

Théorie des groupes

M. Jacques Tits, membre de l'Institut
(Académie des Sciences), professeur

Le cours de cette année avait pour thème annoncé la *Cohomologie galoisienne des groupes semi-simples sur les corps de nombres*. Le résultat central de cette théorie est le « principe de Hasse » pour les groupes semi-simples simplement connexes et l'événement exceptionnel qui a déterminé le choix de ce sujet a été la solution récente par V. I. Černousov et A. Premet d'un problème posé depuis un quart de siècle, à savoir, la preuve du principe de Hasse pour les groupes de type E_8 , seul cas laissé ouvert par les travaux de M. Kneser et G. Harder au milieu des années soixante. Il s'agissait, dans le cours, non seulement d'exposer la preuve de Černousov-Premet, mais aussi de reprendre les anciens résultats de Harder dont l'exposé publié est parfois excessivement succinct. Une présentation unifiée et détaillée de la preuve complète du principe de Hasse était certes souhaitable mais s'est avérée dépasser les possibilités du cours d'une seule année. On a donc fait un choix, en essayant qu'il illustre au mieux les principales méthodes de la démonstration. On s'est aussi attaché à mettre en évidence les principes généraux sous-jacents à ces méthodes et à rechercher systématiquement ce qui, dans tel ou tel raisonnement, reste valable pour des corps plus généraux que les corps de nombres. C'est pourquoi les corps de nombres ne jouent en fin d'un compte qu'un rôle assez secondaire dans le présent résumé, où nous n'évoquons d'ailleurs que quelques-uns des sujets abordés dans le cours.

I. L'INVARIANT β

1.1. TROIS ÉTAPES DE LA CLASSIFICATION DES GROUPES ALGÈBRIQUES SIMPLES SUR UN CORPS

Dans ce résumé, k désigne toujours un corps dont on choisit une clôture algébrique \bar{k} . Toutes les extensions de k que l'on considère sont contenues

dans \bar{k} . On pose $\Gamma = \text{Gal}(\bar{k}/k)$. Sauf mention expresse du contraire, la caractéristique du corps k est supposée égale à 0 bien que les résultats énoncés soient souvent indépendants de cette hypothèse.

Pour l'approche que nous avons en vue, il est commode de poser le problème de la classification dans les termes suivants : on se donne un graphe de Dynkin Δ — nous le supposons connexe pour simplifier — et l'on cherche à classer les couples (G, i) formés d'un k -groupe presque simple simplement connexe G (le cas de groupes semi-simples quelconques se ramène facilement à celui-là) et d'un isomorphisme i de Δ sur le graphe de Dynkin $\Delta(G, \bar{k})$ de G sur \bar{k} . Par abus de langage, on parlera parfois du « groupe G » alors qu'il s'agira en fait du couple (G, i) .

Le graphe $\Delta(G, \bar{k})$ étant canoniquement associé à G et \bar{k} , le groupe de Galois Γ opère sur lui, donc, via i , sur Δ . L'homomorphisme $\gamma : \Gamma \rightarrow \text{Aut } \Delta$ ainsi défini est un premier invariant de l'objet (G, i) . Si l'on choisit un couple (G_γ, i) d'invariant γ donné, l'ensemble des classes d'isomorphisme de tels couples est en bijection canonique avec $H^1(\Gamma, \tilde{G}_\gamma)$ (groupe que l'on note aussi $H^1(k, \tilde{G}_\gamma)$, ou encore $H^1(\tilde{G}_\gamma)$), où \tilde{G}_γ désigne le groupe adjoint de G_γ .

Le centre de G_γ , noté Z_γ , est un k -groupe entièrement déterminé par Δ et γ . La suite exacte de cohomologie associée à la suite exacte courte $1 \rightarrow Z_\gamma \rightarrow G_\gamma \rightarrow \tilde{G}_\gamma \rightarrow 1$ fournit un homomorphisme $\delta : H^1(\tilde{G}_\gamma) \rightarrow H^2(Z_\gamma)$, d'où l'on déduit un second invariant $\beta \in H^2(Z_\gamma)$, à savoir, l'image par δ de l'élément de $H^1(\tilde{G}_\gamma)$ représentant (G, i) . Cet invariant β a une interprétation bien connue en termes de représentations linéaires (cf. [7], [8]).

Soient donnés $\gamma \in \text{Hom}(\Gamma, \text{Aut } \Delta)$ et $\beta \in H^2(Z_\gamma)$. Si (G_β, i) est un couple ayant γ et β pour invariants, l'ensemble des classes d'isomorphisme de couples ayant ces mêmes invariants est paramétré par l'image de l'application canonique $H^1(G_\beta) \rightarrow H^1(\tilde{G}_\beta)$, image que nous désignerons par $H^1(G_\beta)^-$.

