Classification of all connected subgroup schemes of a reductive group containing a split maximal torus

Ekaterina Sopkina
Department of Mathematics and Mechanics
St. Petersburg University
and
Fakultät für Mathematik
Universität Bielefeld
E-mail: sopkina@yandex.ru

26th March 2006

Abstract. The main result of the paper is a classification of all connected subgroup schemes of a reductive group that contain a split maximal torus, over an arbitrary field. The classification is expressed in terms of functions on the root system.

2000 Mathematical Subject Classifications: 20G15, 20G35, 14L15.

Keywords: reductive groups, non-reduced affine group schemes.

§ 1 Introduction

In the paper we completely describe connected subgroup schemes of a reductive group that contain a split maximal torus over an arbitrary field. This description is stated in purely combinatorial terms and depends only on the corresponding root system. This is a decisive step towards a description of **all** (not necessarily connected) subgroup schemes containing a torus. We intend to return to this problem in a subsequent paper.

The main theorem is a broad generalization of classical results describing algebraic subgroups of a split reductive group (see A. Borel's and J. Tits's paper [1] and Séminaire de Géométrie Algébrique [5]). In context of our problem, algebraic subgroups correspond to reduced subgroup schemes. We briefly recall the results on algebraic subgroups in Section § 5.

These results were generalized to groups over some classes of rings, including semi-local ones, by Z. Borewicz, N. Vavilov, and others. On the other hand, over a finite field G. Seitz described overgroups of all not necessarily split maximal tori. Surveys of research in these directions and further references can be found in the papers [9, 10].

In the present paper we generalize in a different direction. Namely, we include not necessarily reduced subgroup schemes. Recall that by Cartier's theorem (see, for example, [12] 11.4) any affine group scheme over a field of characteristic zero is reduced. But in positive characteristic, subgroup schemes of a reductive group are not exhausted by reduced ones.

Non-reduced subgroup schemes of reductive groups were considered, in particular, by C. Wenzel (see [13, 14]) and F. Knop (see [4]). Namely, in the special case of parabolic subgroup schemes, an analogous problem was addressed by Ch.Wenzel. He gave a complete description of parabolic subschemes under some mild restriction on characteristic. Futhermore, F. Knop for [4] described all subgroup schemes of SL_2. One of our initial motivations was exactly to generalize these results.

In the preceding paper [6] we classified all (not necessarily reduced) overgroup schemes of a maximal torus in GL_n. The result of the present paper generalizes simultaneously the classical result on reduced subgroup schemes, the result by Ch. Wenzel on parabolic schemes, and the above result for GL_n. In the proof we develop the approach applied to the case of GL_n in [6]. The proof uses standard technics and tools from algebraic geometry: reduction to an algebraically closed field, Frobenius morphism, functorial properties. But the most difficult step, Main Lemma 16, concerns groups over rings and involves ideas from the works by Z. Borewicz and N. Vavilov [2], [8].

The rest of the article is organized as follows. In Section 2, we fix notation and recall some results on the structure of reductive groups. In Section 3, we formulate the main theorem. In Section 4, we discuss the concept of quasi-closed sets. Section 5 contains a review of the description of connected intermediate algebraic subgroups in a reductive group. In Section 6, we discuss a Frobenius morphism. In Section 7, we specialize and start proving Theorem 1, namely, we construct all connected intermediate group schemes. In Section 8, we reduce Theorem 1 to the case of an algebraically closed field. In Section 9, we consider the reduced subscheme of an intermediate group scheme. Finally, in Section 10, we prove Main Lemma on intermediate subgroups in the group of R-points of a reductive group and complete the proof of Theorem 1.

Acknowledgements

This research was partially supported by INTAS 04-83-3000 Young Scientist Fellowship, INTAS 03-51-3251, DAAD-program "Michail Lomonosov", and INTAS 00-566.

It is a special plesure for me to thank Prof. N. Vavilov and Prof. A. Bak for their attention to the work and support in the preparing of this article.

§ 2 Preliminaries

In this section we fix notation and recall necessary results concerning reductive groups. We follow the books [3], [7], and [5] Exp. XXII.

Let G be a reductive group containing a split maximal torus T over a field K. Let $(X, \Phi, X\check{}, \Phi\check{})$ be the root data of (G, T). In particular, X is the character group of T, $X\check{}$ is the cocharacter group of T, i.e. the group of all homomorphisms from G_m to T, and the groups X and $X\check{}$ are in duality by a pairing $\langle\ ,\ \rangle : X \times X\check{} \to \mathbb{Z}$. For any root $\beta \in \Phi$, any K-algebra R, and any element $t \in T(R)$ we have by definition

$$(-\beta)(t) = \beta(t)^{-1}.$$

Consider an adjoint representation of G on its Lie algebra L. The T-module L admits a decomposition

$$L = L_0 \oplus (\bigoplus_{\beta\in\Phi} L_\beta)$$

Each root subspace L_β has dimension 1.

For each root $\beta \in \Phi$ there is a homomorphism $x_\beta : G_a \to G$ such that the corresponding tangent map induces an isomorphism of the Lie algebra of G_a onto L_β. Any element t of the torus $T(R)$ acts on the root subgroup corresponding to a root β by

$$tx_\beta(a)t^{-1} = x_\beta(\beta(t)a).$$

In particular, for $t = \lambda(\varepsilon)$, where λ is a cocharacter and ε is an invertible element of R, we have

$$\lambda(\varepsilon)x_\beta(a)\lambda(\varepsilon)^{-1} = x_\beta(\varepsilon^{\langle\beta,\lambda\rangle}a).$$

Such a root homomorphism is unique up to multiplication by an element of K^*. For each root β we fix a homomorphism x_β that comes from a homomorphism over $\mathbb{Z}$.

Fix a Weyl basis $\{e_\beta, \beta \in \Phi, h_\lambda, 1 \le \lambda \le \dim T\}$ in L, where $\{e_\beta, \beta \in \Phi\}$ is a Chevalley system in L. Then the adjoint action of a root subgroup $x_\alpha(G_a)$ on a basis element e_β with $\beta \neq -\alpha$ is given by

$$\mathrm{Ad}(x_\alpha(a))e_\beta = e_\beta + \sum_{r>0} M_{\alpha\beta r}a^r e_{r\alpha+\beta},$$

where $M_{\alpha\beta r}$ are integral coefficients.

