SÉMINAIRE N. BOURBAKI

ROGER GODEMENT

Groupes linéaires algébriques sur un corps parfait

Séminaire N. Bourbaki, 1961, exp. n° 206, p. 11-32

<http://www.numdam.org/item?id=SB_1960-1961__6__11_0>

Séminaire BOURBAKI
13e année, 1960/61, n° 206

Décembre 1960

GROUPES LINÉAIRES ALGÉBRIQUES SUR UN CORPS PARFAIT

par Roger GODEMENT

Le but de cet exposé est essentiellement de fournir des outils qui se révèleront certainement nécessaires à l'étude des fonctions automorphes. Soit G un groupe linéaire algébrique semi-simple défini sur le corps $\mathbb{Q}$ des nombres rationnels, et soit G_A le groupe des adèles de G, dans lequel $G_{\mathbb{Q}}$ (points de G rationnels sur $\mathbb{Q}$) se plonge comme sous-groupe discret. Il est facile de conjecturer que $G_A/G_{\mathbb{Q}}$ est compact si et seulement si tout élément de $G_{\mathbb{Q}}$ est semi-simple, i. e. si $G_{\mathbb{Q}}$ ne contient aucun élément unipotent $\neq e$; c'est en tous cas démontré pour les groupes "classiques". Lorsque $G_A/G_{\mathbb{Q}}$ n'est pas compact, il est non moins facile de conjecturer qu'on doit pouvoir définir quelque chose d'analogue aux classiques "pointes paraboliques" de Poincaré, lesquelles doivent correspondre à des sous-groupes unipotents non triviaux de $G_{\mathbb{Q}}$, servir à définir un "domaine fondamental" dans G_A par des inégalités à la Minkowski, et permettre comme dans le cas de $SL(2, \mathbb{Q})$ la construction de "séries d'Eisenstein" fournissant le "spectre continu" de la représentation évidente de G_A dans l'espace de Hilbert $L^2(G_A/G_{\mathbb{Q}})$. On va, dans cet exposé, définir et étudier les "sous-groupes paraboliques", à l'aide des méthodes de la théorie des groupes algébriques. On montrera plus tard (dans le cas de $\mathbb{Q}$) comment on peut effectivement les utiliser à construire des "séries d'Eisenstein", qui convergent.

Les questions précédentes ont conduit le rédacteur, en 1959, à poser à BOREL (qui les a résolus) un certain nombre de problèmes de théorie des groupes algébriques ; le rédacteur a ensuite amélioré les méthodes de BOREL, principalement en éliminant presque totalement les algèbres de Lie (qui rendent triviales certaines démonstrations - celle du théorème 7 par exemple - en caractéristique 0), et en supprimant certaines hypothèses de caractéristique 0. Cela n'implique pas que BOREL n'en ait pas fait autant de son côté bien entendu.

Dans cet exposé, la lettre k désigne un corps "de base" a priori quelconque, la lettre Ω une extension algébriquement close de k, et Σ le groupe des k-automorphismes de Ω.

On utilisera constamment le Séminaire Chevalley [3] lequel, pour des raisons évidentes, sera cité Bible dans tout ce qui suit.

0. Espaces homogènes.

On aura constamment à parler de "variétés algébriques définies sur k "; cette expression sera prise au sens des Foundations de WEIL, attendu que les autres points de vue possibles, s'ils existent, n'ont encore fait l'objet d'aucun exposé si petit soit-il, et qu'en les adoptant "on" risquerait encore plus d'énoncer des assertions fausses ou non démontrées.

Une variété X définie sur k sera donc définie par les données suivantes : (a) un corps $k(X)$, extension régulière de type fini de k ; (b) un schéma dans $k(X)$ (Bible, 2-18). Si K est une extension de k, on notera X_K l'ensemble des points de X rationnels sur K ; un tel point est un couple formé par une localité $(M, \mathfrak{m})$ du schéma de X et par un k-homomorphisme $M \to K$ nul sur l'idéal maximal $\mathfrak{m}$ de M (cf. Bible, 2-20). On peut identifier X à l'ensemble X_Ω.

Pour tout corps K tel que $k \subset K \subset \Omega$, on peut définir sur X_Ω une K-topologie de Zariski. Des expressions telles que "connexe", "irréductible", "fermé", etc. se rapporteront toujours à la Ω-topologie ; si l'on a à utiliser la k-topologie on dira par exemple "k-fermé" au lieu de "fermé".

Soient X une variété définie sur k, et Y une partie k-fermée de X ; les composantes irréductibles de Y sont alors des variétés définies sur une extension algébrique de k, et si Y est elle-même irréductible c'est une variété définie sur une extension radicielle de k (donc sur k si k est parfait) ; on dira que Y est séparable sur k, si chaque composante irréductible de Y est définie sur une extension séparable de k. Noter que le groupe de Galois Σ opère sur X (i. e. sur X_Ω) et que les parties k-fermées de X ne sont autres que les parties fermées stables par Σ. Si k est parfait (hypothèse qui sera réalisée le plus souvent dans cet exposé), pour qu'une partie fermée Y de X soit une variété définie sur k il est donc nécessaire et suffisant qu'elle soit irréductible et stable par Σ.

Un groupe algébrique connexe défini sur k sera une variété G définie sur k, et munie d'une structure de groupe telle que l'application $(x, y) \to xy^{-1}$ soit un morphisme de variétés définies sur k. Si X est une variété définie sur k, on dira que G opère sur X si le groupe G opère sur l'ensemble X et si l'application $(g, x) \to gx$ de $G \times X$ dans X est un morphisme de variétés définies sur k. Un groupe algébrique connexe défini sur k sera dit linéaire si c'est une variété affine.

THÉORÈME 0. - Soient G un groupe algébrique défini sur k et H un sous-groupe k-fermé et séparable sur k de G. Il existe alors sur l'ensemble G/H une et une seule structure de variété algébrique définie sur k vérifiant les conditions suivantes :

(a) : l'application canonique $\pi : G \to G/H$ est un morphisme de variétés définies sur k ;

(b) : G opère sur G/H (au sens de la géométrie algébrique sur k ...) ;

(c) : soit f un k-morphisme de la variété G dans une variété X définie sur k ; pour que f se compose de π et d'un k-morphisme $G/H \to X$ il faut et il suffit que f soit constant sur les classes gH ;

(d) : Soient $K \subset \Omega$ une extension de k et ξ un point de $(G/H)_K$; alors la fibre $\pi^{-1}(\xi) \subset G$ est K-fermée et séparable sur K.

La Bible (exposé 8) ne traite, hélas, que le cas d'un corps de base algébriquement clos ; pour le cas général, on est obligé de s'en remettre aux papiers de Weil([5] et [6]) qui, n'adoptant pas (et pour cause) le langage des schémas, sont d'une lecture peu agréable pour les non spécialistes, et au surplus ne semblent pas démontrer (d), qui sert pourtant à tout propos. Il semble au rédacteur qu'une méthode "naturelle" de construction de la variété G/H devrait être la suivante : le corps $k(G/H)$ sera formé des $f \in k(G)$ invariantes à droite par H, et une localité de $k(G/H)$ appartient au schéma de G/H si et seulement si c'est l'intersection de $k(G/H)$ avec une localité de $k(G)$ appartenant au schéma de G. Cela ne semble d'ailleurs pas rendre triviale la vérification des axiomes. Bref, la situation est à tout le moins pénible (même en caractéristique 0, et même sur $\underset{\sim}{Q}$). Savoir qu'elle sera clarifiée par la théorie de Grothendieck n'est pas une consolation ...

"On" a donc décidé de prendre le théorème 0 pour argent comptant, et de s'en servir sans scrupules, en attendant qu'un spécialiste veuille bien en rédiger une démonstration dans le langage des schémas.

Il faudrait évidemment compléter l'énoncé en disant que, si H est invariant dans G, alors la structure algébrique de G/H est compatible avec sa structure de groupe.

1. Existence de points rationnels.

Le résultat suivant est dû à ROSENLICHT [2].

THÉORÈME 1 (k parfait infini). - Soit G un groupe linéaire algébrique connexe défini sur k ; alors G_k est dense dans G pour la topologie de Zariski sur Ω.