Le problème de la classification des objets (G, i) se trouve ainsi décomposé en trois étapes faisant apparaître comme ensembles de paramètres $\text{Hom}(\Gamma, \text{Aut } \Delta)$, une partie de $H^2(Z_\gamma)$ et $H^1(G_\beta)^-$. Lorsque k est un corps de nombres, c'est à la seconde et à la troisième étape qu'intervient le principe de Hasse : injectivité de l'application canonique $X \rightarrow \prod X_\nu$, où ν parcourt l'ensemble des places du corps k , X est l'un des ensembles de paramètres en question et X_ν est l'ensemble analogue sur le corps complété k_ν . En effet, chacun des ensembles $H^2(Z_\gamma)$ et $H^1(G_\beta)^-$ (ainsi d'ailleurs que $H^1(G_\beta)$ et $H^1(\tilde{G}_\beta)$) satisfait à ce principe. C'est le principe de Hasse pour $H^1(G_\beta)$ auquel on se réfère le plus souvent et qui est le plus difficile à établir : la seule preuve dont on dispose procède cas par cas ; elle combine des résultats dus à plusieurs auteurs et concernant les divers types de groupes.

1.2. REPRÉSENTANTS « NATURELS » DES CLASSES D'ISOMORPHISME D'INVARIANTS DONNÉS

Rappelons que les classes de conjugaison de \bar{k} -sous-groupes paraboliques de G sont en bijection canonique avec les parties de Δ (nous désignons aussi par Δ l'ensemble des sommets du graphe Δ) ; ici, la correspondance sera choisie de telle sorte qu'aux sous-groupes de Borel corresponde l'ensemble vide. Pour (G, i) comme ci-dessus, notons $\Delta^\circ = \Delta^\circ(G, i)$ la partie de Δ correspondant à la classe de conjugaison des k -sous-groupes paraboliques minimaux. Etant donné $\gamma \in \text{Hom}(\Gamma, \text{Aut } \Delta)$, il existe, dans l'ensemble des classes d'isomorphisme de couples (G, i) d'invariant γ , une unique classe réalisant le minimum de $\text{Card } \Delta^\circ(G, i)$; autrement dit, en termes moins précis mais plus suggestifs, il existe un groupe d'invariant γ qui est plus isotrope que tous les autres : c'est le groupe *quasi-déployé*, caractérisé par la relation $\Delta^\circ = \emptyset$. Pour la classification des groupes d'invariant γ , on choisit en général le groupe quasi-déployé comme groupe G_γ de référence.

Pour l'invariant β , la propriété analogue à celle que l'on vient d'énoncer pour γ n'est évidemment pas vraie en général, mais elle l'est dans un cas particulier important : *supposons $\gamma(\Gamma) = 1$ (cas des formes intérieures), de sorte que $H^2(Z_\gamma)$ est un sous-groupe du groupe de Brauer $\text{Br } k$ de k ou d'un produit de deux copies de ce groupe, et soit β un élément de $H^2(Z_\gamma)$ tel que l'indice de chaque composante de β dans $\text{Br } k$ soit égal à son exposant (condition automatiquement satisfaite si k est un corps de nombres) ; alors, dans l'ensemble des classes d'isomorphisme de couples (G, i) d'invariant $\gamma = 1$ et β , la fonction $\text{Card } \Delta^\circ$ prend son minimum en un et un seul élément.*

Ici encore, pour la classification des couples (G, i) d'invariants $\gamma = 1$ et β comme ci-dessus, il est naturel de prendre le groupe réalisant le minimum de $\text{Card } \Delta^\circ$ comme groupe G_β de référence. L'énoncé précédent se démontre très simplement à l'aide du théorème d'unicité et d'un critère d'existence d'un groupe de type Δ ayant un noyau anisotrope de type Δ° donné (cf. par exemple [7], 1.5, 1.6). On se ramène ainsi à la vérification du fait suivant :

le sous-graphe de Δ ayant pour sommets les sommets de Δ dont le poids fondamental dominant associé n'appartient pas au réseau des racines est une réunion disjointe de graphes de type A.

1.3. GROUPES DE TYPES E_6 ET E_7

Un homomorphisme $\gamma \in \text{Hom}(\Gamma, \text{Aut } \Delta)$ étant donné, on peut se demander quels éléments de $H^2(Z_\gamma)$ sont les invariants β de couples (G, i) . Le cas des groupes de type E_6 intérieur et de type E_7 est particulièrement intéressant. Ici, β est un élément d'exposant $p = 3$ (pour E_6) ou 2 (pour E_7) du groupe de Brauer $\text{Br } k$. L'interprétation de β en termes de représentations

linéaires et l'existence de représentations de dimensions $27 = 3^3$ et $56 = 7 \cdot 2^3$ pour E_6 et E_7 respectivement montre que, dans les deux cas, l'indice de l'invariant β d'un couple (G, i) divise p^3 . D'après ce que l'on a vu en 1.2, toute algèbre à division de degré p (i.e. de dimension p^2) est l'invariant β d'un groupe de type E_6 ou E_7 . Jusqu'à présent, aucune autre valeur possible de β n'était connue, à cela près que, dans [7], 6.4 et 6.5, une méthode était décrite qui devait « probablement » fournir des exemples de degré p^2 . Dans le cours, cette méthode a été reformulée en termes cohomologiques puis améliorée de façon à atteindre en principe l'indice limite p^3 . Par la suite, des renseignements fournis par J.-P. Tignol ont montré que la méthode en question fournit bien des exemples d'indice p^2 et aussi p^3 . Nous décrirons avec quelques détails les résultats concernant E_6 et donnerons ensuite de brèves indications sur le cas, analogue mais un peu plus compliqué, du type E_7 .

