^2 = (q\overline{q})^2$. On en déduit que $\mathrm{Nrd}(q) = q\overline{q}$ pour tout $q \in \mathbb{H}$.

Revenons à la question des k-formes d'un k-groupe semi-simple déployé. Pour $n \geq 3$, le groupe des automorphismes du diagramme de Dynkin de SL_n est S_2 donc $\mathscr{A}(K) = \mathrm{Aut}_{K\text{-gpe}}(\mathrm{SL}_{n,K})$ est un produit semi-direct $\mathrm{PGL}_n(K) \rtimes S_2$. Dans la section suivante, on va interpréter $H^1(\Gamma, \mathscr{A}(K))$, pour $n \geq 3$, en termes d'algèbres « centrales simples à involution ». Mais d'abord introduisons le groupe de Brauer de k.

Définition 4.24 **(Groupe de Brauer)**. — On note $\mathrm{Br}(k)$ le quotient de l'ensemble des classes d'isomorphisme de k-algèbres centrales simples par la relation d'équivalence définie par $A \sim B$ s'il existe $p, q \in \mathbb{N}^*$ tels que $M_p(A) \simeq M_q(B)$. C'est bien une relation d'équivalence, car si $M_r(B) \simeq M_s(C)$ alors, d'après le lemme 4.12, on a :

$$M_{rp}(A) \simeq M_r(M_p(A)) \simeq M_r(M_q(B)) \simeq M_q(M_r(B)) \simeq M_q(M_s(C)) \simeq M_{qs}(C).$$

Cet ensemble est muni d'une loi de composition associative et commutative, définie par $[A_1] + [A_2] = [A_1 \otimes A_2]$, où $[A]$ désigne la classe de A dans $\mathrm{Br}(k)$. Cette loi est bien définie,

car si $M_{p_i}(A_i) \simeq M_{q_i}(B_i)$ pour $i = 1, 2$, alors

$$M_{p_1 p_2}(A_1 \otimes A_2) \simeq M_{p_1}(A_1) \otimes M_{p_2}(A_2) \simeq M_{q_1}(B_1) \otimes M_{q_2}(B_2) \simeq M_{q_1 q_2}(B_1 \otimes B_2)$$

donc $A_1 \otimes A_2$ et $B_1 \otimes B_2$ définissent la même classe. Bien entendu, l'élément neutre est la classe de $[k]$, qu'on notera 0. De plus, $\mathrm{Br}(k)$ est un *groupe*, d'après la proposition suivante.

Proposition 4.25. — *Soit A une k-algèbre centrale simple, $n = \deg(A)$. On a $A \otimes A^{\mathrm{op}} \simeq M_{n^2}(k)$. Par conséquent, $[A] + [A^{\mathrm{op}}] = 0$, i.e. $[A^{\mathrm{op}}]$ est l'opposé de $[A]$.*

Démonstration. — Posons $B = A \otimes A^{\mathrm{op}}$; c'est une k-algèbre centrale simple et A est un B-module à gauche via $(a_1 \otimes a_2^{\mathrm{op}}) \cdot a = a_1 a\, a_2$. Alors les sous-$B$-modules sont les idéaux bilatères de A, donc A est un B-module simple.

D'autre part, $\mathrm{End}_{A^{\mathrm{op}}}(A) = A$ car si $f : A \to A$ vérifie $f(aa_2) = f(a)a_2$ pour tout $a, a_2 \in A$, alors $f(a) = f(1a) = f(1)a$, donc f est la multiplication à gauche par l'élément $f(1)$. Donc $\mathrm{End}_B(A) \subset \mathrm{End}_{A^{\mathrm{op}}}(A)$ est l'ensemble des multiplications à gauche par les éléments du centre $Z(A)$ de A, qui par hypothèse est k. Donc d'après le théorème 4.11 on a $B \simeq M_m(k)$, avec $m^2 = \dim_k(B) = n^4$ d'où $m = n^2$. Ceci prouve (i), et (ii) en découle. □

On a de plus les théorèmes suivants.

Théorème 4.26. — *Soit D un corps gauche de centre k, de degré d. Alors $d \cdot [D] = 0$ dans* $\mathrm{Br}(k)$. *Par conséquent,* $\mathrm{Br}(k)$ *est un groupe abélien* de torsion*, i.e. tout élément est d'ordre fini.*

Démonstration. — Voir [Bl, Th. IV.4] ou [BAlg, §VIII.16.11, Cor. 1]. □

Définitions 4.27 **(Indice et exposant)**. — Soit A une k-algèbre centrale simple.

(i) Son *indice* $\mathrm{ind}(A)$ est $\deg(D)$, où D est l'unique corps gauche D tel que $A \simeq M_m(D)$.

(ii) Son *exposant* $\exp(A)$ est l'ordre de $[A]$ dans $\mathrm{Br}(k)$; d'après le théorème précédent on a $\mathrm{ind}(A)[A] = \deg(D)[D] = 0$ donc $\exp(A)$ divise $\mathrm{ind}(A)$.