La démonstration est trop longue pour être exposée ici.

COROLLAIRE (k parfait). - Soit G un groupe linéaire algébrique connexe défini sur k ; alors G possède un tore maximal T défini sur k .

Si k est infini, alors d'après le théorème 1 et la Bible (7-04, corollaire 2) il existe un élément régulier $g \in G_k$; comme la décomposition d'un élément de G en parties semi-simple et unipotente est rationnelle sur tout corps de base, on aura aussi $g_s \in G_k$; donc le centralisateur $Z(g_s)$ est défini sur k , donc aussi sa composante connexe $Z_o(g_s)$ puisque k est parfait, et par suite le groupe de Galois de Ω sur k permute les tores maximaux de $Z_o(g_s)$; mais $Z_o(g_s)$ possède un seul tore maximal T , qui est donc défini sur k , et celui-ci est un tore maximal de G . Si k est fini, on utilise un argument de SERRE ([4], p. 119) consistant à remarquer que les tores maximaux de G forment un espace homogène sur G défini sur k (i. e. une variété définie sur k , sur laquelle G opère transitivement), lequel a donc (loc. cit.) au moins un point rationnel sur k (le rédacteur ne considère naturellement ce raisonnement que comme un schéma de démonstration).

2. Groupes résolubles décomposés.

Dans ce qui suit on désigne par A le groupe des matrices de la forme $\begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix}$, regardé comme groupe linéaire algébrique sur k , et par M le groupe des matrices $\begin{pmatrix} x & 0 \\ 0 & y \end{pmatrix}$, $xy = 1$, regardé aussi comme groupe linéaire algébrique sur k ; on les appellera groupe additif et groupe multiplicatif sur k (les notations standard sont G_a et G_m , mais on n'a que trop d'occasions d'utiliser la lettre G pour l'immobiliser une fois pour toutes ...)

Soit G un groupe linéaire algébrique connexe résoluble défini sur k ; on sait (Bible, 6-03, corollaire 1, et 7-06, Théorème 1) que G admet sur Ω une suite de composition

$$G = G_o \supset G_1 \supset \dots \supset G_n = e$$

dont les termes sont des sous-groupes fermés connexes, et dont les quotients sont isomorphes (sur Ω) soit à A soit à M . On dira que G est décomposé sur k si l'on peut former une suite de composition possédant les propriétés suivantes : chaque G_i est défini sur k , et chaque quotient G_i/G_{i+1} est isomorphe, comme groupe algébrique sur k , soit à A soit à M .

Les résultats qui suivent sont dûs essentiellement à ROSENLICHT.

THÉORÈME 2 (k quelconque). - Soient G un groupe linéaire algébrique connexe, résoluble, défini et décomposé sur k , et X une variété complète définie sur k et sur laquelle opère G .

Soit Y une partie k-fermée de X , stable par G , et contenant au moins un point de X_k ; alors G laisse fixe un point de $Y \cap X_k$.

Le cas ou $\dim(G) = 0$ étant trivial, on va raisonner par récurrence sur la dimension de G . Comme G est décomposé sur k , il y a dans G un sous-groupe fermé, connexe, résoluble, défini et décomposé sur k , soit H , tel que G/H soit isomorphe sur k soit à A soit à M . Par l'hypothèse de récurrence il y a un $y \in Y \cap X_k$ fixe par H ; l'application $g \to g.y$ définit alors, par passage au quotient, une application θ de G/H dans X qui est rationnelle sur k (propriété "universelle" des quotients), et en désignant par π l'application canonique $G \to G/H$ on a évidemment la formule $g.\theta(t) = \theta(\pi(g)t)$ pour $g \in G$, $t \in G/H$. Soit D la droite projective sur k ; comme X est complète, et comme G/H s'identifie (en tant que variété sur k) soit à $D - \{\infty\}$, soit à $D - \{0 , \infty\}$, l'application θ se prolonge en un morphisme défini sur k de D dans X , et on peut donc définir $\theta(\infty)$; comme $\infty \in D_k$ on a $\theta(\infty) \in X_k$, et comme $\theta(G/H)$ est contenu dans Y qui est k-fermé on a $\theta(\infty) \in Y$; reste à voir que $\theta(\infty)$ est fixe par G ; or considérons, pour g donné, les applications

$$\varphi : t \to \pi(g)\, t \qquad \text{de } T = G/H \text{ dans } T$$

$$\psi : x \to gx \qquad \text{de } X \text{ dans } X ;$$

on a la relation $\psi \circ \theta(t) = \theta \circ \varphi(t)$ pour tout $t \in T$, et en désignant encore par φ le prolongement de φ à D il vient donc $\psi(\theta(\infty)) = \theta(\varphi(\infty))$ i. e. $g.\theta(\infty) = \theta(\varphi(\infty))$, de sorte qu'il reste à montrer que $\varphi(\infty) = \infty$, ce qui est évident car φ est soit une translation $t \to t + t_0$ (cas du groupe A) soit une homothétie $t \to tt_0$ (cas du groupe M).

Dans l'énoncé qui suit, les notations sont les suivantes. On prend une clôture algébrique $\overline{k}$ de k , et on note k_s l'ensemble des $\xi \in \overline{k}$ séparables sur k (plus grande extension séparable de k contenue dans $\overline{k}$) ; si X est une variété algébrique définie sur k , on note X_s l'ensemble X_{k_s} ; on note Σ_s le groupe de Galois de l'extension k_s/k ; il opère sur X_s , et X_k est formé des points fixes de Σ_s dans X_s . Si X est un groupe algébrique défini sur k , on peut alors définir le groupe (sic) de cohomologie $H^1(\Sigma_s , X_s)$: c'est l'ensemble des applications $\sigma \to g(\sigma)$ de Σ_s dans X_s vérifiant $g(\sigma\tau) = g(\sigma)^{\tau} g(\sigma)$, modulo celles qui sont de la forme $g^{\sigma}.g^{-1}$ pour au moins un $g \in X_s$.

LEMME 1 (k quelconque). - Soit G un groupe linéaire algébrique connexe, résoluble, défini et décomposé sur k ; on a $H^1(\Sigma_s , G_s) = (e)$.

Supposons $\dim(G) = 1$; on a deux possibilités ; si $G = A$, alors G_s est le groupe additif k_s , et l'énoncé se réduit au théorème de la base normale ; si $G = M$, on a $G_s = k_s^*$, et l'énoncé se réduit au théorème 90 de Hilbert. Raisonnons maintenant par récurrence sur $\dim(G)$ et soit H un sous-groupe connexe, défini et décomposé sur k , de G , tel que G/H soit décomposé sur k et de dimension 1 . Montrons d'abord que la suite $(e) \to H_s \to G_s \to (G/H)_s \to (e)$ de Σ_s-modules est exacte ; il suffit de voir que tout $x \in (G/H)_s$ se remonte en un $g \in G_s$; or l'image réciproque de x dans G est une sous-variété de G définie, sur k_s (théorème 0), donc (S. LANG, [1], p. 76) possède un point rationnel sur la clôture séparable de k_s dans $\overline{k}$, i. e. rationnel sur k_s , ce qui prouve l'exactitude de la suite donnée. Ceci dit, on a une suite exacte de cohomologie

$$H^1(\Sigma_s , H_s) \to H^1(\Sigma_s , G_s) \to H^1(\Sigma_s , (G/H)_s)$$

et comme les termes extrêmes sont nuls d'après l'hypothèse de récurrence il en est de même du terme intermédiaire.

THÉORÈME 3 (k quelconque). - Soient G un groupe linéaire algébrique connexe, résoluble défini et décomposé sur k , et X un espace homogène principal pour G ([1]) ; alors X_k est non vide.