For root subgroups corresponding to roots α and β with $\beta \neq -\alpha$, we have the Chevalley commutator formula

$$[x_\alpha(a), x_\beta(b)] = \prod_{r,s>0} x_{r\alpha+s\beta}(N_{\alpha\beta rs}a^r b^s),$$

where $N_{\alpha\beta rs}$ are integral coefficients. We take the values of $M_{\alpha\beta r}$ and $N_{\alpha\beta rs}$ from the paper [11].

In case of $\beta = -\alpha$, but one of a and b is nilpotent, we use the formula

$$x_\alpha(a)x_{-\alpha}(b) = x_{-\alpha}(\frac{b}{1+ab})\alpha\check{}(1+ab)x_\alpha(\frac{a}{1+ab})$$

(see [5] Exp.XX 2.1).

Fix an arbitrary ordering on Φ that is compatible with root heights, i.e. if $ht(\alpha) < ht(\beta)$, then α goes before β. When we consider a product like $\prod_{\beta\in\Phi}$, we take the factors in this order.

§ 3 Statement of main results

In this section we formulate a main result of the paper.

Let K be a field of characteristic $p > 0$. Let Φ be a root system, $G(\Phi)$ be a reductive group of type Φ over the field K, T be a split maximal torus in $G(\Phi)$.

Theorem 1. *There is a one-to-one correspondence between all* **connected** *subgroup schemes of $G(\Phi)$ that contain T, and all functions $\varphi : \Phi \to \mathbb{N} \cup \{0, \infty\}$ satisfying*

$$\varphi(r\alpha + s\beta) \geq \min(\varphi(\alpha) - \log_p r, \varphi(\beta) - \log_p s) \qquad (*)$$

for any roots α, β, $r\alpha + s\beta \in \Phi$ such that $p \not| N_{\alpha\beta rs}$.

Remark. Suppose that the following restriction on characteristic holds:

- if $\Phi \supseteq B_2$, then $p > 2$;
- if $\Phi \supseteq G_2$, then $p > 3$.

Then $p \not| N_{\alpha\beta 11}$ for any two roots α and β such that $\alpha + \beta$ is a root. So in this case the condition $(*)$ is equivalent to the following one:

$$\varphi(\alpha + \beta) \geq \min(\varphi(\alpha), \varphi(\beta))$$

for any roots α, $\beta \in \Phi$ such that $\alpha + \beta \in \Phi$.

Examples. 1. A function φ satisfying $(*)$ corresponds to a reduced subgroup scheme if and only if all values of φ are zero and infinity. In the notation of Section § 5, the function φ corresponds to the scheme $G(S)$, where S is a quasi-closed set, if and only if

$$\varphi(\beta) = \begin{cases} \infty, & \text{if } \beta \in S; \\ 0, & \text{otherwise.} \end{cases}$$

2. The product of the torus T and the kernel E_N of the N-th power of a Frobenius morphism is a non-reduced connected subgroup scheme. All values of the corresponding function are equal to N.

3. Suppose that $\Phi = A_{n-1}$, $G = \mathrm{GL_n}$, and T is the group of diagonal matrices. $\mathrm{GL_n}$ is represented by $K[\mathrm{GL_n}] = K[x_{11}, \ldots, x_{nn}, t]/(t\det(x_{ij}) = 1)$. In this case the subscheme corresponding to a function $\varphi : A_{n-1} \to \mathbb{N} \cup \{0, \infty\}$ is represented by $K[\mathrm{GL_n}]/(x_{ij}^{p^{\varphi(ij)}} = 0)$, where $\varphi(ij) = \varphi(e_i - e_j)$. See [6] for details.

§ 4 Quasi-closed sets of roots

In this section we introduce and discuss a notion of quasi-closed sets of roots, and an equivalent definition of the property $(*)$. The notion of quasi-closed set is taken from the paper [1] by A. Borel and J. Tits, but the definition we use is distinct from the initial one.

Definition. Let S be a subset of a root system Φ. Suppose that for any two roots α and β in S and positive integers r and s such that $r\alpha + s\beta$ is a root and $p \not| N_{\alpha\beta rs}$, the root $r\alpha + s\beta$ lies in S. Then the subset S is called *quasi-closed*.

Remark. Any closed set of roots is quasi-closed. Conversely, any quasi-closed set is closed under the restriction

- if $\Phi \supseteq B_2$, then $p > 2$;
- if $\Phi \supseteq G_2$, then $p > 3$.

Lemma 2. *Let Φ be a root system, p be a prime number.*

1. The condition $(*)$ is equivalent to the following one:

$$\varphi(r\alpha + \beta) \geq \min(\varphi(\alpha) - \log_p r, \varphi(\beta)) \tag{$**$}$$

for any roots α, β, $r\alpha + \beta \in \Phi$ such that $p \not| M_{\alpha\beta r}$.

2. A set S is quasi-closed if and only if the following condition holds: for any two roots α and β in S and positive integer r such that $r\alpha + \beta$ is a root and $p \not| M_{\alpha\beta r}$, the root $r\alpha + \beta$ lies in S.

Proof. 1. If $s = 1$, then $N_{\alpha\beta rs} = M_{\alpha\beta r}$ and the conditions $(*)$ and $(**)$ are the same. The case $r = 1$ is similar. The only case, when $r, s > 1$ and $r\alpha+s\beta$ is a root, is as follows: α and β are simple roots of G_2, $r = 2$, and $s = 3$ (or, symmetrically, $r = 3$ and $s = 2$). In this case we have $N_{\alpha\beta 31} = 1$ and $N_{3\alpha+\beta,\beta 11} = 1$ (see [11]), so

$$\begin{aligned}\varphi(3\alpha + 2\beta) &\geq \min(\varphi(3\alpha + \beta), \varphi(\beta)) \geq \min(\varphi(\alpha) - \log_p 3, \varphi(\beta)) \\ &\geq \min(\varphi(\alpha) - \log_p 3, \varphi(\beta) - \log_p 2).\end{aligned}$$

2. The condition holds if and only if the function φ_S satisfies $(**)$, where

$$\varphi_S(\beta) = \begin{cases} \infty, & \text{if } \beta \in S; \\ 0, & \text{otherwise.} \end{cases}$$

The set S is quasi-closed if and only if the function φ_S satisfies $(*)$. Apply the first assertion of the lemma to the function φ_S. □

§ 5 Connected smooth subgroup schemes containing a torus

This section is based on [5] Exp. XXII. In this section we consider connected smooth subgroup schemes containing a torus and show that they correspond to quasi-closed subsets of roots.