Théorème 4.28. — *Soit A une k-algèbre centrale simple. Alors* $\exp(A)$ *et* $\mathrm{ind}(A)$ *ont les mêmes facteurs premiers.*

Démonstration. — Voir [BAlg, §VIII.16.11, Cor. 2]. □

5. Groupes classiques et k-algèbres centrales simples à involution

Définition 5.0 **(Involutions)**. — Soit A une k-algèbre de dimension finie. Une **involution** de A est une application k-linéaire $s : A \to A$ telle que $s^2 = \mathrm{id}_A$ et qui est un *anti-automorphisme* de la structure d'algèbre, i.e. $s(ab) = s(b)s(a)$ pour tout $a, b \in A$.[(12)] Ceci équivaut à dire que l'application $A \to A^{\mathrm{op}}$, $a \mapsto s(a)^{\mathrm{op}}$ est un isomorphisme de k-algèbres et que $s^2 = \mathrm{id}_A$.

[(12)] Il serait plus approprié de dire « *anti-involution* », mais **involution** est le terme consacré.

5.1. Formes de SL_n pour $n \geq 3$. — Fixons $n \geq 3$. Alors le groupe des automorphismes du diagramme de Dynkin $\mathscr{D}$ de type A_{n-1} est S_2 et l'automorphisme non trivial de $\mathscr{D}$ se relève en un automorphisme $i_\top : g \mapsto {}^\top g^{-1}$ de SL_n (et de GL_n) qui laisse stable le tore maximal des matrices diagonales et le sous-groupe de Borel des matrices triangulaires supérieures (resp. inférieures) : pour tout $g \in \mathrm{GL}_n(R)$, ${}^\top g$ est la « transposée de g par rapport à la seconde diagonale », i.e. si $g = \begin{pmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{pmatrix}$ alors ${}^\perp g = \begin{pmatrix} a_{33} & a_{23} & a_{13} \\ a_{32} & a_{22} & a_{12} \\ a_{31} & a_{21} & a_{11} \end{pmatrix}$. Si l'on note J_n l'élément de $\mathrm{GL}_n(k)$ dont tous les coefficients sont nuls sauf ceux de la seconde diagonale, qui valent 1, alors $J_n^2 = \mathrm{id}$ et ${}^\top g = J_n\, {}^t g J_n = \mathrm{Int}(J_n) \circ \tau$, où $\mathrm{Int}(J_n)$ désigne l'automorphisme intérieur défini par J_n.

On voit ainsi que $g \mapsto {}^\top g$ est un anti-automorphisme de SL_n (et de GL_n), et donc $i_\top : g \mapsto {}^\top g^{-1}$ est bien un automorphisme, d'ordre 2 (i.e. $i_\top^2 = \mathrm{id}$). D'après le théorème 1.11, pour tout corps K contenant k on a :

$$\mathrm{Aut}_{K\text{-gpe}}(\mathrm{SL}_{n,K}) \simeq \mathrm{PGL}_n(K) \rtimes \{1, i_\top\}$$

et comme $i_\top = \mathrm{Int}(J_n) \circ i_t$, où $i_t(g) = {}^t g^{-1}$, on a aussi :

$$\mathrm{Aut}_{K\text{-gpe}}(\mathrm{SL}_{n,K}) \simeq \mathrm{PGL}_n(K) \rtimes \{1, i_t\}.$$

D'autre part, comme on a la suite exacte

$$1 \longrightarrow \mu_n \longrightarrow \mathbb{G}_m \times \mathrm{SL}_n \longrightarrow \mathrm{GL}_n \longrightarrow 1,$$

où $\mathbb{G}_m$ est le centre de GL_n, on voit que se donner un automorphisme de GL_n revient à se donner un automorphisme α de SL_n et un élément β de $\mathrm{Aut}(\mathbb{G}_m) = \{\pm 1\}$ qui coïncide avec α sur μ_n. Or, pour $n > 2$, l'automorphisme non trivial $t \mapsto t^{-1}$ de $\mathbb{G}_m$ est déterminé par sa restriction à μ_n, donc on obtient $\mathrm{Aut}_{K\text{-gpe}}(\mathrm{SL}_{n,K}) = \mathrm{Aut}_{K\text{-gpe}}(\mathrm{GL}_{n,K})$, donc les k-formes de SL_n sont en bijections avec les k-formes de GL_n. [(13)] Posons

$$(\dagger) \qquad \mathscr{A}(K) = \mathrm{Aut}_{K\text{-gpe}}(\mathrm{SL}_{n,K}) = \mathrm{Aut}_{K\text{-gpe}}(\mathrm{GL}_{n,K}) \simeq \mathrm{PGL}_n(K) \rtimes \{1, i_t\}.$$