Soient G un groupe simplement connexe déployé de type E_6 et \tilde{G} son groupe adjoint. On sait que G possède des sous-groupes déployés de type $A_2 \times A_2 \times A_2$. Compte tenu du fait que ces sous-groupes sont de rang maximal, il est facile de voir qu'ils sont tous conjugués et que si X est l'un d'eux, le normalisateur Y de X dans G est extension par X d'un groupe cyclique d'ordre 3. Soient X^-, Y^- les images de X et Y dans \tilde{G} . La méthode proposée dans [7], en termes un peu différents, consiste à tordre G par un élément de $H^1(X^-) \subset H^1(\tilde{G})$ dont l'image dans $H^2(Z_\gamma) \subset \text{Br } k$ soit d'indice 9 (c'est manifestement le mieux que l'on puisse faire). Il s'agit de montrer que pour certains corps k , un tel élément existe. Un calcul élémentaire montre que cela revient à trouver un corps k et des algèbres à division D, D' de degré 3 sur k telles que, si l'on désigne par $[*]$ l'image de $*$ dans le groupe de Brauer, $[D] + [D']$ soit d'indice 3 tandis que $[D] - [D']$ est d'indice 9. J'ai appris par Tignol l'existence de l'article [6] dont la proposition 5.1 assure l'existence de tels k, D, D' (3 étant remplacé par un entier impair quelconque).

Selon une suggestion de J.-P. Serre, on peut essayer d'obtenir un exemple de groupe de type E_6 dont l'invariant β est d'indice 27 en utilisant le groupe non connexe Y^- au lieu de X^- . La traduction du problème en termes d'algèbres à division n'est guère plus difficile. Tout élément de $H^1(Y^-)$ définit un élément de $H^1(Y^-/X^-) = H^1(\mathbf{Z}/3\mathbf{Z}) = \text{Hom}(\Gamma, \mathbf{Z}/3\mathbf{Z})$, donc une extension K de k , cyclique d'ordre 3. On montre alors que, si l'on désigne par μ' le noyau de l'application norme $R_{K/k} \mu_3 \rightarrow \mu_3$ et par π l'homomorphisme canonique $\mu' \rightarrow \mu'/\mu_3 \cong \mu_3$ (le groupe μ_3 est naturellement inclus dans μ' via $R_{K/k} \mu_3$), il s'agit à présent de trouver un élément de $H^2(\mu')$ dont l'image dans $H^2(\mu_3) \subset \text{Br } k$ par $H^2(\pi)$ soit d'indice 27. Selon Tignol (lettre du 24.7.1991), il existe effectivement un corps k et un élément de $H^2(\mu')$ ayant ces propriétés.

Il est intéressant de noter que

un groupe de type E_6 intérieur dont l'invariant β est d'indice 27 n'a pas d'autres k -sous-groupes connexes propres non triviaux que ses k -tores maximaux et éventuellement des sous-groupes de type $(A_2)^3$.

Pour le type E_7 , on a le choix entre deux sous-groupes X possibles : groupe de type $A_1 \times A_3 \times A_3$ ou groupe de type A_7 . Dans les deux cas, X est d'indice 2 dans son normalisateur Y . Le problème concernant des algèbres à division auquel on ramène la construction, à l'aide de X , d'un groupe de type E_7 dont l'invariant β est d'indice 4 a effectivement des solutions pour chacun des deux choix de X . Je dois à nouveau ce renseignement à J.-P. Tignol qui m'a signalé en particulier que, pour X de type A_7 , la solution du problème (il s'agit de trouver une algèbre à division d'indice 8 et d'exposant 4 dont le carré est d'indice 4) se trouve déjà dans un article ancien de Richard Brauer [1]. Enfin, on doit s'attendre à ce qu'à l'aide de chacun des deux groupes Y , normalisateurs des groupes X en question, on puisse obtenir des exemples de groupes de type E_7 avec invariants β d'indice 8. Cela vient d'ailleurs de m'être confirmé par Tignol sous réserve de vérification de deux identités d'apparence assez anodine.

1.4. SUR CERTAINS SOUS-GROUPES

Dans ce numéro, G est supposé déployé. Si l'on choisit un tore maximal déployé T de G et un sous-groupe de Borel qui le contient, Δ s'identifie à une base du système de racines Φ de G par rapport à T . Soit α_0 l'opposée de la racine dominante correspondante et α_* un élément quelconque de Δ . On sait que $(\Delta - \{\alpha_*\}) \cup \{\alpha_0\}$ est une base d'un sous-système de racines, que nous notons $\Phi(\alpha_*)$, lequel définit un sous-groupe de rang maximum G_{α_*} de G dont l'image dans le groupe adjoint \tilde{G} sera désignée par \tilde{G}_{α_*} . Les groupes X du n° 1.3 sont des cas particuliers de tels G_{α_*} et d'autres cas particuliers joueront un rôle au § 4 ci-dessous ; ces exemples montrent l'intérêt qu'il y a à pouvoir déterminer commodément les centres de G_{α_*} et \tilde{G}_{α_*} . Il s'agit d'un exercice sur les systèmes de racines (cf. [9], 1.7) mais il est utile de retenir les deux algorithmes particulièrement simples suivants.