Definition.([5] Exp. XXII 5.2.1) Let X be a prescheme, G be a smooth finitely represented group X-prescheme with connected fibres, H be a subgroup prescheme of G. We say that H is *of type* (R) if the following conditions hold:

1. H is smooth finitely represented X-prescheme with connected fibres;
2. for any $x \in X$, $H_{\bar{x}}$ contains a Cartan subgroup of $G_{\bar{x}}$.

Assume now that $G = G(\Phi)$ is a split reductive group over a field. In this case any connected subgroup scheme containing a maximal torus T is of type (R) if and only if the scheme is smooth. By [5] Exp. XXII 5.4.1, any subgroup scheme of type (R) containing T is uniquely determined by its Lie algebra, which has a form

$$L_S = L_0 \oplus \big(\bigoplus_{\beta \in S} L_\beta\big)$$

for some subset S of Φ.

Definition.([5] Exp. XXII 5.4.2) A subset S of Φ is called a set *of type* (R) if L_S is the Lie algebra of a subgroup scheme of type (R) containing T.

By $G(S)$ denote the subgroup scheme of type (R) uniquely determined by the set S.

Lemma 3.

$$x_\beta(G_a)\cap G(S)=\begin{cases} x_\beta(G_a), & \text{if } \beta\in S;\\ 1, & \text{otherwise.}\end{cases}$$

Proof. See [5] Exp. XXII 5.4.3. □

Lemma 4. *Any quasi-closed set is of type (R). And conversely, any set of type (R) is quasi-closed.*

Proof. We show first that any set of type (R) is quasi-closed. By Lemma 2 it is enough to check that for any two roots α and β in S and positive integer r such that $r\alpha+\beta$ is a root and $p\nmid M_{\alpha\beta r}$, the root $r\alpha+\beta$ lies in S.

Since $\alpha\in S$ and $\beta\in S$, we have $e_\beta\in L_S$ and $x_\alpha(G_a)\subseteq G(S)$ by Lemma 3. Therefore the element $\mathrm{Ad}(x_\alpha(a))e_\beta=e_\beta+\sum_{r>0}M_{\alpha\beta r}a^r e_{r\alpha+\beta}$ lies in L_S for any a. Since $L_S=L_0\oplus(\bigoplus_{\beta\in S}L_\beta)$ and $p\nmid M_{\alpha\beta r}$, we conclude $L_{r\alpha+\beta}\subseteq L_S$, and therefore the root $r\alpha+\beta$ lies in S.

Now we need to prove the converse. The assertion that any closed set is of type (R) is established in Theorem [5] Exp. XXII 5.4.7. In fact, the proof of this theorem uses only properties of quasi-closed sets and is therefore a valid proof for our assertion. □

The above lemmas imply the following corrolary.

Corollary 5. *The correspondence $S\mapsto G(S)$ gives a bijection between all quasi-closed subsets of Φ and all connected smooth subgroup schemes containing the torus T in $G(\Phi)$.*

§ 6 Frobenius morphism

In this section we discuss a Frobenius morphism and introduce a scheme E_N.

Let G be an affine scheme over a perfect field K. Consider a Frobenius morphism $F: G\to F(G)$ corresponding to the natural embedding

$$K[F(G)]=K[G]^p\hookrightarrow K[G].$$

Lemma 6. *Let H and H' be closed subschemes of any algebraic affine scheme G over a perfect field K. If the subschemes $F^N(H)$ and $F^N(H')$ of $F^N(G)$ coincide, then the schemes H_{red} and H'_{red} coincide.*

Proof. Let the scheme G be represented by $K[G]$, and let the subschemes H and H' be represented by $K[G]/I$ and $K[G]/I'$ for some ideals I and I' respectively. Then the subscheme $F^N(H)$ (respectively $F^N(H')$) is represented by the algebra $(K[G]/I)^{p^N}=K[G]^{p^N}/(K[G]^{p^N}\cap I)$ (respectively $K[G]^{p^N}/(K[G]^{p^N}\cap I')$). Since the subscheme $F^N(H)$ equals to the subscheme $F^N(H')$, the corresponding ideals $K[G]^{p^N} \cap I$ and $K[G]^{p^N} \cap I'$ coincide. So we get $\sqrt[p^N]{I} = \sqrt[p^N]{I'}$, and therefore the ideals $\sqrt{I}$ and $\sqrt{I'}$ coincide. Thus we conclude

$$K[H_{\mathrm{red}}] = K[G]/\sqrt{I} = K[G]/\sqrt{I'} = K[H'_{\mathrm{red}}]$$

and $H_{\mathrm{red}} = H'_{\mathrm{red}}$. □

Let $F^N : G(\Phi) \to F^N(G(\Phi))$ be the N-th power of a Frobenius morphism. Denote the kernel of F^N by E_N.

Lemma 7. $E_N = T_N \prod_{\beta \in \Phi} x_\beta(\alpha_{p^N})$,
where $T_N = \mathrm{Ker}(F^N) \cap T$, *and this product is direct.*

Proof. See [3], II.3.2. □

Lemma 8. $G(S) \cap E_N = T_N \prod_{\beta \in S} x_\beta(\alpha_{p^N})$,
where $T_N = \mathrm{Ker}(F^N) \cap T$, *and this product is direct.*

Proof. Since the group schemes $G(S)$ and E_N contain T_N and $x_\beta(\alpha_{p^N})$ for each $\beta \in S$, the intersection $G(S) \cap E_N$ contains the right-hand member of the equality. So it is enough to prove the other inclusion.

By Lemma 7, for any K-algebra R and any element $g \in G(S,R) \cap E_N(R)$ there is an *fppf* R-algebra R' such that $g = t \prod_{\beta \in \Phi} x_\beta(a_\beta)$, where $t \in T_N(R')$ and $a_\beta \in R'$ with $a_\beta^{p^N} = 0$. Since t lies in $G(S,R') \cap E_N(R')$, the intersection $G(S,R') \cap E_N(R')$ contains the product $\prod_{\beta \in \Phi} x_\beta(a_\beta)$.

Note that $G(S,R') \cap E_N(R')$ is a subgroup of $G(\Phi,R')$ and contains $T(R)$. So we may apply Main Lemma 16, which is proven in Section § 10. Thus we get $x_\beta(a_\beta) \in G(S,R')$ for each $\beta \in \Phi$. Lemma 3 implies $a_\beta = 0$ for each $\beta \notin S$, and this completes the proof. □

§ 7 Construction of H_φ

In this section we construct a subgroup scheme H_φ corresponding to a function φ that satisfies the inequality $(*)$.