Montrons maintenant que le foncteur $K \mapsto \mathscr{A}(K)$ est le foncteur des automorphismes d'une autre k-structure algébrique, dont les k-formes sont plus faciles à classifier. Désignons par (A_0, s) le couple formé par la k-algèbre $A_0 = M_n(k) \times M_n(k)^{\mathrm{op}}$ et où $s(x, y^{\mathrm{op}}) = (y, x^{\mathrm{op}})$. Alors $s^2 = \mathrm{id}$ et s est un *anti-automorphisme* de A_0, car

$$\begin{aligned} s\big((x_1, y_1^{\mathrm{op}})(x_2, y_2^{\mathrm{op}})\big) = s(x_1x_2, (y_2y_1)^{\mathrm{op}}) = (y_2y_1, (x_1x_2)^{\mathrm{op}}) = (y_2, x_2^{\mathrm{op}})(y_1, x_1^{\mathrm{op}}) \\ = s(x_2, y_2)s(x_1, y_1), \end{aligned}$$

i.e. s est une **involution** de A_0 (cf. Définition 5.0). De plus, le centre de A_0 est $Z_0 = k \times k$; son groupe d'automorphisme est S_2 et la restriction de s à Z_0 est l'automorphisme non trivial : on dit que s est une involution de A_0 **de 2ème espèce**.

Pour tout corps K contenant k, posons $A_{0,K} = A_0 \otimes K$ et notons $\mathrm{Aut}_K(A_0, s)$ le groupe des automorphismes de K-algèbre α de $A_0 \otimes K$ qui préservent $s_K = s \otimes \mathrm{id}$, i.e. qui vérifient $\alpha \circ s_K = s_K \circ \alpha$.

Lemme 5.1. — *Soit $B = B_1 \times B_2$ un produit de deux K-algèbres centrales simples. Notons $\mathrm{Int}(B)$ le sous-groupe de $\mathrm{Aut}_{K\text{-alg}}(B)$ formé des automorphismes intérieurs.*

(i) *On a $\mathrm{Int}(B) = \mathrm{Aut}_{K\text{-alg}}(B)$ si B_1, B_2 ne sont pas K-isomorphes.*

(ii) *S'il existe un K-isomorphisme $\phi : B_1 \xrightarrow{\sim} B_2$ alors $\mathrm{Aut}_{K\text{-alg}}(B) \simeq \mathrm{Int}(B) \rtimes \{1, \sigma\}$, où σ est l'automorphisme de B défini par $\sigma(b_1, b_2) = \big(\phi^{-1}(b_2), \phi(b_1)\big)$.*

[(13)] Ceci n'est pas le cas pour $n = 2$, cf. [Se, §III.1.4, Exercices 1, 2].

Démonstration. — Commençons par remarquer que B n'a que deux idéaux bilatères non triviaux, qui sont B_1 et B_2. Donc tout automorphisme α de B laisse B_1 et B_2 stables, ou bien les échange.

Dans le premier cas, α induit un automorphisme de chaque B_i donc, d'après le théorème de Skolem-Noether, il existe $a_i \in B_i^\times$ tel que $\alpha(b) = a_i b a_i^{-1}$ pour tout $b \in B_i$, et donc α est l'automorphisme intérieur défini par (a_1, a_2). Si B_1 et B_2 ne sont pas isomorphes, on est toujours dans ce cas, d'où (i).

Supposons donc qu'il existe un K-isomorphisme $\phi : B_1 \xrightarrow{\sim} B_2$ et définissons σ comme plus haut. Alors $\sigma^2 = \mathrm{id}$ et, pour tout automorphisme α de B échangeant B_1 et B_2, $\alpha \circ \sigma$ laisse stable B_1 et B_2 donc, d'après ce qui précède, égale $\mathrm{Int}(b)$ pour un certain $b \in B^\times$, d'où $\alpha = \mathrm{Int}(b) \circ \sigma$. De plus, pour tout $b \in B^\times$ et $b' \in B$ on a :

$$(\sigma \circ \mathrm{Int}(b) \circ \sigma)(b') = \sigma(b\sigma(b')b^{-1}) = \sigma(b)b'\sigma(b)^{-1} = \mathrm{Int}(\sigma(b))(b')$$

d'où $\sigma \circ \mathrm{Int}(b) \circ \sigma = \mathrm{Int}(\sigma(b))$. Combiné avec ce qui précède, ceci prouve (ii). □

Lemme 5.2. — (i) $\mathrm{GL}_n(K)$ *s'identifie via* $g \mapsto (g, (g^{-1})^{\mathrm{op}})$ *au sous-groupe de* $A_{0,K}^\times$ *formé des* a *tels que* $s(a)a = 1$. *Ce sous-groupe est noté* $U(A_{0,K})$ *ou* $U(A_0)(K)$.

(ii) *On a* $\mathrm{Aut}_K(A_0, s) \simeq \mathscr{A}(K) = \mathrm{PGL}_n(K) \rtimes \{1, i_t\}$.