G étant connexe et opérant transitivement sur X , X est connexe, donc est une variété à la Weil, donc (S. LANG, loc. cit.) X_s est non vide ; choisissons un $x \in X_s$; pour tout $\sigma \in \Sigma_s$ il y a un et un seul $g(\sigma) \in G$ tel que $x^\sigma = g(\sigma).x$; vu l'axiome (FP) , on a $g(\sigma) \in G_s$, et il est clair que $\sigma \to g(\sigma)$ est un 1-cocycle de Σ_s à valeurs dans G_s ; donc (lemme 1) il y a un $g \in G_s$ tel que $g(\sigma) = g^\sigma . g^{-1}$; le point $g^{-1}.x$ est encore dans X_s , il est fixe par Σ_s , donc il est dans X_k (Cf. J. P. SERRE, [4], p. 170).

THÉORÈME 4. - Soient G un groupe linéaire algébrique connexe défini sur k et H un sous-groupe fermé, connexe, résoluble de G , défini et décomposé sur k .

([1]) Cela signifie que X est une variété définie sur k , que G opère sur X (l'application $G \times X \to X$ étant définie sur k), que quels que soient $x , y \in X$ il y a un $g(x , y) \in G$ et un seul tel que $y = g(x , y).x$, et enfin que l'application de $X \times X$ dans G ainsi définie est rationnelle sur k (axiome (FP) ...)

(a) (k quelconque). - Si G_k est dense dans G (ce qui est le cas si k est (2) parfait infini) la fibration de G par H est localement triviale, en particulier l'application $G_k \to (G/H)_k$ est surjective.

(b) (k parfait). - Soit X une variété définie sur k sur laquelle opère G , et supposons que H soit le stabilisateur d'un $x \in X_k$; alors $G.x \cap X_k = G_k.x$.

Montrons d'abord l'existence d'une "section rationnelle" de G au-dessus d'un ouvert de G/H . Pour cela, prenons pour Ω un "domaine universel" pour k , et soit x un point de G générique sur k ; son image $\xi = \pi(x)$ par l'application canonique $\pi : G \to G/H$ est un point de G/H générique sur k ; la classe $xH = \pi^{-1}(\xi)$ est donc une sous-variété de G définie sur $k(\xi) = K$ d'après le théorème Q. Regardant H comme défini sur K et opérant sur xH , il est évident que xH est un espace principal homogène pour H (car l'application $(u , v) \to u^{-1} v$ de $G \times G$ dans G est rationnelle sur k , donc induit une application $xH \times xH \to H$ rationnelle sur K) ; donc (théorème 3) il existe un $y \in xH$ rationnel sur $k(\xi)$, i. e. tel que $k(\xi) = k(y)$.

Comme ξ est point générique de G/H sur k , ceci montre l'existence d'une partie k-ouverte U de G/H , contenant ξ (et pour cause ...), et d'un k-morphisme $s : U \to G$ tel que $s(\xi) = y$; l'application $\pi \circ s$ de U dans G/H est rationnelle sur k et applique ξ sur ξ , c'est donc l'identité, et s la section rationnelle cherchée.

Supposons maintenant G_k dense dans G , alors $(G/H)_k$ est dense dans G/H puisque π est continue pour la topologie de Zariski sur k ; donc les ouverts GU , $g \in G_k$, recouvrent G/H , et on a, au-dessus d'un tel ouvert, une section rationnelle sur k , à savoir la translatée à gauche de s par g , ce qui achève la démonstration de (a).

Pour démontrer (b), considérons un $g \in G_\Omega$ tel que $g.x \in X_k$; pour tout $\sigma \in \Sigma$ on aura $g^\sigma.g^{-1} = h(\sigma)$ pour un $h(\sigma) \in H_\Omega$, et l'application $\sigma \to h(\sigma)$ est un cocycle de Σ à valeurs dans H_Ω , donc (lemme 1) un cobord ; par suite on peut "rectifier" g de façon que $g^\sigma = g$ pour tout σ , d'où le théorème.

---

(2) Soit $f : X \to Y$ un morphisme surjectif de variétés définies sur k ; on dit que f est localement trivial si, pour toute partie k-ouverte U assez petite de Y , il y a une application rationnelle $s : U \to X$ définie sur k telle que $f(s(u)) = u$ pour tout $u \in U$. Dans ce cas, l'application $X_k \to Y_k$ est évidemment surjective.

THÉORÈME 5 (k parfait). - Soit G un groupe linéaire algébrique connexe résoluble défini sur k . Pour que G soit décomposé sur k , il faut et il suffit que tout caractère rationnel de G soit défini sur k .

(On appelle caractère rationnel de G tout homomorphisme rationnel de G dans le groupe multiplicatif M , où l'on considère G et M comme groupes algébriques sur Ω , i. e. sur une clôture algébrique de k).

Supposons tout caractère de G rationnel sur k . Il existe un espace vectoriel V défini sur k tel que G soit un sous-groupe défini sur k de GL(V) . Comme G est résoluble et connexe, il y a un caractère χ de G tel que le sous-espace $V(\chi)$ de V formé des $x \in V$ vérifiant $g(x) = \chi(g)x$ soit non nul ; mais χ étant rationnel sur k , $V(\chi)$ est défini sur k , donc possède un point rationnel non nul. Raisonnant par récurrence on voit donc qu'il existe une base de V_k sur k par rapport à laquelle les matrices de G sont triangulaires. Il s'ensuit que G possède un sous-groupe fermé H , défini sur k , invariant dans G , tel que G/H soit de dimension 1 . Comme k est parfait, la composante connexe H^0 de H est aussi définie sur k (le groupe de Galois de Ω/k laisse en effet H^0 stable), ce qui permet de supposer H connexe. Tout caractère de H se prolonge en un caractère de G (on se ramène immédiatement au cas où G est un tore, auquel cas cela résulte de la Bible, 4-06), donc est défini sur k ; raisonnant par récurrence sur dim(G) , on peut donc supposer H décomposé sur k , et il reste à voir que G/H l'est aussi ; autrement dit, on peut supposer dim(G) = 1 .

Supposons d'abord G unipotent et considérons un isomorphisme $f : G \to A$ de groupes algébriques sur Ω ; pour tout $\sigma \in \Sigma$ groupe de Galois de Ω/k , l'application f^σ donnée par $x \to f(x^{\sigma-1})^\sigma$ est encore un isomorphisme de G sur A ; donc f et f^σ ne diffèrent que par un automomorphisme de A , i. e. on peut écrire

$$f^\sigma(x) = a(\sigma).f(x)$$

où $a(\sigma) \in \Omega^*$ est bien déterminé ; évidemment $\sigma \to a(\sigma)$ est un 1-cocycle de Σ à valeurs dans Ω^* , donc un cobord, et par suite $a(\sigma) = a^\sigma.a^{-1}$ pour au moins un $a \in \Omega^*$; alors $x \to a^{-1}.f(x)$ est un isomorphisme de G sur A invariant par Σ , i. e. rationnel sur k ; l'homomorphisme réciproque f^{-1} est défini sur k pour la même raison, et par suite G et A sont isomorphes sur k .

Supposons maintenant que G soit un tore ; il y a alors un caractère χ de G tel que $x \to \chi(x)$ soit un isomorphisme, sur Ω , de G sur le groupe multiplicatif M ; puisque χ est rationnel sur k , l'application réciproque l'est aussi

(car invariante par Σ), donc χ est un isomorphisme de groupes algébriques sur k.

Il reste enfin à vérifier que tout caractère χ d'un groupe G décomposé sur k est rationnel sur k. Soit H un sous-groupe connexe de G, défini et décomposé sur k, tel que G/H soit isomorphe sur k au groupe multiplicatif M. Raisonnant par récurrence sur la dimension de G, on peut supposer que la restriction de χ à H est définie sur k. Pour tout automorphisme $\sigma \in \Sigma$, les caractères χ^σ et χ coïncident alors sur H, donc $\chi^\sigma - \chi$ définit par passage au quotient un caractère $\chi(\sigma)$ de $G/H = M$; or le groupe des caractères de G/H est nul ou isomorphe à $\underset{\sim}{Z}$, et Σ opère trivialement sur ce groupe (car les caractères de M sont les applications $x \to x^r$, lesquelles sont évidemment rationnelles sur k) ; ainsi $\sigma \to \chi(\sigma)$ est un 1-cocycle de Σ à valeurs dans $\{0\}$ ou $\underset{\sim}{Z}$, qui d'ailleurs ne fait intervenir qu'un quotient fini de Σ (car χ est rationnel sur une extension finie de k), et par suite le cocycle en question est un homomorphisme dans $\{0\}$ ou dans $\underset{\sim}{Z}$ d'un quotient fini de Σ, donc est nul, ce qui achève la démonstration.