For a given function $\varphi : \Phi \to \mathbb{N} \cup \{0, \infty\}$ define a subset

$$S = \{\beta \in \Phi \mid \varphi(\beta) = \infty\}$$

of Φ. If the function φ satisfies the condition $(*)$, then the set S is quasi-closed by definition. Fix any positive integer N such that $N > \max\{\varphi(\beta) \mid \varphi(\beta) < \infty\}$.

Assume at first that the field K is perfect. Set $\psi(\beta) = \min(\varphi(\beta), N)$. Obviously if φ satisfies the condition $(*)$ then ψ satisfies too. Consider a subscheme $E_{\varphi,N} = T_N \prod_{\beta \in \Phi} x_\beta(\alpha_{p^{\psi(\beta)}})$ of E_N.

Lemma 9. *If* φ *satisfies* $(*)$, *then* $E_{\varphi,N}$ *is a subgroup scheme.*

Proof. To prove this lemma it is enough to check that for any k-algebra R the set $E_{\varphi,N}(R)$ is a subgroup of $G(\Phi, R)$. Obviously $E_{\varphi,N}(R)$ contains a unit, and for any $t \in T_N(R)$ we have $t^{-1} \in T_N(R)$, and $x_\beta(a)^{-1} = x_\beta(-a)$. So it is enough to show that an arbitrary product of elements of $T_N(R)$ and $x_\beta(\alpha_{p^{\psi(\beta)}}(R))$ can be written in the form $t\prod_{\beta\in\Phi} x_\beta(a_\beta)$, where $t \in T_N(R)$ and each $a_\beta^{p^{\psi(\beta)}} = 0$.

Consider an element h of $G(\Phi, R)$, which is equal to a product of elements $t_i \in T_N(R)$ and $x_\beta(a_{\beta,j})$ with $a_{\beta,j}^{p^{\psi(\beta)}} = 0$ in some order. Let I be the ideal of R generated by all $a_{\beta,j}$. The ideal I is finitely generated and is contained in the nilradical $\mathrm{Nil}(R)$, so we have $I^M = 0$ for some positive integer M. We prove that h modulo I^r can be written in the required form, by induction. Obviously the case $r = M$ completes the proof.

If r is equal to 1, this is trivial, because $a_{\beta,j} \in I$. Now we prove that the case r imlies the result for $r + 1$.

First of all we note that we anytime can permute any element t_i with any element of $x_\beta(a_{\beta,j})$, because $x_\beta(a_{\beta,j})t_i = t_i x_\beta(\beta(t_i^{-1})a_{\beta,j})$.

Suppose that h is equal to a product of t_i and $x_\beta(a_{\beta,j})$ with the following property: if we omit the factors $x_\beta(a_{\beta,j})$ with $a_{\beta,j} \in I^r$, then we get a product like $t\prod_{\beta\in\Phi} x_\beta(a_\beta)$. Consider an omitted factor $x_\alpha(a'_\alpha)$ with $a'_\alpha \in I^r\backslash I^{r+1}$. We can permute it with t, with $x_\beta(a_{\beta,j})$, where $\beta \neq \pm\alpha$, and with $x_{-\alpha}(a_{-\alpha,j})$, as follows.

When we permute $x_\alpha(a'_\alpha)$ and t, we use the formula

$$x_\alpha(a'_\alpha)t = tx_\alpha(\alpha(t^{-1})a'_\alpha).$$

When we permute $x_\alpha(a'_\alpha)$ and $x_\beta(a_{\beta,j})$, where $\beta \neq \pm\alpha$, we use the Chevalley commutator formula

$$x_\alpha(a'_\alpha)x_\beta(a_{\beta,j}) = x_\beta(a_{\beta,j})x_\alpha(a'_\alpha)\prod_{r,s>0} x_{r\alpha+s\beta}(N_{\alpha\beta rs}{a'_\alpha}^r a_{\beta,j}^s).$$

By the inequality $(*)$, we have $(N_{\alpha\beta rs}{a'_\alpha}^r a_{\beta,j}^s)^{p^{\psi(r\alpha+s\beta)}} = 0$. So each new factor $x_\gamma(a'_\gamma)$ satisfies ${a'_\gamma}^{p^{\psi(\gamma)}} = 0$ and $a'_\gamma \in I^{r+1}$.

When we permute $x_\alpha(a'_\alpha)$ and $x_{-\alpha}(a_{-\alpha,j})$, we use the formula

$$x_\alpha(a'_\alpha)x_{-\alpha}(a_{-\alpha,j}) = x_{-\alpha}(\frac{a_{-\alpha,j}}{1 + a'_\alpha a_{-\alpha,j}})\alpha\check{}(1 + a'_\alpha a_{-\alpha,j})x_\alpha(\frac{a'_\alpha}{1 + a'_\alpha a_{-\alpha,j}})$$

for a homomorphism $\alpha\check{} : G_m \to T$ (see [5] Exp.XX 2.1). Obviously we have $\alpha\check{}(1 + a'_\alpha a_{-\alpha,j}) \in T_N(R)$.

Using these permutations, we put $x_\alpha(a'_\alpha)$ near the factor $x_\alpha(a_\alpha)$ and eliminate the former by the formula

$$x_\alpha(a_\alpha)x_\alpha(a'_\alpha) = x_\alpha(a_\alpha + a'_\alpha).$$

Proceeding this process for each omitted factor $x_\alpha(a'_\alpha)$ with $a'_\alpha \in I^r\backslash I^{r+1}$, we get a required product modulo I^{r+1}. □

Lemma 10. *$G(S)$ normalizes $E_{\varphi,N}$.*

Proof. Let us show that conjugation by $G(S)$ leaves T_N inside $E_{\varphi,N}$. In particular, then conjugation by $x_\gamma(G_a)$ leaves T_N inside $E_{\varphi,N}$ for any $\gamma \in S$. Since $G(S)$ contains T and since E_N is a normal subgoup scheme of $G(\Phi)$, we have the inclusion

$$T_N^{G(S)} = (T \cap E_N)^{G(S)} \subseteq G(S) \cap E_N.$$

Using Lemma 8, we conclude

$$T_N^{G(S)} \subseteq T_N \prod_{\beta \in S} x_\beta(\alpha_{p^N}) \subseteq E_{\varphi,N}.$$