Démonstration. — La première assertion est immédiate, prouvons la seconde. L'application $\tau : a \mapsto {}^t a$ est un isomorphisme de $M_n(K)$ sur $M_n(K)^{\mathrm{op}}$; elle induit donc un automorphisme de $A_{0,K}$ défini par :

$$\tau'(x, y^{\mathrm{op}}) = ({}^t y, {}^t x^{\mathrm{op}}).$$

On voit aussitôt que $\tau' \circ s = s \circ \tau'$, donc $\tau' \in \mathrm{Aut}_K(A_0, s)$. Comme $\tau'(g, (g^{-1})^{\mathrm{op}}) = ({}^t g^{-1}, ({}^t g)^{\mathrm{op}})$, on voit que τ' induit sur $\mathrm{GL}_n(K)$ l'automorphisme i_t.

D'après le lemme 5.1, $\mathrm{Aut}_{K\text{-alg}}(A_{0,K})$ est le produit semi-direct de $\mathrm{Int}(A_{0,K})$ par $\{1, \tau'\}$. Déterminons le sous-groupe $\mathrm{Aut}_K(A_0, s)$. Comme τ' commute à s, il suffit de déterminer le sous-groupe des éléments de $\mathrm{Int}(A_{0,K})$ qui commutent à s. Or, pour tout $g_1, g_2 \in \mathrm{GL}_n(K)$ et $x, y \in M_n(K)$, on a :

$$(\mathrm{Int}(g_1, g_2^{\mathrm{op}}) \circ s)(x, y^{\mathrm{op}}) = (g_1 y g_1^{-1}, (g_2^{-1} x g_2)^{\mathrm{op}})$$

$$(s \circ \mathrm{Int}(g_1, g_2^{\mathrm{op}}))(x, y^{\mathrm{op}}) = s(g_1 x g_1^{-1}, (g_2^{-1} y g_2)^{\mathrm{op}}) = (g_2^{-1} y g_2, (g_1 x g_1^{-1})^{\mathrm{op}})$$

donc $\mathrm{Int}(g_1, g_2^{\mathrm{op}})$ commute à s ssi $g_2 = g_1^{-1}$. Il en résulte que les automorphismes intérieurs de $A_{0,K}$ qui commutent à s s'identifient à $\mathrm{GL}_n(K)/K^*$, via $g \mapsto \mathrm{Int}(g, g^{-1})$, et donc $\mathrm{Aut}_K(A_0, s) \simeq \mathrm{PGL}_n(K) \rtimes \{1, \tau'\}$. □

Corollaire 5.3. — *Soit* $n \geq 3$. *Pour toute extension galoisienne* K/k, *de groupe de Galois* Γ, *on a des bijections :*

$$\left\{ \begin{array}{c} K/k\text{-formes de } \mathrm{GL}_{n,k} \\ \text{à isomorphisme près} \end{array} \right\} \leftrightarrow H^1(\Gamma, \mathscr{A}(K)) \leftrightarrow \left\{ \begin{array}{c} K/k\text{-formes de } (A_0, s) \\ \text{à isomorphisme près} \end{array} \right\}.$$

La bijection composée associe à une k*-algèbre à involution* (A, σ) *le* k*-foncteur en groupes* $U(A)$ *qui à toute* k*-algèbre* R *associe* $U(A)(R) = \{u \in (A \otimes R)^\times \mid \sigma(u)u = 1\}$.

Explicitons ce qu'est une K/k-forme de (A_0, s). Pour simplifier l'exposition, faisons-le dans le cas où $K = k_s$.

Définition 5.4 (**k-algèbres étales de rang 2**). — (i) Soit d un entier ≥ 1. Par définition, une k-algèbre étale de rang d est une k-forme E de la k-algèbre $k \times \cdots \times k$ (d facteurs) ; ceci équivaut à dire que $E \simeq L_1 \times \cdots \times L_r$, où les L_i sont des corps *séparables* sur k et $\sum_{i=1}^r [L_i : k] = \dim_k(E) = d$ (cf. [BAlg, §V.6, Déf. 1 & Th. 4]).

(ii) Lorsque $d = 2$, comme toute extension séparable L/k de degré 2 est galoisienne, on voit qu'une k-algèbre étale de rang 2 est soit $k \times k$, soit une extension galoisienne L/k de degré 2. Dans les deux cas, $\mathrm{Aut}_{k\text{-alg}}(L) \simeq S_2$ et $L \otimes k_s \simeq k_s \times k_s$, l'isomorphisme étant donné dans le second cas par $x \otimes y \mapsto (xy, \sigma(x)y)$ où σ est l'élément non trivial de $\mathrm{Gal}(L/k)$ (cf. [BAlg, §V.10.4, Cor. de la Prop. 8]).

Soit (A, σ) une k-forme de (A_0, s), i.e. A est une k-algèbre de dimension $2n^2$ munie d'une involution σ, qui devient isomorphe à (A_0, s) sur k_s. Alors $Z(A)$ est une k-algèbre étale de rang 2, et la restriction de σ à $Z(A)$ est l'unique k-automorphisme non trivial. Il y a deux possibilités.