PROPOSITION 1. — *Si c désigne le coefficient de α_* dans la racine dominante, le centre de \tilde{G}_{α_*} est isomorphe au groupe μ_c des racines c -ièmes de l'unité.*

C'est immédiat.

PROPOSITION 2. — *Supposons α_0 isolé dans le graphe $(\Delta - \{\alpha_*\}) \cup \{\alpha_0\}$, soit Δ'_* le graphe $\Delta - \{\alpha_*\}$ et soit G'_* le sous-groupe semi-simple de G dont le graphe de Dynkin est Δ'_* (lequel est, on le sait, simplement connexe). Alors, le centre de G_{α_*} coïncide avec celui de G'_* ; autrement dit, G'_* contient le centre du sous-groupe de type A_1 correspondant à α_0 .*

Avec les notations et hypothèses de cette dernière proposition, il est facile de voir que le groupe de Weyl de Δ'_* contient -1 si et seulement si le groupe de Weyl de Δ contient -1 . La proposition 2 entraîne donc, par induction sur le rang, l'assertion suivante, d'ailleurs bien connue :

Corollaire. — *Le système de racines Φ possède des sous-systèmes de type $(A_1)^r$, où $r = \text{Card } \Delta$, si et seulement si -1 appartient au groupe de Weyl W de Φ ; ces sous-systèmes sont alors conjugués entre eux par W .*

Lorsque $-1 \in W$, la discussion précédente fournit un procédé effectif pour exhiber un sous-groupe de type $(A_1)^r$ de G et, toujours via la proposition 2, en déterminer le centre. Considérons par exemple le cas où Δ est de type E_8 . Par application itérée de la substitution $G \mapsto G_{\alpha_*}$, où α_* est comme dans la proposition 2, on obtient une suite décroissante de sous-groupes de rang 8, successivement de types

$$E_8, A_1 \times E_7, A_1^2 \times D_6, A_1^3 \times (A_1 \times D_4), A_1^4 \times (A_1 \times A_1^3) \cong A_1^8.$$

La proposition 2 implique que le centre du sous-groupe de type $(A_1)^8$ — appelons-le X — coïncide avec le centre, abélien élémentaire d'ordre 16, du facteur simplement connexe $A_1 \times (A_1)^3$ du dernier terme de la suite. La construction explicite ainsi décrite permet de déterminer l'action du normalisateur de X dans G sur l'ensemble des huit facteurs de type A_1 de X ; le résultat, énoncé ci-après, sera encore utilisé par la suite.

PROPOSITION 3. — *L'ensemble A des huit facteurs de type A_1 de X a une structure naturelle d'espace affine à trois dimensions sur \mathbf{F}_2 , caractérisée par la propriété suivante : si $\tilde{X} (\cong (\text{SL}_2)^8)$ désigne un revêtement universel de X et si l'on identifie, de façon évidente, le centre $C(\tilde{X})$ de \tilde{X} avec $(\mu_2)^8 = \mathcal{P}(A)$ (groupe des parties de A), le noyau de l'homomorphisme canonique $C(\tilde{X}) \rightarrow C(X)$ est constitué par l'ensemble vide, A et les quatorze plans de l'espace A . Le normalisateur de X dans G induit sur cet espace le groupe affine $\text{Aff}_3(\mathbf{F}_2)$.*

1.5. APPLICATION A QUELQUES QUESTIONS D'ALGÈBRE

On a observé dans le cours que la considération de l'invariant β fournit des explications naturelles de plusieurs faits bien connus, de nature purement algébrique. Citons trois exemples.

— *Il n'existe pas de forme quadratique anisotrope à dix variables de discriminant -1 et d'invariant de Witt nul* (sinon, en vertu d'un critère d'existence rappelé dans [8], il existerait un groupe de type E_6 dont le noyau anisotrope serait de type $\Delta^0 = D_5$, or Δ^0 doit être invariant par l'involution d'opposition qui, dans ce cas, permute les deux branches « longues » de $\Delta = E_6$).

— Si K est une extension quadratique de k , pour qu'une K -algèbre simple de dimension d^2 invariante par $\text{Gal}(K/k)$ possède une involution de seconde espèce σ fixant k il faut que l'image de sa classe dans $\text{Br } K$ par la corestriction $\text{Cores} : \text{Br } K \rightarrow \text{Br } k$ soit nulle (cela résulte du même critère d'existence appliqué aux groupes de type A_{d+1} extérieur tels que Δ^0 ne contienne pas les deux extrémités de Δ). (N.B. On sait que la condition est aussi suffisante).

— Toute algèbre simple à involution de première espèce de dimension 16 est produit tensoriel de deux algèbres de quaternions (le groupe unitaire d'une telle algèbre est de type C_2 , or $C_2 = B_2$ et l'invariant β d'un groupe de type B_2 est la classe de l'algèbre de Clifford paire d'une forme quadratique à cinq variables, donc d'un produit tensoriel de deux algèbres de quaternions).

Bien entendu, les démonstrations esquissées ici valent en toute caractéristique.