3. Théorèmes de conjugaison.

Les résultats de ce numéro sont dûs à A. BOREL.

THÉORÈME 6 (k parfait). - *Soit G un groupe linéaire algébrique connexe défini sur k ; soient M et N deux sous-groupes fermés, connexes, résolubles, définis et décomposés sur k, et maximaux relativement aux conditions énoncées. Il existe un $g \in G_k$ tel que $gNg^{-1} = M$.*

Nous utiliserons deux lemmes.

LEMME 2 (k quelconque). - *Soient G un groupe linéaire algébrique connexe défini sur k et H un sous-groupe fermé défini sur k de G. Il existe un espace vectoriel V défini sur k, une représentation linéaire ρ de G dans V définie sur k, et un vecteur non nul $a \in V_k$, tel que H soit l'ensemble des $g \in G$ pour lesquels la droite (a) est stable par $\rho(g)$.*

(Cf. Bible, 10-06, pour le cas d'un corps algébriquement clos). Soient $A = \Omega[G]$ l'algèbre affine de G et α l'idéal de H dans A ; il est engendré par des fonctions f_i rationnelles sur k et linéairement indépendantes sur k. Les translatées des f_i engendrent sur Ω un espace vectoriel W de dimension finie, et en qualifiant de "rationnels sur k" les éléments de W qui, (comme fonctions sur G) sont définis sur k, on obtient sur W une structure d'espace vectoriel défini

sur k. Si les f_i sont en nombre r, on prend alors pour V la puissance extérieure r-ième de W, pour a le vecteur $f_1 \wedge \dots \wedge f_r$ et pour ρ la puissance extérieure r-ième de la représentation régulière de G dans W.

LEMME 3 (k quelconque). - Soient V un espace vectoriel défini sur k, et X la variété des drapeaux de V (qui est complète et définie sur k) ; alors X_k est l'ensemble des drapeaux définis par les bases de V_k sur k.

Soit $(e_1, \dots, e_n)$ la base de V_k servant à définir la structure de variété sur k de X : si B est le stabilisateur dans $GL(V)$ du drapeau défini par cette base, on identifie X à $GL(V)/B$. Or il est clair que B est connexe, résoluble, défini et décomposé sur k ; et si k est infini, il est clair que $GL(V)_k$ est dense dans $GL(V)$; dans ce cas, le lemme résulte donc du théorème 4, (a) ; si k est fini, k est parfait, et le lemme résulte heureusement du théorème 4, (b). Il y a naturellement d'autres possibilités pour définir sur X une structure de variété sur k, par exemple en plongeant X dans un produit d'espaces projectifs ; on peut espérer que ces structures coïncident avec celle qu'on a définie ici ...)

Démonstration du théorème 6. - Vu le lemme 2 on peut supposer que G est un sous-groupe (fermé, connexe, défini sur k) d'un $GL(V)$, où V est défini sur k, et que M est le stabilisateur dans G d'une droite (a_1) de V, avec $a_1 \in V_k$; faisant opérer M sur la variété des drapeaux de $V/(a_1)$, et tenant compte du lemme 3 et du théorème 2, on voit qu'il existe une base $(a_1, a_2, \dots, a_n)$ de V_k par rapport à laquelle les matrices de M sont triangulaires, et cette propriété caractérise les éléments de M puisque M est déjà le stabilisateur de la droite (a_1). Par conséquent, si X désigne la variété des drapeaux de V, on voit que M est le stabilisateur dans G d'un $x \in X_k$. Soit alors Y l'adhérence dans X de l'orbite $G.x$; d'après le théorème 2, N laisse fixe un $y \in Y_k$; soit S le stabilisateur de y dans G ; il est k-fermé, donc sa composante connexe S^0 est définie sur k (puisque k est parfait) ; de plus les matrices de S^0 sont triangulaires par rapport à une base de V_k, donc S^0 est décomposé sur k ; comme $S^0 \supset N$ on a $S^0 = N$ en vertu de la maximalité de N. Il résulte de là qu'en supposant (ce qui est permis) que $\dim(M) \geqslant \dim(N)$, on a

$$\dim(G.y) = \dim(G) - \dim(N) \geqslant \dim(G) - \dim(M) = \dim(G.x)$$

et par suite $y \in G.x \cap X_k$; donc (théorème 4, (b)) $y = g.x$ pour un $g \in G_k$, et $g^{-1} Ng \subset M$, ce qui termine la démonstration.

COROLLAIRE 1 (k parfait). - Soient S et T deux sous-tores de G , définis et décomposés sur k , et maximaux relativement à ces conditions. Il existe un $g \in G_k$ tel que $gSg^{-1} = T$.

En immergeant S et T dans des sous-groupes résolubles définis et décomposés sur k et maximaux, on se ramène au cas où G est résoluble et décomposé sur k ; soit X l'ensemble des $g \in G$ tels que $gSg^{-1} = T$; X est non vide (Bible, 6-06), et le normalisateur N(S) opère sur X de façon simplement transitive ; mais comme S est un tore maximal de G qui est résoluble, on a $N(S) = Z(S)$, (Bible, 6-14) et Z(S) est connexe (idem) ; comme Z(S) est contenu dans G qui est décomposé sur k , Z(S) est aussi défini et décomposé sur k (d'ailleurs tout caractère de Z(S) se prolonge à G donc est défini sur k). Ceci fait, X est évidemment k-fermé et connexe, donc (puisque k est parfait) c'est une variété définie sur k , et même un espace homogène principal pour Z(S) ; donc (théorème 3) X a un point rationnel sur k .

COROLLAIRE 2 (k parfait). - Soient G un groupe linéaire algébrique connexe défini sur k , et U , V des sous-groupes fermés, connexes, unipotents, définis sur k , et maximaux relativement à ces conditions. Alors il existe un $g \in G_k$ tel que $V = gUg^{-1}$.

En effet U est décomposé sur k (théorème 5) donc contenu dans un sous-groupe résoluble M défini et décomposé sur k , et maximal ; évidemment $U = M^u$, d'où immédiatement le corollaire.

4. Sous-groupes paraboliques (trivialité locale).

Soit G un groupe linéaire algébrique défini sur k ; on appelle sous-groupe parabolique de G tout sous-groupe H de G qui est fermé, défini sur k , et contient un sous-groupe de Borel (défini sur Ω) de G , autrement dit (Bible, 6-09) tel que la variété G/H soit complète.

Un sous-groupe parabolique H est nécessairement connexe et identique à son normalisateur dans G . Établissons la seconde assertion ; soit B un sous-groupe de Borel de H , donc de G ; si $g \in N(H)$, gBg^{-1} est encore un sous-groupe de Borel de H , donc (Bible, 6-09) on a $gBg^{-1} = hBh^{-1}$ pour un $h \in H$; donc $N(H) \subset H.N(B)$; mais $N(B) = B$ (Bible, 9-03), d'où $N(H) = H$. Le fait que H est connexe résulte de là si l'on observe que (en prenant Ω pour corps de base) H^o est un sous-groupe parabolique normalisé par H .

Le résultat qui suit a été établi par A. BOREL en caractéristique 0 (il y a un an) à l'aide de la théorie des algèbres de Lie.

THÉORÈME 7 (k parfait infini). - Soient G un groupe linéaire algébrique connexe défini sur k et H un sous-groupe parabolique de G ; alors la fibration de G par H est localement triviale. Si U est la partie unipotente du radical de H , alors H est le normalisateur de U dans G .

Soit R^u la partie unipotente du radical de G ; comme k est parfait, R^u est décomposé sur k , et d'après le théorème 4, (a), la fibration de G par R^u est localement triviale ; de plus H contient un sous-groupe de Borel de G , donc contient R^u ; il suffit donc d'établir le théorème pour G/R^u , ce qui revient à supposer G réductif (ce qui veut dire que le radical de G est un tore, à savoir la composante connexe du centre de G ; les théorèmes démontrés dans la Bible pour les groupes semi-simples s'étendent trivialement aux groupes réductifs, au besoin avec des modifications évidentes).