(1) $Z(A) \simeq k \times k$. Soit B_1 (resp. B_2) l'idéal bilatère engendré par l'idempotent central $e_1 = (1, 0)$ (resp. $e_2 = (0, 1)$), alors $A = B_1 \times B_2$ et comme $\sigma(e_1) = e_2$, σ induit un anti-automorphisme $\phi : B_2 \xrightarrow{\sim} B_1$ défini par $\sigma(0, b_2) = (\phi(b_2), 0)$. Posant $B = B_1$ et identifiant B_2 à B^{op} via $b_2 \mapsto \phi(b_2)^{\mathrm{op}}$, on obtient que $A = B \times B^{\mathrm{op}}$ et $\sigma(x, y^{\mathrm{op}}) = (y, x^{\mathrm{op}})$. De plus, comme $B \otimes k_s \simeq M_n(k_s)$ alors B est une k-algèbre centrale simple.

Réciproquement, pour toute k-algèbre centrale simple B, la k-algèbre $A(B) = B \times B^{\mathrm{op}}$ munie de l'involution $s(x, y^{\mathrm{op}}) = (y, x^{\mathrm{op}})$ est une k-forme de (A_0, s). Notons de plus que si $(A(B), s)$ et $(A(C), s)$ sont isomorphes, alors C est isomorphe à B ou à Bop, et que $(A(B), s)$ et $(A(B^{\mathrm{op}}), s)$ sont isomorphes via $(b_1, b_2^{\mathrm{op}}) \mapsto (b_2^{\mathrm{op}}, b_1)$.

On obtient alors la bijection suivante. Soit $\mathrm{CS}_n(k)$ l'ensemble des classes d'isomorphisme de k-algèbres centrales simples de dimension n^2 ; il est muni d'une action de S_2 où l'élément non trivial de S_2 envoie la classe de A sur celle de A^{op}. Notons $\mathrm{CS}_n(k)/S_2$ l'ensemble quotient (i.e. l'ensemble des orbites). Alors on a une bijection :

$$\mathrm{CS}_n(k)/S_2 \xrightarrow{\sim} \left\{ \begin{array}{c} \text{classes d'isomorphisme de} \\ k\text{-formes } (A, \sigma) \text{ de } (A_0, s) \\ \text{telles que } Z(A) \simeq k \times k \end{array} \right\}, \qquad B \mapsto (B \times B^{\mathrm{op}}, s).$$

La k-forme de $\mathrm{GL}_{n,k}$ correspondant à $B = M_m(D)$, où D est un corps gauche de centre k, est le k-foncteur en groupes noté $\mathrm{GL}_1(B)$ ou $\mathrm{GL}_m(D)$, qui à toute k-algèbre R associe $\mathrm{GL}_m(D \otimes R) = M_m(D \otimes R)^\times$.

D'autre part, la norme réduite (cf. 4.22) est un morphisme de k-groupes algébriques $\mathrm{Nrd} : \mathrm{GL}_1(B) \to \mathbb{G}_{m,k}$ et son noyau, noté $\mathrm{SL}_1(B)$ ou $\mathrm{SL}_m(D)$, est la k-forme correspondante de $\mathrm{SL}_{n,k}$.

Ces k-formes (de (A_0, s), $\mathrm{GL}_{n,k}$ ou $\mathrm{SL}_{n,k}$) sont appelées des formes **intérieures** car elles correspondent aux éléments de $H^1(\Gamma, \mathscr{A}(k_s))$ qui sont dans l'image de l'application

$$H^1(\Gamma, \mathrm{PGL}_n(k_s)) \to H^1(\Gamma, \mathscr{A}(k_s)),$$

$\mathrm{PGL}_n(k_s)$ étant le groupe des automorphismes « intérieurs » de (A_0, s), GL_{n,k_s} ou SL_{n,k_s}.

Considérons maintenant le second cas, i.e. celui des formes « **extérieures** ». Rappelons que $\mathscr{D}$ désigne le diagramme de Dynkin de $\mathrm{SL}_{n,k}$ et $\mathrm{GL}_{n,k}$; son automorphisme non trivial se relève en l'automorphisme $i_\top = \mathrm{Int}(J_n) \circ i_t$ de $\mathrm{GL}_{n,k}$, où $i_t(g) = {}^t g^{-1}$.

(2) Soit (A, σ) une k-forme de (A_0, s) et $G = U(A)$ la k-forme correspondante de $\mathrm{GL}_{n,k}$; elles sont données par un cocycle $c : \Gamma \to \mathscr{A}(k_s) = \mathrm{PGL}_n(k_s) \times \{1, i_t\}$ tel que $\pi \circ c$ soit non trivial, où π est la projection de $\mathscr{A}(k_s)$ sur $\{1, i_t\}$. Dans ce cas, $\pi \circ c : \Gamma \to \{1, i_t\} = \mathrm{Aut}(\mathscr{D})$ est un morphisme de groupes surjectif [14] ; notons Γ_c son noyau. Alors $L = k_s^{\Gamma_c}$ est une extension quadratique galoisienne de k ; on notera $\lambda \mapsto \overline{\lambda}$ l'action de l'élément non trivial de $\mathrm{Gal}(L/k)$.