2. CORPS DE DÉPLOIEMENT

2.1. L'une des techniques essentielles pour la preuve du principe de Hasse est la descente galoisienne. Plusieurs leçons du cours ont été consacrées au problème du déploiement d'un groupe absolument presque simple G par des extensions de k « aussi petites que possibles ». Pour déployer G , une méthode se présente aussitôt à l'esprit, celle qui consiste à déployer un k -tore maximal T de G . Le groupe de Galois Γ opère sur le groupe des caractères de T par un sous-groupe de l'extension naturelle E du groupe des automorphismes extérieurs de G (groupe isomorphe à $\text{Aut } \Delta$) par le groupe de Weyl ; il s'ensuit que T , donc aussi G , se déploie sur une extension galoisienne de k dont le groupe de Galois est un sous-groupe de E . Il est intéressant de noter, à ce propos, que le groupe E avait été introduit par Elie Cartan, bien avant l'apparition du groupe de Weyl, comme « groupe de Galois de l'équation caractéristique de G ». On voit que E fournit une « borne supérieure » de la complication d'une extension nécessaire pour déployer G . Mais cette borne est étonnamment grossière, comme on va le voir.

2.2. GROUPES DE TYPE A

THÉORÈME 1 (Merkurjev-Suslin). — Soit n un entier. Supposons que k contienne les racines $(n + 1)$ -ièmes de l'unité et que tout élément de k soit une puissance $2(n + 1)$ -ième. Alors tout k -groupe de type A_n est déployé.

En fait, Merkurjev et Suslin donnent des renseignements beaucoup plus précis sur les extensions qui suffisent à déployer tous les k -groupes de type A_n , pour un corps k donné quelconque (cf. par exemple l'exposé [12] de C. Soulé). Dans l'énoncé ci-dessus, la présence du facteur 2 est rendue nécessaire par l'existence de groupes de type A extérieur ($\gamma(\Gamma) \cong \mathbf{Z}/2\mathbf{Z}$).

2.3. GROUPES DE TYPE DIFFÉRENT DE A_n (TOUT n) ET E_8

THÉORÈME 2. — (i) Si tout élément de k est un carré, tout k -groupe de type B_n , C_n , D_n ($n \neq 4$), D_4 non trialityaire (i.e. tel que 3 ne divise pas $\text{Card } \gamma(\Gamma)$) ou G_2 est déployé.

(ii) Si tout élément de k est une puissance sixième, tout k -groupe de type D_4 , F_4 , E_6 ou E_7 est déployé.

Soit G un groupe presque simple de l'un des types énumérés.

(i) L'hypothèse de l'énoncé et le théorème 1 (en fait, un théorème plus ancien de A.S. Merkurjev) impliquent que G est intérieur (i.e. $\gamma(\Gamma) = 1$), d'invariant β nul. Si G est de type B, C ou D, cela entraîne, vu l'interprétation de β en termes de représentations linéaires, qu'à isogénie centrale près, G est orthogonal ou symplectique, donc déployé (dans le cas orthogonal, on utilise à nouveau l'hypothèse $k^\times = k^{\times 2}$). Si G est de type G_2 , la forme quadratique invariante par sa représentation de dimension 7 est déployée et l'on sait qu'alors, G l'est aussi.

(ii) A nouveau, $\gamma(\Gamma) = 1$ et $\beta = 0$ en vertu de l'hypothèse de l'énoncé et du théorème 1. Si G est de type D_4 , on se trouve dans les conditions de (i). S'il est de type F_4 , il possède un k -sous-groupe de type D_4 , groupe engendré par les sous-groupes radiciels correspondant aux racines longues relativement à un k -tore maximal ; ce sous-groupe est déployé, comme on vient de le voir, donc G l'est aussi. Si G est de type E_6 (resp. E_7), il possède une k -représentation linéaire de dimension 27 (resp. 56), car $\beta = 0$, et l'on achève la preuve en utilisant le fait que le stabilisateur dans G d'un point de l'espace de cette représentation en position générale est un k -sous-groupe de type F_4 (resp. E_6).

Le cas des groupes de type E_8 sera considéré au § 4.

3. COHOMOLOGIE DE TORES MAXIMAUX

3.1. La cohomologie des tores maximaux joue un rôle primordial dans la démonstration par G. Harder du principe de Hasse pour certains types de groupes simples (cf. [4]). Son importance résulte principalement du théorème de Steinberg selon lequel si G est un groupe presque simple quasi-déployé, toute classe de cohomologie dans $H^1(\Gamma, G(k))$ est représentée par un cocycle à valeurs dans un k -tore maximal.

3.2. TORSION DE $H^1(k, T)$

Comme précédemment, G désigne un groupe absolument presque simple (non nécessairement simplement connexe) et T un k -tore maximal de G .

Plusieurs résultats auxiliaires établis dans [4], I, concernent la torsion de $H^1(k, T)$. Moyennant une addition de peu d'importance, ils peuvent être réunis en un énoncé unique :

PROPOSITION 4. — *Si p désigne un nombre premier ne divisant ni l'ordre de Aut Δ , ni l'ordre du centre d'un revêtement universel de G ni aucun des coefficients des racines simples de G dans la racine dominante, alors $H^1(k, T)$ n'a pas de p -torsion.*

Cette proposition est prouvée dans [4], I, § 3, pour tous les types de groupes simples à l'exception de G_2 et F_4 . Pour ces derniers, il suffit d'observer qu'un k -tore maximal T d'un groupe de type G_2 (resp. F_4) est contenu dans le k -sous-groupe de type A_2 (resp. D_4) engendré par les sous-groupes radiciels correspondant aux racines longues relatives à T .