Soient G un groupe réductif connexe défini sur k , H un sous-groupe parabolique de G , et T un tore maximal défini sur k de H . T est un tore maximal d'un sous-groupe de Borel de H , donc d'un sous-groupe de Borel de G , c'est donc un tore maximal de G ; on peut donc parler des racines de G par rapport à T (Bible, 12-04), dont on désignera l'ensemble par $\mathcal{R}_G$. Chaque $\alpha \in \mathcal{R}_G$ est un caractère de T qui est défini sur Ω ; la composante connexe Q_α du noyau de α est un sous-tore de codimension 1 de T (rappelons que ces sous-tores sont caractérisés par le fait d'être contenus dans une infinité de sous-groupes de Borel de G), dont le centralisateur dans G est noté Z_α ; le radical de Z_α est Q_α (Bible, 12-09), Z_α est connexe (Bible, 6-14), et possède deux sous-groupes de Borel contenant T , qui sont du reste les intersections avec Z_α des sous-groupes de Borel de G contenant T , et dont les parties unipotentes sont de dimension 1 , donc isomorphes (sur Ω) au groupe additif G_a (Bible, 13-05) ; plus précisément, il existe un isomorphisme τ_α de G_a sur un sous-groupe P_α (fermé et défini sur Ω) de Z_α , invariant par T , tel que l'on ait

$$t.\tau_\alpha(x).t^{-1} = \tau_\alpha(\alpha(t)x) \qquad \text{pour } t \in T , \ x \in G_a \ ;$$

le sous-groupe $T.P_\alpha$ est un groupe de Borel bien déterminé de Z_α , et P_α en est la partie unipotente ; l'autre groupe de Borel de Z_α est $T.P_{-\alpha}$ (on note additivement le groupe des caractères de T).

Notons enfin que le groupe de Galois Σ de l'extension Ω/k opère sur les racines de G par rapport à T - autrement dit, si α est racine, il en est de même du caractère α^σ ($\sigma \in \Sigma$) de T, et on a les relations

$$Q_{\alpha^\sigma} = (Q_\alpha)^\sigma , \qquad Z_{\alpha^\sigma} = (Z_\alpha)^\sigma , \qquad P_{\alpha^\sigma} = (P_\alpha)^\sigma \quad .$$

Cela posé, revenons au sous-groupe parabolique $H \supset T$ de G. Soit $\mathcal{R}_H$ l'ensemble des $\alpha \in \mathcal{R}_G$ telles que $P_\alpha \subset H$; cet ensemble de racines se décompose en deux parties disjointes :

$$\mathcal{R}'_H : \ \alpha \in \mathcal{R}_H \quad \text{telles que} \quad -\alpha \in \mathcal{R}_H$$

$$\mathcal{R}''_H : \ \alpha \in \mathcal{R}_H \quad \text{telles que} \quad -\alpha \notin \mathcal{R}_H \quad .$$

Comme H est défini sur k, il est clair que $\mathcal{R}_H$, $\mathcal{R}'_H$ et $\mathcal{R}''_H$ sont stables par le groupe de Galois Σ. Dans ce qui suit on pose

$$U = \text{partie unipotente du radical de } H \quad ;$$

U est un sous-groupe fermé, connexe, unipotent et défini sur k de G, invariant dans H, donc invariant par T ; donc (Bible, 13-05) U est le produit semi-direct des P_α contenus dans U.

LEMME 4 (k quelconque). - *Les relations* $P_\alpha \subset U$ *et* $\alpha \in \mathcal{R}''_H$ *sont équivalentes.*

Supposons $\alpha \in \mathcal{R}'_H$; alors H contient P_α, $P_{-\alpha}$ et T, donc contient les deux groupes de Borel $T.P_\alpha$ et $T.P_{-\alpha}$ de Z_α qui contiennent T, donc (Bible, 12-07) contient Z_α ; ainsi

$$\alpha \in \mathcal{R}'_H \quad \text{équivaut à} \quad Z_\alpha \subset H \quad .$$

Pour une telle racine α, $Z_\alpha \cap U$ est un sous-groupe invariant et unipotent de Z_α, dont la composante connexe est donc dans le radical de Z_α, i. e. dans Q_α, donc se réduit à l'élément neutre ; autrement dit $Z_\alpha \cap U$ est fini (et en fait réduit à $\{e\}$, car $Z_\alpha \cap U$ est connexe en vertu des allusions contenues dans la Bible, 6-02, bas de la page). Il s'ensuit que $P_\alpha \subset U$ exige $\alpha \in \mathcal{R}''_H$. Inversement, supposons $\alpha \in \mathcal{R}''_H$; le centralisateur de Q_α dans H, i. e. $H \cap Z_\alpha$, contient $T.P_\alpha$; mais $\dim(Z_\alpha/T.P_\alpha) = 1$; on a donc soit $H \cap Z_\alpha = T.P_\alpha$, soit $H \cap Z_\alpha = Z_\alpha$; le second cas est exclu comme on l'a vu plus haut, donc $H \cap Z_\alpha = T.P_\alpha$; mais alors P_α est le radical unipotent du centralisateur de Q_α dans H, donc est contenu dans le radical unipotent de H (Bible, 12-09), i. e. dans U, ce qui achève la démonstration.

COROLLAIRE. - H est le normalisateur de U dans G .

On a $N(U) \supset H$ donc $N(U)$ est un sous-groupe parabolique de G , engendré par T et les P_β qu'il contient ; si $\beta \in \mathcal{R}_H$ on a $P_\beta \subset H$; sinon on a $\beta = -\alpha$ pour un $\alpha \in \mathcal{R}''_H$, et alors $N(U)$ contient le sous-groupe engendré par T , P_α et $P_{-\alpha}$, i. e. Z_α , et de plus (comme $U \cap Z_\alpha = P_\alpha$) $P_{-\alpha}$ normalise P_α ; mais Z_α/Q_α est un revêtement du groupe projectif à une variable (Bible, 12-01) et dans celui-ci l'assertion que $P_{-\alpha}$ normalise P_α est fausse. Donc $N(U)$ est engendré par les P_α , $\alpha \in \mathcal{R}_H$, d'où le corollaire.

LEMME 5 (k quelconque). - Toute racine $\alpha \in \mathcal{R}_G$ qui est combinaison linéaire à coefficients rationnels positifs d'éléments de $\mathcal{R}''_H$ est dans $\mathcal{R}''_H$.

Soit B un sous-groupe de Borel de H (donc de G) contenant T ; dans l'ensemble $\Gamma(T)$ des sous-groupes à un paramètre de T , soit (B) la chambre déterminée par B (Bible, 10-09); on sait (Bible, 13-05) que les racines α telles que $P_\alpha \subset B$ sont celles qui sont négatives sur (B) . Or U est contenu dans tout sous-groupe de Borel de H , et c'est même (Bible, 12-07) la composante connexe de la partie unipotente de l'intersection des sous-groupes de Borel de H contenant T . Vu le lemme 4, l'ensemble $\mathcal{R}''_H$ est donc formé des racines de G par rapport à T qui sont négatives sur (B) dès que $T \subset B \subset H$, ce qui implique trivialement le lemme.

LEMME 6 (k parfait). - Soit $\tilde{U}$ le sous-groupe fermé de G engendré par les $P_{-\alpha}$, $\alpha \in \mathcal{R}''_H$; alors la relation $P_\beta \subset \tilde{U}$ équivaut à $-\beta \in \mathcal{R}''_H$; le sous-groupe $\tilde{U}$ est défini sur k et unipotent.

Le groupe de Galois Σ permute les éléments de $\mathcal{R}_H$ puisque H est défini sur k , donc aussi ceux de $-\mathcal{R}''_H$; il s'ensuit que $\tilde{U}$ est défini sur k .