[14] I.e. l'action de Γ sur $\mathscr{D}$ est non triviale.

Lemme 5.5. — (i) *Le centre de A est L et la restriction de σ à L est l'élément non trivial de* $\mathrm{Gal}(L/k)$.

(ii) *Le centre de $G = U(A)$ est $U(L)$, i.e. le foncteur en groupes qui à toute k-algèbre R associe $U(L \otimes R) = \{u \in (R \otimes L)^\times \mid \sigma(u)u = 1\}$.* [(15)]

Démonstration. — (i) A est l'algèbre des invariants pour l'action de Γ sur $A_0 \otimes k_s$ donnée par $\gamma *_c (a \otimes \lambda) = c(\gamma)(a \otimes \gamma(\lambda))$, et le centre de A provient du centre $Z_0 = k_s \times k_s$ de $A_0 \otimes k_s$. Comme les automorphismes intérieurs agissent trivialement sur Z_0, l'action $*_c$ de Γ_c sur Z_0 coïncide avec l'action standard $\gamma(x, y) = (\gamma(x), \gamma(y))$, donc en prenant les invariants sous Γ_c on obtient $L \times L$. Alors, tout élément γ de $\Gamma - \Gamma_c$ envoie un couple (λ, μ) sur $(\overline{\mu}, \overline{\lambda})$ et l'on obtient donc un isomorphisme

$$L \xrightarrow{\sim} Z(A), \qquad \lambda \mapsto (\lambda, \overline{\lambda}).$$

Enfin, comme σ est la restriction à A de l'involution s de $A_0 \otimes k_s$, elle induit sur $Z(A) \simeq L$ l'involution $\lambda \mapsto \overline{\lambda}$.

(ii) Il est clair que $U(L)$ est contenu dans le centre $Z(G)$ de $G = U(A)$. De plus, en étendant les scalaires de k à k_s on voit facilement que $U(L)_{k_s} = Z(G)_{k_s}$ (c'est le foncteur qui à toute k_s-algèbre R associe le centre de $\mathrm{GL}_n(R \otimes k_S)$) donc $U(L) = Z(G)$. □

Notons enfin que A est une L-algèbre simple. En effet, si I est un idéal bilatère non nul de A, alors $I \otimes k_s$ est un idéal bilatère non nul de $A \otimes k_s \simeq A_0 \otimes k_s$, stable par l'action de Γ, et comme l'action de Γ échange les deux idempotents $(1, 0)$ et $(0, 1)$ de $A_0 \otimes k_s$ alors $I \otimes k_s = A_0 \otimes k_s$ et donc $I = A$.

Réciproquement, si L/k est une extension quadratique contenue dans k_s et A une L-algèbre centrale simple munie d'une involution σ induisant sur L l'élément non trivial de $\mathrm{Gal}(L/k)$, on peut vérifier que (A, σ) devient isomorphe à (A_0, s) sur k_s. On obtient donc :

Proposition 5.6. — *Pour toute extension quadratique L/k contenue dans k_s, on a une bijection*

$$\left\{ \begin{array}{c} \textit{classes d'isomorphisme de} \\ k\textit{-formes de } \mathrm{GL}_{n,k} \\ \textit{de centre} \simeq U(L) \end{array} \right\} \leftrightarrow \left\{ \begin{array}{c} \textit{classes d'isomorphisme de} \\ k\textit{-formes } (A, \sigma) \textit{ de } (A_0, s) \\ \textit{avec } Z(A) \simeq L \textit{ et } \sigma|_L \neq \mathrm{id}. \end{array} \right\}$$

La discussion précédente conduit à la définition suivante.

***Définition 5.7* (Involutions de 1ère ou 2ème espèce)**. — Soit A une k-algèbre de dimension finie munie d'une involution σ et soit Z le centre de A. On dit que (A, σ) est une « k-algèbre à involution centrale simple » dans les cas suivants :

(1) $Z = k$ et A est une k-algèbre centrale simple. Dans ce cas, on dit que σ est une involution de **1ère espèce**.

(2) $Z = L$ est un corps, extension quadratique galoisienne de k, A est une L-algèbre centrale simple et la restriction de σ à L est l'élément non trivial de $\mathrm{Gal}(L/k)$.

(3) $Z = k \times k$ et (A, σ) est isomorphe à $(B \times B^{\mathrm{op}}, s)$, où B est une k-algèbre centrale simple et $s(b_1, b_2^{\mathrm{op}}) = (b_2, b_1^{\mathrm{op}})$.

Dans les cas (2) et (3) on dit que σ est une involution de **2ème espèce**.