On peut évidemment donner des bornes plus précises de l'exposant de $H^1(k, T)$. Dans cet ordre d'idée, le théorème 3.3 de [4], I, assure que si G est un groupe de type A_n intérieur, on a $(n + 1)^2 \cdot H^1(k, T) = \{0\}$, mais O. Gabber a fait observer que, convenablement analysée, la preuve de Harder, exposée dans le cours, établit en fait la relation $(n + 1) \cdot H^1(k, T) = \{0\}$.

3.3. SUR LE NOYAU DE L'APPLICATION $H^1(k, T) \rightarrow H^1(k, G)$

Soit $i : T \rightarrow G$ l'inclusion d'un k -tore maximal de G dans G . Dans la preuve du principe de Hasse, on se trouve parfois dans la situation suivante : on sait que l'application $i_* : H^1(T) \rightarrow H^1(G)$ s'annule sur une partie génératrice de $H^1(T)$ et l'on voudrait en déduire qu'elle s'annule sur $H^1(T)$. Cela ne va pas de soi puisque i_* n'est pas un homomorphisme de groupes. Dans un cas crucial, Harder tourne la difficulté par un calcul direct dont il m'a paru instructif de dégager le lemme suivant, non explicité dans [4]. Dans l'énoncé de ce lemme, K désigne une extension cyclique de k déployant T et σ est un générateur de $\text{Gal}(K/k)$. On note que si $g \in G(K)$ est tel que $g^{-1}g^\sigma \in T(K)$, alors sT est un k -tore.

LEMME 1. — *Soit $\text{Ker}_s i_*$ (« noyau stable ») l'intersection des noyaux des applications composées $H^1(T) \rightarrow H^1({}^sT) \rightarrow H^1(G)$, où g parcourt l'ensemble des éléments de $G(K)$ tels que $g^{-1}g^\sigma \in T(K)$ et où les deux flèches sont induites respectivement par $\text{ad } g$ et par l'inclusion ${}^sT \rightarrow G$. Alors, $\text{Ker}_{i_*} + \text{Ker } i_* \subset \text{Ker } i_*$; en particulier, le groupe engendré par $\text{Ker}_s i_*$ est contenu dans $\text{Ker } i_*$.*

La vérification est immédiate.

4. GROUPES DE TYPE E_8

Ceux-ci ont occupé une place importante dans le cours et fait l'objet d'un séminaire commun avec la chaire d'Algèbre et Géométrie.

4.1. CORPS QUADRATIQUEMENT ET CUBIQUEMENT CLOS

La proposition suivante, qui découle aisément des résultats du numéro 2.3 et de la proposition 3 du numéro 1.4, montre qu'un groupe de type E_8 qui ne se déploie pas sur un composé d'extensions quadratiques et cubiques « possède très peu de k -sous-groupes ». Dans tout ce numéro, k désigne un corps dont tout élément est une puissance sixième.

PROPOSITION 5. — Soit G un k -groupe non déployé de type E_8 . Alors, tout k -sous-groupe propre connexe non trivial de G est soit un tore de dimension 4 ou 8, soit un groupe de type A_4 ou $A_4 \times A_4$, soit, à isogénie centrale près, un groupe de la forme $R_{K/k} G_1$, où K est une extension galoisienne de degré 8 de k dont le groupe de Galois est isomorphe à un sous-groupe de $\text{Aff}_3(\mathbb{F}_2)$ et G_1 est un K -groupe simple anisotrope de rang 1.

Plus difficile est le théorème suivant qui, avec les résultats déjà obtenus par Harder, entraîne le principe de Hasse pour les groupes de type E_8 .

THÉORÈME 3 (Černousov-Premet). — Un k -groupe de type E_8 se déployant sur une extension cyclique de degré 5 de k possède un k -sous-groupe de type A_4 .

(N.B. L'énoncé de Černousov-Premet est un peu différent de celui-ci, qui tient compte de la proposition 5). Le lemme-clef pour la preuve de ce théorème est le suivant :

LEMME 2. — Soient L une algèbre de Lie complexe, E l'ensemble des éléments x de L tels que $[x, [x, L]] = Cx$, n un entier naturel et $(e_i \mid i \in \mathbb{Z}/n\mathbb{Z})$ une famille d'éléments de E tels que, pour $i, j \in \mathbb{Z}/n\mathbb{Z}$, e_i commute avec e_j dès que $i - j \neq \pm 1$. Alors, la sous-algèbre de L engendrée par les e_i est de dimension $\leq n^2 - 1$ et linéairement engendrée par les monômes de la forme $[e_i[e_{i+1}[\dots e_j]]\dots]$ de longueur $\leq n$.

Une preuve très simple de ce lemme a été donnée par J.-P. Serre dans le séminaire commun aux deux chaires.