Le groupe $\tilde{U}$ est unipotent ; en effet, si B est un groupe de Borel contenant U , le symétrique $\tilde{B}$ de B par rapport à T (Bible, 13-07), engendré par les P_α avec $P_{-\alpha} \subset B$, contient évidemment $\tilde{U}$, et comme $\tilde{U}$ est engendré par des groupes unipotents, on a même $\tilde{U} \subset \tilde{B}^u$, d'où notre assertion. Ceci dit, le lemme 5 et la Bible, 17-03, corollaire, montrent que $\tilde{U}$ est produit semi-direct (sic) des P_α , $\alpha \in -\mathcal{R}''_H$; et d'après la Bible, 13-05, ces P_α sont les seuls que contient U , d'où le lemme.

LEMME 7 (k parfait). - L'application (u , h) $\to$ uh de $\tilde{U} \times H$ dans G est un k-isomorphisme de la variété $\tilde{U} \times H$ sur une sous-variété ouverte et définie sur k de G (à savoir $\tilde{U}.H$) .

Soit B un sous-groupe de Borel de H contenant T et soit $\tilde{B}$ le sous-groupe de Borel de G symétrique de B par rapport à T ; on sait (Bible, 15-01) que $\tilde{B}.B$ est ouvert pour la topologie de Zariski de G . Pour montrer que $\tilde{U}.H$ est ouvert, il suffit donc de montrer qu'il contient $\tilde{B}.B$, ou même $\tilde{B}^u$. Or soit $R_B \supset R''_H$ l'ensemble des racines α telles que $P_\alpha \subset B$; notons $(\alpha_i)_{1\leqslant i\leqslant m}$ les éléments de R''_H et $(\beta_j)_{1\leqslant j\leqslant n}$ les éléments de R_B qui ne sont pas dans R''_H ; comme $\tilde{B}$ est engendré par T et les $P_{-\gamma}$, avec $\gamma \in R_B$, on a (Bible, 13-05)

$$\tilde{B}^u = P_{-\alpha_1} \dots P_{-\alpha_m} P_{-\beta_1} \dots P_{-\beta_n} \quad ;$$

les m premiers termes sont dans $\tilde{U}$, les suivants sont dans H , ce qui montre comme annoncé que $\tilde{U}.H \supset \tilde{B}.B$.

Montrons maintenant que $\tilde{U} \cap H$ se réduit à l'élément neutre. Celle-ci est contenue dans un groupe de Borel contenant T , donc (Bible, 13-05) est engendrée par les P_α qu'elle contient ; mais $P_\alpha \subset \tilde{U} \cap H$ exige $-\alpha \in R''_H$ d'après le lemme 6, et $\alpha \in R_H$, ce qui est impossible ; d'où le résultat annoncé.

On voit donc déjà que l'application évidente $f : \tilde{U} \times H \to \tilde{U}.H$ est une bijection rationnelle et définie sur k de $\tilde{U} \times H$ sur une partie k-ouverte de G . En raisonnant comme dans la Bible, 15-02, on voit que f^{-1} est rationnelle, et évidemment définie sur k puisqu'invariante par le groupe de Galois Σ ; donc f est un isomorphisme de variétés définies sur k .

Démonstration du théorème 7. - D'après le lemme 7, l'application canonique $G \to G/H$ induit un k-isomorphisme de $\tilde{U}$ sur une partie k-ouverte de G/H , d'où l'existence d'une section rationnelle ; comme k est parfait et infini, G_k est dense dans G , et par suite la fibration de G par H est localement triviale. (On notera que l'hypothèse que k est infini n'avait pas été utilisée jusqu'à maintenant).

COROLLAIRE 1 (k parfait infini). - *Soient G un groupe linéaire algébrique connexe défini sur k , H un sous-groupe parabolique de G , et M un sous-groupe fermé, connexe, résoluble de G , défini et décomposé sur k . Il existe un $g \in G_k$ tel que $gMg^{-1} \subset H$.*

On fait opérer M sur G/H et on applique le théorème 2 .

COROLLAIRE 2 ($k = \underset{\sim}{Q}$). - *Soient G un groupe linéaire algébrique connexe défini sur $\underset{\sim}{Q}$ et H un sous-groupe parabolique de G ; soit G_A (resp. H_A) le groupe des adèles de G (resp. H) ; alors G_A/H_A est compact.*

Comme la fibration de G par H est localement triviale, on a $(G/H)_A = G_A/H_A$, et comme G/H est complète, l'espace $(G/H)_A$ est compact (cf. A. Weil [7]).

5. Existence de sous-groupes paraboliques.

THÉORÈME 8 (k parfait). - Soit G un groupe linéaire algébrique réductif connexe défini sur k ; les propriétés suivantes sont équivalentes :

(a) G possède un sous-groupe parabolique $H \neq G$;

(b) G contient un tore S défini et décomposé sur k et non contenu dans le centre de G.

Démonstration de (a) $\Longrightarrow$ (b). (On utilise les notations et résultats du paragraphe précédent). Considérons le caractère

$$\chi = \sum_{\alpha \in \mathcal{R}''_H} \alpha$$

de T ; comme le groupe de Galois Σ permute les $\alpha \in \mathcal{R}''_H$, il est clair que χ est défini sur k ; si de plus B est un groupe de Borel contenant T et contenu dans H, donc contenant le radical unipotent U de H, les $\alpha \in \mathcal{R}''_H$ sont négatives sur la chambre de Weyl définie par B (cf. démonstration du lemme 5), donc χ n'est pas le caractère unité. (Il faut encore, pour que ce raisonnement soit correct, vérifier que $\mathcal{R}''_H$ est non vide ; mais si $\mathcal{R}''_H$ est vide, alors $\mathcal{R}_H = \mathcal{R}_G$ et $G = H$ puisque G est engendré par les P_α, $\alpha \in \mathcal{R}_G$). Il est de plus clair que χ est trivial sur le centre de G. Pour montrer que (a) $\Longrightarrow$ (b) il suffit donc d'établir le lemme suivant :

LEMME 8 (k parfait). - Soit T un tore défini sur k possédant un caractère χ non trivial défini sur k ; alors T contient un tore défini et décomposé sur k, sur lequel χ est non trivial.

Soit $\hat{T}$ le groupe additif des caractères définis sur Ω de T ; il est isomorphe à $\underset{\sim}{Z}^n$, $n = \dim(T)$, et le groupe de Galois Σ opère sur $\hat{T}$, en ayant par hypothèse des points fixes non nuls. Soit S un sous-tore de T et $S^\perp$ l'ensemble des $\chi \in \hat{T}$ induisant l'identité sur S ; on sait (Bible, 4-05 et 4-06) que S est l'intersection des noyaux des $\chi \in S^\perp$ et que $\hat{S}$ est isomorphe à $\hat{T}/S^\perp$ (quotient qui n'a donc pas de torsion) ; inversement, si A est un sous-groupe de $\hat{T}$ tel que $\hat{T}/A$ soit sans torsion, il y a un sous-tore et un seul S de T tel que $A = S^\perp$, et il est clair que S est défini sur k si et seulement si A est stable par Σ ; cette condition étant satisfaite, S sera décomposé sur k si et seulement si Σ opère trivialement sur $\hat{T}/A$.

Pour démontrer le lemme, tout revient donc à construire un sous-groupe A de T satisfaisant aux conditions suivantes :

(i) $\hat{T}/A$ est sans torsion (i. e. A est "primitif") ;

(ii) A est stable par Σ et Σ opère trivialement sur $\hat{T}/A$;

(iii) $\chi \notin A$.

Considérons pour cela l'espace vectoriel $V = \underset{\sim}{Q} \otimes_{\underset{\sim}{Z}} \hat{T}$, de dimension n ; comme Σ opère sur $\hat{T}$ on a une représentation linéaire de $\underset{\sim}{\Sigma}$ dans V , représentation dont le noyau est un sous-groupe d'indice fini de Σ (car T est décomposé sur une extension galoisienne de degré fini de k) ; cette représentation est donc semi-simple (théorème de Mashke) et V est somme <u>directe</u> de deux sous-espaces V' et V'' stables par Σ , à savoir le sous-espace V' des points de V fixes par Σ , et le sous-espace V'' engendré par les vecteurs $v^\sigma - v$ ($v \in V$, $\sigma \in \Sigma$); par hypothèse on a $V' \neq 0$, donc $\dim(V'') < n$; soit $A = V'' \cap \hat{T}$, il est clair que A vérifie les conditions (i), (ii), (iii). (Démonstration fournie gracieusement par C. CHEVALLEY).