Let us show that the commutator of subgroup schemes $x_\beta(\alpha_{p^{\psi(\beta)}})$ and $x_\gamma(G_a)$ with $\gamma \in S$ lies inside $E_{\varphi,N}$. Suppose that $\gamma \neq -\beta$. Then by the Chevalley commutator formula we have

$$[x_\beta(\alpha_{p^{\psi(\beta)}}), x_\gamma(G_a)] \subseteq \prod_{r,s>0} x_{r\beta+s\gamma}(N_{\beta\gamma rs}(\alpha_{p^{\psi(\beta)}})^r).$$

By the inequality $(**)$, if $p \not| N_{\beta\gamma rs}$, then

$$\begin{aligned}\varphi(r\beta + s\gamma) &\geq \min(\varphi(\beta) - \log_p r, \varphi(\gamma) - \log_p s) \\ &= \min(\varphi(\beta) - \log_p r, \infty) = \varphi(\beta) - \log_p r,\end{aligned}$$

and therefore $\psi(r\beta + s\gamma) \geq \psi(\beta) - \log_p r$. So we have the inclusion

$$N_{\beta\gamma rs}(\alpha_{p^{\psi(\beta)}})^r \subseteq \alpha_{p^{\psi(r\beta+s\gamma)}},$$

and therefore the following inclusion holds:

$$[x_\beta(\alpha_{p^{\psi(\beta)}}), x_\gamma(G_a)] \subseteq T_N \prod_{\beta \in \Phi} x_\beta(\alpha_{p^{\psi(\beta)}}) \subseteq E_{\varphi,N}.$$

Now suppose that $\gamma = -\beta$. Then by the commutation formula

$$\begin{aligned}[x_\beta(a), x_{-\beta}(b)] &= x_\beta(a)x_{-\beta}(b)x_\beta(-a)x_{-\beta}(-b) \\ &= x_\beta(a)x_\beta(-\frac{a}{1-ab})\beta\check{}(1-ab)x_{-\beta}(\frac{b}{1-ab})x_{-\beta}(-b) \\ &= x_\beta(a\frac{-ab}{1-ab})\beta\check{}(1-ab)x_{-\beta}(b\frac{ab}{1-ab}),\end{aligned}$$

where a is nilpotent, we get the inclusion

$$[x_\beta(\alpha_{p^{\psi(\beta)}}), x_{-\beta}(G_a)] \subseteq x_\beta(\alpha_{p^{\psi(\beta)}}) \cdot T_N \cdot x_{-\beta}(\alpha_{p^N}) \subseteq E_{\varphi,N}.$$

Since $E_{\varphi,N}$ is a product of subgroups T_N and $x_\beta(\alpha_{p^{\psi(\beta)}})$, the above assertions imply that each root subgroup $x_\gamma(G_a)$ with $\gamma \in S$ normalizes $E_{\varphi,N}$. Obviously T also normalizes T_N and $x_\beta(\alpha_{p^{\psi(\beta)}})$, so T normalizes the whole $E_{\varphi,N}$.

Since $G(\Phi)$ is a group scheme over a field, the normalizer of the subgroup scheme $E_{\varphi,N}$ in $G(\Phi)$ is an affine subgroup scheme (see [5] Exp. VIII 6.7). The reduced subscheme of the normalizer is a closed subgroup of $G(\Phi)$ and contains T and $x_\gamma(G_a)$ with $\gamma \in S$. On the other hand, the product $T\prod_{\gamma\in S} x_\gamma(G_a)$ is an open dense set in $G(S)$ (see [5] Exp. XXII 5.4.4). Thus the whole $G(S)$ is contained in the normalizer, i.e. $G(S)$ normalizes $E_{\varphi,N}$. □

Define a scheme H_φ as a product $G(S)E_{\varphi,N}$. Since the scheme $G(S)$ normalizes $E_{\varphi,N}$ by Lemma 10, H_φ is a group scheme. Since H_φ is defined as a product of subgroup schemes, we can consider H_φ as a functor on k-algebras given by

$$\begin{aligned} H_\varphi(R) = \{g \in G(\Phi, R) \mid & \text{ there are an } \textit{fppf } R\text{-algebra } R' \text{ and elements} \\ & h \in G(S, R'), f \in E_{\varphi,N}(R') \text{ with } hf = g \text{ in } G(\Phi, R')\}. \end{aligned}$$

See [3], I.6.2 for details.

This construction is invariant under field extension, so we can define H_φ over any (not necessarily perfect) field K as usual by $K[(H_\varphi)_K] = K \otimes \mathbb{F}_p[(H_\varphi)_{\mathbb{F}_p}]$, since any field K of characteristic p is an extension of the perfect field $\mathbb{F}_p$. This new definition is compatible with the previous one.

Lemma 11. *The scheme H_φ does not depend on the choice of N and satisfies all the conditions of Theorem 1, i.e. it is a connected subgroup scheme of $G(\Phi)$ containing T. Moreover $(H_\varphi)_{\mathrm{red}} = G(S)$.*

Proof. Let us show that H_φ does not depend on the choice of N. Let N' be greater than N, $N > \max\{\varphi(\beta) \mid \varphi(\beta) = \infty\}$. Obviously $E_{\varphi,N'}$ contains $E_{\varphi,N}$, so we get the inclusion $G(S)E_{\varphi,N'} \supseteq G(S)E_{\varphi,N}$. On the other hand T_N is contained in $G(S)$, $x_\beta(\alpha_{p^{N'}})$ is contained in $G(S)$ for $\beta \in S$, and $x_\beta(\alpha_{p^{\varphi(\beta)}})$ is contained in $E_{\varphi,N}$ for $\beta \notin S$. Thus we get the inclusion

$$E_{\varphi,N'} = T_{N'} \prod_{\beta\in\Phi} x_\beta(\alpha_{p^{\min(\varphi(\beta),N')}}) \subseteq G(S)E_{\varphi,N},$$

and therefore $G(S)E_{\varphi,N'} \subseteq G(S)E_{\varphi,N}$. So the group schemes $G(S)E_{\varphi,N'}$ and $G(S)E_{\varphi,N}$ coincide, and H_φ does not depend on the choice of N.

Let us prove that the reduced subscheme of the scheme H_φ is equal to $G(S)$. Assume at first that the field K is perfect. By definition we get $F^N(H_\varphi) = F^N(G(S))$. So by Lemma 6 we get $(H_\varphi)_{\mathrm{red}} = G(S)$. Any field extension preserves this equality, so it holds for any (not necessarily perfect) field K.

To prove that the scheme H_φ is connected it is enough to check that $(H_\varphi)_{\mathrm{red}}$ is connected, because for any non-trivial idempotent $f \in K[H_\varphi]$ the element $\bar{f} \in (K[H_\varphi]/\mathrm{Nil})$ is also a non-trivial idempotent. But the subscheme $(H_\varphi)_{\mathrm{red}}$ is equal to $G(S)$ and therefore is connected.