La classification des formes extérieures de $\mathrm{SL}_{n,k}$ ou $\mathrm{GL}_{n,k}$ pour $n \geq 3$ est donc ramenée à celle des k-algèbres « centrales simples » avec involution de 2ème espèce (A, σ) dont le centre est une extension galoisienne L/k de degré 2.

(15) C'est le k-tore non déployé de dimension 1 associé à L, i.e. le noyau du morphisme de norme $N_{L/k}$: $\mathrm{Res}_{L/k}(\mathbb{G}_{m,L}) \to \mathbb{G}_{m,k}$.

***Lemme 5.8* (Hilbert 90).** — *Soit L/k une extension quadratique galoisienne. Pour tout $z \in L$, notons $\overline{z}$ son image par l'élément non trivial de* $\mathrm{Gal}(L/k)$*. Pour tout $z \in L$ tel que $z\overline{z} = 1$, il existe $\mu \in L$ tel que $z = \mu/\overline{\mu}$.* [16]

Démonstration. — Posons $\Gamma = \mathrm{Gal}(L/k) = \{1, \gamma\}$; il agit sur $L^\times$ par $\gamma(x) = \overline{x}$. Pour tout cocycle $c : \Gamma \to L^\times$ on a $c(1) = 1$ donc l'on voit que se donner un cocycle équivaut à se donner l'élément $z = c(\gamma)$ de $L^\times$ de façon à vérifier la condition de cocycle :

$$1 = c(1) = c(\gamma\gamma) = c(\gamma)\gamma(c(\gamma)) = z\overline{z}.$$

Or on a vu que $H^1(\Gamma, L^\times) = \{1\}$ donc il existe $\mu \in L^\times$ tel que $z = \mu/\overline{\mu}$. □

Prenons par exemple $k = \mathbb{R}$. La seule extension quadratique est $L = \mathbb{C}$ qui est algébriquement clos, donc la seule L-algèbre centrale simple de degré n est $A = M_n(\mathbb{C})$.

***Définition 5.9*.** — Soient b, b' deux formes hermitiennes non dégénérées sur $\mathbb{C}^n$.

(i) On dit que b, b' sont *équivalentes* s'il existe $g \in \mathrm{GL}_n(\mathbb{C})$ tel que $b'(x, y) = b(gx, gy)$ pour tout $x, y \in \mathbb{C}^n$. On rappelle que b et b' sont équivalentes ssi elles ont la même signature ; les signatures possibles sont $(n - k, k)$, pour $k = 0, \ldots, n$.

(ii) On dit que b, b' sont *similaires* s'il existe $g \in \mathrm{GL}_n(\mathbb{C})$ et $\lambda \in \mathbb{R}^\times$ tels que $b'(x, y) = \lambda b(gx, gy)$ pour tout $x, y \in \mathbb{C}^n$. Si $\lambda = r^2$ on voit que b' est équivalente à b via l'homothétie de rapport $1/r$; on en déduit que b, b' sont similaires ssi b' est équivalente à b ou $-b$. On en déduit que les classes de similitude sont en bijection avec les signatures $(n - k, k)$, pour $0 \leq k \leq n/2$.

***Proposition 5.10*.** — (i) *Soit b une forme hermitienne non dégénérée sur $\mathbb{C}^n$. On lui associe une involution de 2ème espèce σ_b de $A = M_n(\mathbb{C})$, définie comme suit : pour tout $u \in A$ et $x, y \in \mathbb{C}^n$, on a*

$$b(x, u(y)) = b(\sigma_b(u)(x), y),$$

i.e. u est l'adjoint de u pour b.

(ii) *L'application $b \mapsto \sigma_b$ induit une bijection entre les classes de similitude de formes hermitiennes non dégénérées et les classes d'isomorphisme de couples (A, σ) où σ est une involution de 2ème espèce.*

Démonstration. — (i) Soit $\mathscr{B} = (e_1, \ldots, e_n)$ la base canonique de $\mathbb{C}^n$ et $J = (b(e_i, e_j))_{1 \leq i,j \leq n}$ la matrice de b dans $\mathscr{B}$. L'hypothèse que b soit hermitienne et non dégénérée équivaut à dire, respectivement, que J vérifie ${}^t\overline{J} = J$ et est inversible. Pour tout $X, Y \in \mathbb{C}^n$, on a $b(X, Y) = {}^t\overline{X} J Y$ donc pour tout $U \in M_n(\mathbb{C})$ on a :

$$b(X, UY) = {}^t\overline{X} J U Y = {}^t\overline{X} J U J^{-1} J Y$$

donc on voit que $\sigma_b(U) = {}^t\overline{J}^{-1}\, {}^t\overline{U}\, {}^t\overline{J} = J^{-1}\, {}^t\overline{U}\, J$ est l'unique élément de $M_n(\mathbb{C})$ vérifiant

$$b(X, UY) = b(\sigma_b(U)(X), Y) = {}^t\overline{X}\, {}^t\overline{\sigma_b(U)}\, Y$$