<u>Démonstration de</u> (b) $\Longrightarrow$ (a). - Soit S un sous-tore de G , défini et décomposé sur k , et non contenu dans le centre de G . On va lui attacher un sous-groupe parabolique de G en choisissant, sur le groupe $\hat{S}$ des caractères de S , une relation d'ordre totale compatible avec l'addition dans $\hat{S}$. On suppose donc dans ce qui suit choisie une telle relation d'ordre ; on choisit un tore maximal T de G , défini sur k et contenant S ; et pour toute racine α de G par rapport à T , on note $n(\alpha) \in \hat{S}$ la restriction de α à S . Notant R_G l'ensemble des racines de G par rapport à T , on définit les parties suivantes de R_G :

R^+ = ensemble des α telles que $n(\alpha) \geqslant 0$;

R^{++} = ensemble des α telles que $n(\alpha) > 0$;

R^0 = ensemble des α telles que $n(\alpha) = 0$,

de sorte que R^0 et R^{++} constituent une partition de R^+ . Soit H le sous-groupe fermé de G engendré par T et les sous-groupes à un paramètre P_α pour $\alpha \in R^+$: on va montrer que H est un sous-groupe parabolique $\neq G$.

Il est clair puisque S est décomposé sur k que R^+ est stable par le groupe de Galois Σ ; donc H est défini sur k . D'autre part, R^+ vérifie trivialement

les deux conditions suivantes ([3]) : si une racine α est combinaison linéaire à coefficients entiers $\geqslant 0$ d'éléments de R^+, alors $\alpha \in R^+$; pour toute racine α, on a, soit $\alpha \in R^+$, soit $\alpha \in -R^+$. Il s'ensuit (Bible, 14-07) qu'il existe un groupe de Borel $B \supset T$ tel que la relation $P_\alpha \subset B$ implique $\alpha \in R^+$; comme B est engendré par T et les P_α qu'il contient (Bible, 13-05) on voit que $B \subset H$, donc H est bien un sous-groupe parabolique. Il reste à voir que $H \neq G$.

Notons d'abord que R^{++} est non vide ; sinon, toute racine serait triviale sur S, de sorte que S centraliserait T et tous les P_α, lesquels engendrent G ; S serait donc dans le centre de G, ce qui est contraire à l'hypothèse. Soit alors U le sous-groupe fermé de G engendré par les P_α, $\alpha \in R^{++}$; pour montrer que $H \neq G$, il suffit d'établir que H normalise U et que U est unipotent (car si l'on avait $H = G$, il s'ensuivrait que U est dans le radical unipotent de G, ce qui est impossible car $\dim(U) \geqslant 1$).

Pour montrer que H normalise U, il suffit de faire voir que P_β normalise U pour toute $\beta \in R^+$; on va le faire en plusieurs étapes. (Naturellement ce point est trivial en caractéristique 0 vu la théorie des algèbres de Lie ...). On peut évidemment supposer $\beta \in R^0$, sinon il n'y a rien à démontrer.

LEMME 9. - Pour toute $\beta \in R^0$ il y a un sous-groupe de Borel B de H qui contient T, P_β et U.

Soient $\alpha_1, \ldots, \alpha_r$ les racines dans R^{++}, écrites dans un ordre arbitraire, et soit A l'ensemble des racines $\gamma \in R_G$ qui peuvent s'écrire sous la forme

$$\gamma = \Sigma m_i \alpha_i + n\beta$$

avec des coefficients rationnels m_i, $n \geqslant 0$. Evidemment $A \subset R^+$, et pour une racine γ donnée par la formule ci-dessus on a

$$n(\gamma) = \Sigma m_i . n(\alpha_i) \quad ;$$

si donc A contient γ et $-\gamma$, on aura $m_i = 0$ pour tout i, donc $\gamma = n\beta$ avec $n \geqslant 0$ (parce que $\gamma \in A$) et $n \leqslant 0$ (parce que $-\gamma \in A$) ; autrement dit, $A \cap -A$ est vide. Il s'ensuit qu'on peut introduire sur R_G une relation d'ordre total telle que toute $\gamma \in A$ soit > 0 ; mais comme les α positives pour une telle relation d'ordre correspondent à un groupe de Borel B contenant T, il y a donc un B qui contient T et les P_γ, $\gamma \in A$, donc T, U et P_β.

([3]) Le corps k ne joue plus aucun rôle dans la suite de la démonstration : on raisonne sur Ω.

Ceci fait, soit B un groupe de Borel de G contenant T, U et P_β et considérons le sous-groupe $B \cap H$; il contient encore T, U et P_β, est résoluble (comme sous-groupe de B) et contenu dans H ; il est donc contenu dans un sous-groupe de Borel de H, donc de G, ce qui permet de supposer $B \subset H$, et le lemme est démontré.

Nous pouvons maintenant montrer que <u>pour toute racine</u> $\beta \in R^0$, P_β <u>normalise</u> U. Considérons un groupe de Borel $B \subset H$ contenant T, U et P_β, et soit R_B^+ l'ensemble des racines $\gamma \in R^+$ telles que $P_\gamma \subset B$; ("on" conjecture que $R_B^+ = R_B$, ensemble des γ telles que $P_\gamma \subset B$; plus généralement, on peut conjecturer - et démontrer trivialement en caractéristique 0 - que H ne contient pas d'autres racines que celles qui sont dans R^+) ; comme toute racine qui est combinaison linéaire à coefficients positifs de racines appartenant à B (resp. à H) est encore dans B (resp. H), il est clair que toute racine qui est combinaison linéaire à coefficients positifs de racines dans R_B^+ est encore dans R_B^+ ; donc (<u>Bible</u>, 17-03), si l'on désigne les éléments de R_B^+ par $\alpha_1, \dots, \alpha_r$ (ce sont les éléments de R^{++}), $\beta_1, \dots, \beta_s$ le produit

$$B_u^+ = P_{\alpha_1} \cdots P_{\alpha_r} P_{\beta_1} \cdots P_{\beta_s} = U \cdot P_{\beta_1} \cdots P_{\beta_s}$$

est un sous-groupe fermé de B^u ; de plus, en notant τ_γ un isomorphisme du groupe additif A sur le sous-groupe P_γ pour chaque racine γ, l'application $(A)^{r+s} \to B_u^+$ qui résulte de là est un isomorphisme de variétés sur Ω.

On peut donc pour tout $x \in B_u^+$ écrire

$$x = \Pi\, \tau_{\alpha_i}(\varphi_i(x)) \cdot \Pi\, \tau_{\beta_j}(\psi_j(x))$$

où les φ_i, ψ_j définissent un isomorphisme de la variété B_u^+ sur la variété A^{r+s} ; les formules de multiplication dans B_u^+ sont alors polynomiales en les coordonnées φ_i, ψ_j ; en particulier, prenons un $u \in U$ (de sorte que $\psi_j(u) = 0$ pour tout j) et un $x \in B_u^+$; on aura alors des relations de la forme

$$\psi_j(xux^{-1}) = \Sigma\, c^j_{m,n,p}\, \Pi\, \varphi_i(u)^{m_i}\, \Pi\, \varphi_k(x)^{n_k}\, \Pi\, \psi_h(x)^{p_h}$$

avec des coefficients constants $c^j_{m,n,p} \in \Omega$; or on a évidemment

$$\varphi_i(txt^{-1}) = \alpha_i(t)\, \varphi_i(x), \qquad \psi_j(txt^{-1}) = \beta_j(t)\, \psi_j(x)$$

quels que soient $x \in B_u^+$, $t \in T$; on en déduit immédiatement que, dans la formule pour $\psi_j(xux^{-1})$, le coefficient $c^j_{m,n,p}$ ne peut être $\neq 0$ que si l'on a la relation

$$\beta_j = \sum (m_i + n_k)\, \alpha_k + \sum p_h\, \beta_h \qquad ;$$

comme $\beta_j | S = 0$ et comme $\alpha_k | S > 0$ il s'ensuit que $m_i = n_k = 0$, autrement dit que $\psi_j(xux^{-1})$ est indépendant de u, donc $(u = e)$ est nul, et ceci montre que $xux^{-1} \in U$, donc que U est invariant dans B_u^+, et en particulier est normalisé par P_β. Ceci termine la démonstration.