Since the subscheme $(H_\varphi)_{\mathrm{red}}$ contains the torus T, the scheme H_φ does. $\square$

Lemma 12. $x_\beta(G_a) \cap H_\varphi = x_\beta(\alpha_{p^{\varphi(\beta)}})$.
In particular, all schemes H_φ are distinct.

Proof. Assume at first that the field K is perfect.

Suppose that $\varphi(\beta) = \infty$. Then β lies in S by definition, and by Lemma 3 we get the inclusion $x_\beta(G_a) \subseteq G(S)$. So $x_\beta(G_a) \subseteq H_\varphi$ and $x_\beta(G_a) \cap H_\varphi = x_\beta(G_a)$.

If $\varphi(\beta) < \infty$, then $\varphi(\beta) < N$ by the choice of N. So we have

$$x_\beta(\alpha_{p^{\varphi(\beta)}}) = x_\beta(\alpha_{p^{\min(\varphi(\beta),N)}}) \subseteq E_{\varphi,N} \subseteq H_\varphi.$$

We know that $F^N(E_{\varphi,N}) = 1$, so $F^N(H_\varphi) = F^N(G(S))$. Since $\varphi(\beta)$ is finite, $\beta \notin S$, and by Lemma 3 we have $x_\beta(G_a) \cap G(S) = 1$. Since F preserves root data, we get

$$\begin{aligned} F^N(x_\beta(G_a) \cap H_\varphi) &\subseteq F^N(x_\beta(G_a)) \cap F^N(H_\varphi) \\ &= F^N(x_\beta(G_a)) \cap F^N(G(S)) = F^N(x_\beta(G_a) \cap G(S)), \end{aligned}$$

i.e. $F^N(x_\beta(G_a) \cap H_\varphi) = 1$, so $x_\beta(G_a) \cap H_\varphi \subseteq x_\beta(\alpha_{p^N})$.

Consider an element $x_\beta(a) \in H_\varphi(R)$. By definition of H_φ there exist an *fppf* R-algebra R', an element $g \in G(S, R')$, and an element $h \in E_{\varphi,N}(R')$ such that $x_\beta(a) = gh$. We know that $a^{p^N} = 0$, so $F^N(x_\beta(a)) = 1$. Also we know that $F^N(h) = 1$. Thus $F^N(g) = 1$, or, in other words, the element g lies in the intersection $G(S, R') \cap E_N(R')$. By Lemma 8, we have the inclusion $G(S, R') \cap E_N(R') \subseteq E_{\varphi,N}(R')$. So we get $x_\beta(a) \in E_{\varphi,N}(R')$, and therefore $x_\beta(a) \in E_{\varphi,N}(R)$. By the uniqueness of the decomposition in Lemma 7 and by definition of $E_{\varphi,N}(R)$ we get $a \in \alpha_{p^{\varphi(\beta)}}(R)$, so $x_\beta(G_a) \cap H_\varphi \subseteq x_\beta(\alpha_{p^{\varphi(\beta)}})$.

We proved the assertion for a perfect field K. Since any field extension preserves the equality required, it holds for an arbitrary field K. □

§ 8 Reduction to an algebraically closed field

Now to prove Theorem 1 it is enough to show that any connected subgroup scheme H of $G(\Phi)$ containing T over K is a scheme H_φ for some function φ satisfying the inequality $(*)$. In this section we reduce the general situation to the case of an algebraically closed field K.

Let H be a connected intermediate group scheme $T \leq H \leq G(\Phi)$. Let $H_{\overline{K}}$ be the scheme over the algebraic closure $\overline{K}$ represented by $\overline{K}[H] = \overline{K} \otimes K[H]$. Then $H_{\overline{K}}$ is a subgroup scheme of $G(\Phi)_{\overline{K}}$ containing the split maximal torus $T_{\overline{K}}$. The scheme $H_{\overline{K}}$ is also connected, because field extension preserves connectedness of group schemes, see [5], exp. VIa 2.4.

Any subgroup scheme of a given group scheme is closed (see [5] Exp. VIb 1.4.2).

Suppose now that Theorem 1 is proved in the case of an algebraically closed field. Then the following lemma implies Theorem 1 in the general case.

Lemma 13. *Let H and H' be closed subschemes of any algebraic affine scheme G over a field K. If the schemes $H_{\overline{K}}$ and $H'_{\overline{K}}$ coincide as subschemes of the scheme $G_{\overline{K}}$ over the algebraic closure $\overline{K}$, then the schemes H and H' coincide.*

Proof. Let the scheme G be represented by $K[G]$, and let the subschemes H and H' be represented by $K[G]/I$ and $K[G]/I'$ for some ideals I and I' respectively. Then the subscheme $H_{\overline{K}}$ is represented by $\overline{K} \otimes (K[G]/I) = \overline{K}[G]/\overline{K}[G]I$, and similarly the subscheme $H'_{\overline{K}}$ is represented by $\overline{K}[G]/\overline{K}[G]I'$. Since the schemes $H_{\overline{K}}$ and $H'_{\overline{K}}$ coincide, we get $\overline{K}[G]I = \overline{K}[G]I'$. Thus we can conclude

$$I = K[G] \cap \overline{K}[G]I = K[G] \cap \overline{K}[G]I' = I',$$

because the embedding $K[G] \hookrightarrow \overline{K}[G]$ is faithfully flat. □

Now we may assume the field K is algebraically closed in the proof of Theorem 1.

§ 9 Reduced subscheme

In this section we assume that the field K is algebraically closed.

Let H be a connected subgroup scheme of $G(\Phi)$ containing a split maximal torus T over an algebraically closed field K. Consider the reduced subscheme H_{red}. It is represented by $K[H]/\text{Nil}(K[H])$. The scheme H_{red} contains the torus T, because the torus T is reduced. The reduced subscheme of a group scheme over a perfect (e.g. over an algebraically closed) field is a group scheme (see [5] Exp. VIa 0.2). The reduced subscheme of a connected group scheme is also connected. Any reduced group scheme over an algebraically closed field is smooth (see [12] 11.6). So H_{red} is a connected smooth subgroup scheme of $G(\Phi)$ containing the torus T. By Corollary 5, the scheme H_{red} is equal to $G(S)$ for some quasi-closed subset S of Φ.