4.2. CORPS DE NOMBRES

Pour déduire du théorème 3 le principe de Hasse pour les groupes de type E_8 , on a besoin des deux faits suivants. Ici, k désigne un corps de nombres et G est un k -groupe de type E_8 .

(i) *Le groupe G se déploie sur le corps des racines 30^N -ièmes de l'unité, pour N assez grand.*

Cela résulte facilement de la proposition 4 de 3.2 (qui provient de [4] dans le cas en question).

(ii) *Si G possède un k -sous-groupe de type $A_4 \times A_4$, il est déployé.*

La preuve esquissée par Harder dans [4] est calquée sur celle, due à M. Kneser, de l'assertion analogue sur un corps local. Elle fait usage de la remarque suivante : si $T \subset G$ est un k -tore maximal anisotrope de G se déployant sur une extension cyclique K de k de degré 5, toute orbite de $\text{Gal}(K/k)$ dans l'ensemble des racines de G relatives à T engendre un système de racines de type A_4 . Cela fournit six k -sous-groupes X_i ($i = 1, \dots, 6$) de type $A_4 \times A_4$ de G contenant T . Soient alors \tilde{X}_i un revêtement universel de X_i et T_i l'image réciproque de T dans \tilde{X}_i . On montre que les applications composées $H^1(\tilde{X}_i) \rightarrow H^1(X_i) \rightarrow H^1(G)$, donc aussi $H^1(T_i) \rightarrow H^1(T) \rightarrow H^1(G)$, sont nulles, et que les images des homomorphismes $H^1(T_i) \rightarrow H^1(T)$ engendrent $H^1(T)$. On utilise alors le lemme 1 ci-dessus pour faire voir que l'homomorphisme $H^1(T) \rightarrow H^1(G)$ est nul. L'assertion (ii) s'ensuit, car si G_1 est un k -groupe déployé de type E_8 , il est facile, utilisant un sous-groupe déployé de G_1 de type $A_4 \times A_4$, de trouver un k -tore maximal $T_1 \subset G_1$ et un K -isomorphisme $\varphi : G \rightarrow G_1$ induisant un k -isomorphisme de T sur T_1 , de sorte que la classe de cohomologie associée à φ appartient à l'image de $H^1(T)$ dans $H^1(G)$ et est donc nulle.

4.3. EXEMPLES DE FORMES ANISOTROPES

4.3.1. On peut se demander si l'assertion (ii) de 4.2 ne serait pas vraie quel que soit le corps de base k . En fait, elle est déjà fautive pour $k = \mathbf{Q}(t)$. De façon générale, reprenons les notations $G, \Delta, \alpha_*, G_*, c$ du numéro 1.4 ; le groupe G est donc déployé sur k (il ne sera pas l'exemple annoncé !). Posons $G_{\alpha_*} = X$ et soit ξ un cocycle continu de Γ à valeurs dans $X(\bar{k})$. D'après le théorème 1 de [9], il existe un élément g de $X(k(t^{1/c}))$ possédant les propriétés suivantes :

— l'image de g dans le groupe adjoint \tilde{X} de X appartient à $\tilde{X}(\bar{k}(t))$, de sorte que $\xi_1 = {}^g\xi$ est un cocycle à valeurs dans $X(\bar{k}(t))$ et que le groupe X tordu par ξ_1 , appelons-le X_1 , est $k(t)$ -isomorphe à X tordu par ξ ;

— tout $k(t)$ -tore déployé maximal de X_1 est aussi $k(t)$ -déployé maximal (et même $k((t))$ -déployé maximal) dans le groupe G tordu par ξ_1 , un $k(t)$ -groupe que nous notons G_1 .

Par exemple, si G est de type E_8 , on peut choisir α_* tel que X soit de type $A_4 \times A_4$, et ξ tel que X_1 , donc aussi G_1 , soit anisotrope. C'est le contre-exemple promis.

Une autre propriété de cet exemple peut être utile. S'il est anisotrope, le groupe ${}_{\xi}X$ (c'est-à-dire X tordu par ξ) de départ est « caractéristique » de la situation, en ce sens qu'il peut être retrouvé à partir du $k(t)$ -groupe G_1 ; en particulier, dans le cas de E_8 , deux racines α_* différentes fournissent des familles disjointes de formes anisotropes. En effet, il résulte de la construction et des théorèmes de Bruhat-Tits [2] que $G_1(k((t)))$ possède un seul sous-groupe parahorique, à savoir lui-même, et que ${}_{\xi}X$ n'est autre que le quotient semi-simple de la fibre spéciale du schéma en groupes associé à ce sous-groupe parahorique.

4.3.2. Un autre exemple de groupe de type E_8 « très tordu », provenant d'un résultat de A. Grothendieck [3], a été mis en évidence par Serre dans un exposé du séminaire. Soient G un groupe de type E_8 sur le corps des nombres complexes, V un espace vectoriel complexe et $G \rightarrow \mathrm{SL}(V)$ une représentation linéaire fidèle de G . Identifions G avec son image dans $\mathrm{SL}(V)$, posons $X = \mathrm{SL}(V)/G$, soit k le corps des fonctions rationnelles sur X et soit G_k le k -groupe de type E_8 déployé déduit de G par extension du corps de base. Les fibres fermées de la fibration $\mathrm{SL}(V) \rightarrow X$ sont des espaces homogènes principaux sur G , donc sa fibre générique est un espace homogène principal sur G_k dont le groupe d'automorphismes (commutant à G_k) est une k -forme tordue \hat{G} de G_k .