6. Sous-groupes paraboliques en caractéristique 0.

Le résultat qui suit est dû à A. BOREL.

THÉORÈME 9 (k de caractéristique 0). - Soit G un groupe linéaire réductif connexe défini sur k. Les propriétés suivantes sont équivalentes :

(a) G possède un sous-groupe parabolique $H \neq G$;

(b) G contient un tore S défini et décomposé sur k et non contenu dans le centre de G ;

(c) G contient un élément unipotent $u \neq e$ rationnel sur k. S'il en est ainsi, soit U un sous-groupe fermé, unipotent, défini sur k, et maximal, de G ; alors N(U) est un sous-groupe parabolique minimal de G.

On sait déjà que (a) $\Longleftrightarrow$ (b) ; l'implication (a) $\Longrightarrow$ (c) est triviale (sur un corps de base k parfait) vu le corollaire du lemme 4.

Montrons maintenant que (c) $\Longrightarrow$ (b). Considérons dans G_k un élément unipotent $u \neq e$; celui-ci engendre dans G un sous-groupe fermé, connexe, unipotent, et de dimension 1 (Bible, 4-09), et ce sous-groupe U est évidemment défini sur k. Nous allons d'abord établir que le normalisateur connexe $N_o(U)$ contient un tore $S \neq e$. S'il n'en était pas ainsi, $N_o(U)$ serait nilpotent (Bible, 6-11) et unipotent, et de plus centraliserait U : car l'automorphisme $u \to nun^{-1}$ s'écrit, en identifiant U au groupe additif A, sous la forme $t \to \chi(n)t$, où χ est un caractère de $N_o(U)$, nécessairement trivial si $N_o(U)$ ne contient aucun tore.

Il faut donc prouver que $N_o(U) \neq Z_o(U)$. Soit C la composante connexe du centre de G, de sorte que G/C est semi-simple ; C est contenu dans $N_o(U)$ et $Z_o(U)$; soit U' l'image de U dans G' = G/C ; montrons que $N_o(U)$ et $Z_o(U)$ sont les images réciproques de $N_o(U')$ et $Z_o(U')$; en effet celles-ci consistent des $g \in G$ tels que, pour tout $u \in U$, on ait $gug^{-1} \in U.C$ (resp. $gug^{-1} = uz$ avec $z \in C$) ;

mais si $gug^{-1} = vz$ (resp. $gug^{-1} = uz$) alors, comme z commute à v (resp. u) qui est unipotent, et comme z est semi-simple, z est la partie semi-simple de gug^{-1} , qui est unipotent, donc $z = e$, ce qui prouve notre assertion.

Pour montrer que $N_o(U) \neq Z_o(U)$ on peut donc supposer G semi-simple. Soit alors $\mathfrak{g}$ l'algèbre de Lie de G , et soit $X \in \mathfrak{g}$ un générateur de U . Il suffit évidemment de prouver que $X \in Ad(X)\mathfrak{g}$; or la forme de Killing $\langle\ ,\ \rangle$ de $\mathfrak{g}$ est non dégénérée, donc tout revient à montrer que tout $Y \in \mathfrak{g}$ orthogonal à $Ad(X)\mathfrak{g}$ est orthogonal à X ; or la relation $\langle Y\ ,\ Ad(X)Z\rangle = -\langle Ad(X)Y\ ,\ Z\rangle$ montre que ces Y commutent à X ; on a de plus $\langle Y\ ,\ X\rangle = Tr(Ad(Y)Ad(X))$; mais $Ad(X)$ est nilpotent, donc $Ad(Y)Ad(X)$ l'est aussi, et le résultat annoncé s'ensuit.

Nous pouvons maintenant démontrer que (a) $\Longrightarrow$ (b). Soit toujours U un sous-groupe unipotent de G , défini sur k et de dimension 1 . Ce qu'on vient d'établir prouve que $N_o(U)$ possède un caractère χ non trivial, trivial sur le centre de G et défini sur k . Soit S un tore maximal défini sur k de $N_o(U)$; la restriction de χ à S est non triviale (cela prouvera (c) modulo le lemme 8) ; en effet supposons χ trivial sur S ; comme tout groupe de Borel B de $N_o(U)$ contenant S est produit semi-direct de S et de sa partie unipotente, χ est trivial sur B ; mais ces B engendrent $N_o(U)$ (Bible, 12-07), donc χ est trivial sur $N_o(U)$, ce qui est absurde, et montre que (c) $\Longrightarrow$ (b).

Soient U un sous-groupe fermé unipotent de G défini sur k et maximal, et H un sous-groupe parabolique minimal de G . Pour montrer que $N(U)$ est un sous-groupe parabolique minimal, on peut supposer $U \subset H$ et montrer qu'alors $N(U) = H$ (cf. corollaire 1 du théorème 7). Soit R le radical de H ; comme R^u est unipotent, défini sur k , et normalisé par U , le sous-groupe $U.R^u$ est encore unipotent et défini sur k ; comme U est maximal on a donc $U \supset R^u$. Soit U' l'image de U dans $H' = H/R^u$; l'image réciproque dans H d'un sous-groupe parabolique de H' est évidemment un sous-groupe parabolique de H , donc de G (car un sous-groupe de Borel de H est aussi un sous-groupe de Borel de G) ; comme H est minimal, on voit que H' n'a aucun sous-groupe parabolique autre que H' lui-même ; comme on a déjà prouvé que (c) $\Longrightarrow$ (a), H' ne contient aucun sous-groupe unipotent défini sur k , donc $U' = e$. Ceci montre que $U' = R^u$, et comme $H = N(R^u)$ d'après le théorème 7, on a $H = N(U)$ comme annoncé. Ceci termine la démonstration du théorème 9.

Remarque sur le cas d'un corps k parfait infini. - Si l'on savait démontrer dans ce cas que (c) $\Longrightarrow$ (a), la fin de la démonstration précédente s'appliquerait évidemment. Donc pour étendre le théorème 9 au cas d'un corps de base k parfait

infini il suffit de démontrer que (c) implique (b). Or si G contient un sous-groupe unipotent U défini sur k et non trivial, alors (théorème 5) on peut supposer dim(U) = 1 ; et le raisonnement utilisé pour démontrer en caractéristique 0 que (c) $\Longrightarrow$ (b) montre que, dans le cas étudié ici, tout revient à faire voir que

$$N_o(U) \neq Z_o(U) \quad .$$

Il serait scandaleux que ce résultat (sic) fût faux ; mais on ne saurait exclure cette éventualité, attendu que la théorie des racines, en caractéristique p , présente certains aspects pathologiques (par exemple : il peut arriver que $\alpha + \beta$ soit racine et que néammoins P_α et P_β commutent).

BIBLIOGRAPHIE

[1] LANG (Serge). - Introduction to algebraic geometry. - New York, Interscience Publishers, 1958.

[2] ROSENLICHT (Maxwell). - Some rationality questions on algebraic groups, Annali di Mat., t. 43, 1957, p. 25-50.

[3] Séminaire CHEVALLEY. - Classification des groupes de Lie algébrique, t. 1 et 2, 1956-1958. - Paris, Secrétariat mathématique, 1958.

[4] SERRE (Jean-Pierre). - Groupes algébriques et théorie des corps de classe. - Paris, Hermann, 1958 (Act. scient. et ind., 1264; Publ. Inst. Math. Univ. Nancago, 7).

[5] WEIL (André). - On algebraic groups of transformations, Amer. J. of Math., t. 77, 1955, p. 355-391.

[6] WEIL (André). - On algebraic groups and homogeneous spaces, Amer. J. of Math., t. 77, 1955, p. 492-512.

[7] WEIL (André). - Adeles and algebraic groups. - Princeton, Institute for Advanced Study, 1960 (multigraphié).