Consider a nilradical $\text{Nil}(K[H])$ of the algebra $K[H]$. It is a finitely generated nilpotent ideal, so there is a positive integer N such that $\text{Nil}(K[H])^{p^N} = 0$. Obviously we have $F^N(H) = F^N(H_{\text{red}}) = F^N(G(S))$.

Consider any K-algebra R and any element $g \in H(R)$. Since the element $F^N(h)$ lies in the group $F^N(G(S))(R)$, there is an *fppf* R-algebra R' such that $F^N(g) = F^N(h)$ for some element $h \in G(S, R')$. Then the element $f = h^{-1}g$ satisfies $F^N(f) = 1$, and therefore $f \in E_N(R')$. Thus the element h is equal to the product hf, where $h \in G(S, R')$ and $f \in E_N(R')$. By definition this means that H is a subscheme of $G(S)E_N$. The inclusions $G(S) \subseteq H \subseteq G(S)E_{\varphi_N}$ imply $H = G(S) \cdot (H \cap E_N)$.

The above assertions establish the following lemma.

Lemma 14. *Let H be a connected subgroup scheme of $G(\Phi)$ containing T over an algebraically closed field K. Then the following assertions hold.*

1. *$H_{\text{red}} = G(S)$ for some quasi-closed set S;*
2. *$F^N(H_{\text{red}}) = F^N(G(S))$ for some positive integer N;*
3. *$H = G(S)(H \cap E_N)$, where S and N as above.*

§ 10 Subgroups of reductive groups over rings

In this section we prove Main Lemma 16, which is a useful technical result concerning overgroups of the maximal torus in $G(\Phi, R)$.

Let G be any affine scheme over a field K, R any K-algebra, I any ideal in R, h and h' elements of $G(R)$. We write $h \equiv h' \mod I$, if the images of h and h' under the natural map $G(R) \to G(R/I)$ coincide. Obviously this gives an equivalence relation on $G(R)$, and if G is a group scheme, then multiplication preserves the relation.

Lemma 15. $x_\alpha(a)x_\beta(b) \equiv x_\beta(b)x_\alpha(a) \mod ab$.

Proof. It is enough to prove Lemma for the algebra $K[a,b]$, because we can apply the functor G to the commutative diagram

$$\begin{array}{ccc} K[a,b] & \longrightarrow & K[a,b]/(ab) \\ \big\downarrow & & \big\downarrow \\ R & \longrightarrow & R/(ab), \end{array}$$

and if the images of the left and right parts of the equivalence coincide in $K[a,b]/(ab)$, then they coincide in $R/(ab)$.

The ideals (a) and (b) are coprime in $K[a,b]$, i.e. the product $(a)(b)$ is equal to the intersection $(a)\cap(b)$. Therefore the natural map

$$K[a,b]/(ab) \to K[a,b]/(a) \oplus K[a,b]/(b)$$

is injective. So the map

$$G(K[a,b]/(ab)) \to G(K[a,b]/(a) \oplus K[a,b]/(b))$$

is injective, and it is enough to prove that the images of $x_\alpha(a)x_\beta(b)$ and $x_\beta(b)x_\alpha(a)$ in $G(K[a,b]/(a)\oplus K[a,b]/(b)) = G(K[a,b]/(a))\times G(K[a,b]/(b))$ coincide. In other words, it is enough to check that $x_\alpha(a)x_\beta(b)$ is equal to $x_\beta(b)x_\alpha(a)$ modulo a and modulo b, that is obvious. $\square$

Main Lemma 16. *Let R be a K-algebra, where K is an algebraically closed field. Let H be a subgroup of $G(\Phi,R)$ containing $T(R)$, h be an element of H such that $h=\prod_{\beta\in\Phi} x_\beta(a_\beta)$, where $a_\beta\in \mathrm{Nil}(R)$. Then for each root β the element $x_\beta(a_\beta)$ lies in the group H.*

To prove Main Lemma 16 we use several sublemmas.

Sublemma 16.1. *For any element $\varepsilon\in K^*$ and any root $\beta\in\Phi$ there is an element $t\in T(K)$ such that $\beta(t)=\varepsilon$.*

Proof. Since $\langle\ ,\rangle$ is non-degenerated, we can choose a cocharacter λ such that $\langle\beta,\lambda\rangle\neq 0$. Set $t=\lambda(\varepsilon^{\frac{1}{\langle\beta,\lambda\rangle}})$. $\square$

Sublemma 16.2. *Let α and γ be non-collinear roots. Then there is an element $t\in T(K)$ such that $\alpha(t)\neq 1$, $\gamma(t)=1$.*

Proof. Since $\langle\ ,\rangle$ is non-degenerated, we can choose a cocharacter λ such that $\langle\alpha,\lambda\rangle\neq 0$ and $\langle\gamma,\lambda\rangle=0$. Set $t=\lambda(\varepsilon)$, where $\varepsilon^{\langle\gamma,\lambda\rangle}\neq 1$. $\square$

Sublemma 16.3. *In the settings of Main Lemma 16 let $I\le \mathrm{Nil}(R)$ be an ideal. Suppose that $a_\alpha\in I^r$ for some root α, and $a_\beta\in I^s$ for $\beta\neq\alpha$, $1\le r\le s$. Then there is an element h' in H such that $h'=\prod_{\beta\in\Phi}x_\beta(a'_\beta)$, where $a'_\alpha\equiv a_\alpha \mod I^{r+1}$, $a'_{-\alpha}\in I^{s+1}$, and $a'_\beta\in I^s$ for $\beta\neq\pm\alpha$.*

Proof. Since the field K is algebraically closed, there are elements ε and ξ in K^* such that $\varepsilon+\xi+1\in K^*$ and $\varepsilon^{-1}+\xi^{-1}+1=0$. By Sublemma 16.1, there are $t_1,t_2,t_3\in T(K)$ such that $\alpha(t_1)=\varepsilon$, $\alpha(t_2)=\xi$, and $\alpha(t_3)=(\varepsilon+\xi+1)^{-1}$.