pour tout $X, Y \in \mathbb{C}^n$. Il est clair que σ_b est $\mathbb{R}$-linéaire et vérifie $\sigma_b(zU) = \overline{z}\sigma_b(U)$ et $\sigma_b(UU') = \sigma_b(U')\sigma_b(U)$ pour tout $z \in \mathbb{C}$ et $U, U' \in M_n(\mathbb{C})$. De plus, on a :

$$\sigma_b^2(U) = \sigma_b(J^{-1}\, {}^t\overline{U}\, J) = J^{-1}\, {}^t\overline{J}\, U\, {}^t\overline{J}^{-1}\, J = U,$$

la dernière égalité résultant de l'égalité ${}^t\overline{J} = J$. On a donc $\sigma_b^2 = \mathrm{id}$. Ceci prouve (i).

(ii) Pour $J = I_n$ on obtient l'involution de 2ème espèce $\sigma_0 : U \mapsto {}^t\overline{U}$. Si σ en est une autre, alors $\sigma\sigma_0^{-1}$ est un automorphisme de la $\mathbb{C}$-algèbre simple $M_n(\mathbb{C})$ donc d'après le théorème

[16] Ceci est le cas $d = 2$ du théorème original de Hilbert, qui concernait le cas d'une extension galoisienne L/k de groupe de Galois $\mathbb{Z}/d\mathbb{Z}$.

de Skolem-Noether il existe $g \in \mathrm{GL}_n(\mathbb{C})$ tel que $\sigma = \mathrm{Int}(g) \circ \sigma_0$. Pour tout $u \in M_n(\mathbb{C})$ on a :

$$u = \sigma^2(u) = (\mathrm{Int}(g) \circ \sigma_0)(g\sigma_0(u)g^{-1}) = g\sigma_0(g^{-1})u\sigma_0(g)g^{-1}$$

donc il existe $z \in \mathbb{C}^\times$ tel que $\sigma_0(g) = zg$. De plus on a

$$g = \sigma_0^2(g) = \overline{z}\sigma_0(g) = \overline{z}zg,$$

d'où $\overline{z}z = 1$. D'après le Théorème 90 de Hilbert (5.8), il existe $\mu \in \mathbb{C}$ tel que $z = \mu/\overline{\mu}$, alors $\sigma_0(\mu g) = \mu g$, i.e. g est une matrice hermitienne inversible et l'on a $\sigma = \sigma_b$ où b est la forme hermitienne non dégénérée de matrice g^{-1}. Ceci prouve que l'application est surjective.

D'autre part, d'après le théorème de Skolem-Noether, deux couples (A, σ_b) et $(A, \sigma_{b'})$ sont isomorphes ssi il existe $g \in A^\times$ tel que

$$\sigma_{b'} = \mathrm{Int}(g^{-1}) \circ \sigma_b \circ \mathrm{Int}(g)$$

et l'on voit par un calcul facile que ceci équivaut à dire qu'il existe $z \in \mathbb{C}^*$ tel que $J' = z^t\overline{g}Jg$, i.e. $b'(x, y) = zb(gx, gy)$ pour tout $x, y \in \mathbb{C}^n$. Et comme $b'(x, x)$ et $b(gx, gx)$ sont réels pour tout x et $b'(x, x) \neq 0$ pour au moins un x, on obtient $z \in \mathbb{R}^\times$. Ceci prouve (ii). □

On a ainsi obtenu la classification des $\mathbb{R}$-formes extérieures de $SL_{n,\mathbb{R}}$: à isomorphisme près, ce sont les groupes unitaires $\mathrm{SU}(n-k, k)$ pour $0 \leq k \leq n/2$. Parmi eux, seul le groupe $\mathrm{SU}(n)$ est compact (« anisotrope » en langage algébrique).

Pour terminer ce paragraphe, déterminons aussi les formes intérieures. On sait que ce sont les groupes $\mathrm{SL}_m(D)$, où D est un corps de centre $\mathbb{R}$ et $m \deg(D) = n$. Or, à isomorphisme près les seuls corps de centre $\mathbb{R}$ et de degré fini sur $\mathbb{R}$ sont $\mathbb{R}$ et le corps des quaternions $\mathbb{H}$. Comme $\deg(\mathbb{H}) = 2$, on obtient ainsi $\mathrm{SL}_m(\mathbb{H})$ si $n = 2m$. En résumé, on a obtenu le :

Théorème 5.11. — *À isomorphisme près, les $\mathbb{R}$-formes de $\mathrm{SL}_{n,\mathbb{R}}$ sont les suivantes :*

(i) *Les formes extérieures $\mathrm{SU}(n-k, k)$ pour $0 \leq k \leq n/2$.*

(ii) *$\mathrm{SL}_{n,\mathbb{R}}$, qui est la forme déployée.*

(iii) *Si $n = 2m$ le groupe $\mathrm{SL}_m(\mathbb{H})$, qui est la seule forme intérieure non déployée.*

5.2. Formes des groupes orthogonaux et symplectiques. — à compléter ...