Il résulte de [3], proposition 4, que *le degré de toute extension de k déployant \hat{G} est divisible par 30.*

Utilisant la proposition 5, on en déduit facilement que *les seuls k -sous-groupes propres connexes non triviaux de \hat{G} sont ses k -tores-maximaux.*

En outre, si T est un k -tore maximal de \hat{G} et si k_1 est le corps des points fixes du normalisateur dans Γ d'un 5-sous-groupe de Sylow du groupe de Weyl de \hat{G} relatif à T , on peut voir que \hat{G} possède un k_1 -sous-groupe de type $A_4 \times A_4$ contenant T , or il n'est pas k_1 -déployé puisque 30 ne divise par $[k_1 : k]$. Ceci est un autre exemple donnant une réponse négative à la question posée au début du numéro 4.3.

RÉFÉRENCES

[1] R. BRAUER, *Über den Index und den Exponenten von Divisionsalgebren* (Tôhoku Math. J. 37 (1933), 77-87).

[2] F. BRUHAT et J. TITS, *Groupes réductifs sur un corps local* (I. Publ. Math. I.H.E.S., 41 (1972), 5-251 ; II., *ibid.*, 60 (1984), 5-184).

[3] A. GROTHENDIECK, *Torsion homologique et sections rationnelles* (in : Séminaire Chevalley, 2^e année (1958), Ecole Normale Supérieure, exposé n° 5).

[4] G. HARDER, *Über die Galoiskohomologie halbeinfacher Matrizengruppen* (I., *Math. Zeitschr.* 90 (1965), 404-428 ; II., *ibid.* 92 (1966), 396-415).

[5] C. SOULÉ, K_2 et le groupe de Brauer (d'après A.S. Merkurjev et A.A. Suslin) (in : Séminaire Bourbaki 1982-1983, exp. n° 601, novembre 1982, *Astérisque, Soc. Math. Fr.*, 105-106, 1983, 79-93).

[6] J.-P. TIGNOL et A.R. WADSWORTH, *Totally ramified valuations on finite-dimensional division algebras* (*Transactions A.M.S.*, 302 (1987), 223-250).

[7] J. TITS, *Représentations linéaires irréductibles d'un groupe réductif sur un corps quelconque* (*J. reine und angew. Math.*, 247 (1971), 196-220).

[8] — *Résumé de cours 1987-1988* (*Annuaire du Collège de France*, 88^e année, 85-100).

[9] — *Strongly inner anisotropic forms of simple algebraic groups* (*Journal of Algebra*, 131 (1990), 648-677).

J.T.

SÉMINAIRE COMMUN AVEC LA CHAIRE D'ALGÈBRE ET GÉOMÉTRIE

J.P. SERRE. — *Travaux de Černousov sur les groupes de type E_8 .*

J. TITS. — *Travaux de Černousov sur les groupes de type E_8* (2 exposés).

J.-P. SERRE. — *Remarques sur la cohomologie galoisienne des groupes semi-simples.*

PUBLICATION

J. TITS, *Symmetrie* (in : *Miscellanea mathematica*, recueil d'article dédiés à H. Götze, Springer-Verlag, 1991, 293-304).

MISSIONS

Cours et séries de conférences

— *Classification of algebraic simple groups over global fields*, Yale University, septembre à décembre 1990.

— *Kac-Moody groups*, Colloque à l'occasion du 80^e anniversaire de N. Jacobson, Yale U., octobre 1990, 4 exposés.

— *Monster and moonshine : a survey*, 9th Pitcher Lectures, Lehigh University, Bethlehem, PA, 3 exposés.

Exposés

— *Strongly inner simple algebraic groups*, Columbia University, octobre 1990.

— *On k -subgroups of $G(k[[t]])$* , Algebra seminar, Yale U., octobre 1990.

— *Automorphism groups of trees*, Ottawa, octobre 1990 ; Yale U., décembre 1990.

— *On semi-simple groups splitting over quadratic extensions*, Weisfeiler Lecture, PennState University, novembre 1990.

— *Twin buildings and groups of Kac-Moody type*, Institute for Advanced Study, Princeton N. J., novembre 1990.

— *On the splitting of the exact sequence $1 \rightarrow T \rightarrow N \rightarrow W \rightarrow 1$* , Algebra seminar, Yale U., décembre 1990.

— *Immeubles jumelés et groupes de Kac-Moody*, Ecole Polytechnique Fédérale de Lausanne, février 1991.

— *Buildings and Kac-Moody groups*, 18th Brazilian Mathematical Colloquium, Rio de Janeiro, juillet 1991.

Codirection avec P. SLOWOWY et T.A. SPRINGER d'un Colloque sur les Groupes Algébriques, Oberwolfach, avril 1991.

DISTINCTION

Elu associé de l'Académie royale des sciences, des lettres et des beaux-arts de Belgique, mai 1991.