Since $h \equiv 1 \mod \mathrm{Nil}(R)$, we have $t_3((t_1ht_1^{-1})(t_2ht_2^{-1})h)t_3^{-1} \equiv 1 \mod \mathrm{Nil}(R)$, so the element $t_3((t_1ht_1^{-1})(t_2ht_2^{-1})h)t_3^{-1}$ lies in $\mathrm{Ker}(F^M : G \to F^M(G))(R)$ for some M. Then, by Lemma 7, the element $t_3((t_1ht_1^{-1})(t_2ht_2^{-1})h)t_3^{-1}$ lies in the big cell, and therefore we have a decomposition

$$t_3((t_1ht_1^{-1})(t_2ht_2^{-1})h)t_3^{-1} = t_4 \prod_{\beta\in\Phi} x_\beta(a'_\beta)$$

for some $t_4 \in T(R)$ and $a'_\beta \in R$. Consider an element

$$h' = t_4^{-1}t_3((t_1ht_1^{-1})(t_2ht_2^{-1})h)t_3^{-1} = \prod_{\beta\in\Phi} x_\beta(a'_\beta).$$

It lies in the group H, because H contains h and $T(R)$. On the other hand, we have

$$\begin{aligned} h' &= t_4^{-1}t_3((t_1ht_1^{-1})(t_2ht_2^{-1})h)t_3^{-1} \\ &= t_4^{-1} \prod_{\beta\in\Phi} x_\beta(\beta(t_1t_3)a_\beta) \prod_{\beta\in\Phi} x_\beta(\beta(t_2t_3)a_\beta) \prod_{\beta\in\Phi} x_\beta(\beta(t_3)a_\beta) \\ &\equiv t_4^{-1} \prod_{\beta\in\Phi} x_\beta(\beta(t_3)(\beta(t_1)+\beta(t_2)+1)a_\beta) \mod I^{r+s} \end{aligned}$$

by Lemma 15. Since Gauss decomposition is unique for the big cell of the group $G(\Phi, R/I^{r+s})$, we have $a'_\beta \equiv \beta(t_3)(\beta(t_1)+\beta(t_2)+1)a_\beta \mod I^{r+s}$ for each root β. In particular, since $I^{r+1} \subseteq I^{r+s}$ and $I^{s+1} \subseteq I^{r+s}$, we have $a'_\alpha \equiv a_\alpha \mod I^{r+1}$, $a'_{-\alpha} \in I^{s+1}$, and $a'_\beta \in I^s$ for each $\beta \neq \pm\alpha$. ☐

Sublemma 16.4. *Under the assumptions of Sublemma 16.3, there is an element h' in H such that $h' = \prod_{\beta\in\Phi} x_\beta(a'_\beta)$, where $a'_\alpha \equiv a_\alpha \mod I^{r+1}$ and $a'_\beta \in I^{s+1}$ for $\beta \neq \alpha$.*

Proof. By Sublemma 16.3, we may assume that $a_{-\alpha} \in I^{r+1}$.

Fix any root $\gamma \neq \pm\alpha$. By Sublemma 16.2, there is an element $t_1 \in T(K)$ such that $\gamma(t_1) = 1$ and $\alpha(t_1) = \eta \neq 1$. Since $(1-\eta) \in R^*$, Sublemma 16.1 gives an element $t_2 \in T(K)$ such that $\alpha(t_2) = (1-\eta)^{-1}$.

Since $h \equiv 1 \mod \mathrm{Nil}(R)$, we have $t_2[h,t_1]t_2^{-1} \equiv 1 \mod \mathrm{Nil}(R)$, so the element $t_2[h,t_1]t_2^{-1}$ lies in the big cell, and therefore we have a decomposition

$$t_2[h,t_1]t_2^{-1} = t_3 \prod_{\beta\in\Phi} x_\beta(a''_\beta)$$

for some $t_3 \in T(R)$ and $a''_\beta \in R$. Consider an element

$$h'' = t_3^{-1}t_2[h,t_1]t_2^{-1} = \prod_{\beta\in\Phi} x_\beta(a''_\beta).$$

It lies in the group H, because H contains h and $T(R)$. On the other hand, we have

$$\begin{aligned} h'' &= t_3^{-1}t_2[h,t_1]t_2^{-1} = t_3^{-1}(t_2ht_2^{-1})(t_1t_2h^{-1}t_2^{-1}t_1^{-1}) \\ &= t_3^{-1} \prod_{\beta\in\Phi} x_\beta(\beta(t_2)a_\beta) \prod_{-\beta\in\Phi} x_\beta(-\beta(t_1t_2)a_\beta) \\ &\equiv t_3^{-1} \prod_{\beta\in\Phi} x_\beta(\beta(t_2)(1-\beta(t_1))a_\beta) \mod I^{r+s} \end{aligned}$$

by Lemma 15. Since Gauss decomposition is unique for the big cell of the group $G(\Phi, R/I^{r+s})$, we have $a''_\beta \equiv \beta(t_2)(1-\beta(t_1))a_\beta \mod I^{r+s}$ for each root β. In particular, since $I^{r+1} \subseteq I^{r+s}$ and $I^{s+1} \subseteq I^{r+s}$, we have $a''_\alpha \equiv a_\alpha \mod I^{r+1}$, $a''_\gamma \in I^{s+1}$, and if $a_\beta \in I^{s+1}$, then $a''_\beta \in I^{s+1}$.

Proceeding this argument for all roots γ such that $\gamma \neq \pm\alpha$, we obtain an element h' required. □

Sublemma 16.5. *Under the assumptions of Sublemma 16.3, suppose that the ideal I is finitely generated. Then there is an element $a'_\alpha \in R$ such that $a_\alpha \equiv a'_\alpha \mod I^{r+1}$ and $x_\alpha(a'_\alpha) \in H$.*

Proof. This follows from Sublemma 16.4 by induction on s, since some power of the ideal I is equal to zero. □

Sublemma 16.6. *Under the assumptions of Sublemma 16.3, suppose that the ideal I is finitely generated and $r = s$. Then for any positive integer q there is an element $a'_\alpha \in R$ such that $a_\alpha \equiv a'_\alpha \mod I^{r+q}$ and $x_\alpha(a'_\alpha) \in H$.*

Proof. Let us prove the sublemma by induction on q. Sublemma 16.5 implies the assertion for $q = 1$. Suppose now that the assertion holds for q and for each root α, and prove it for $q + 1$.

The element $h = \prod_{\alpha\in\Phi} x_\alpha(a_\alpha)$ lies in H, and for each root α there is an element $a' \in R$ such that $a \equiv a' \mod I^{r+q}$ and $x_\alpha(a') \in H$. Consider an element $(\prod_{\alpha\in\Phi} x_\alpha(a_\alpha))(\prod_{\alpha\in\Phi} x_\alpha(a'_\alpha))^{-1}$. For each root α we have $a_\alpha \in \mathrm{Nil}(R)$ and $a'_\alpha \in \mathrm{Nil}(R)$, so this element lies in the big cell, and therefore we have a decomposition

$$(\prod_{\alpha\in\Phi} x_\alpha(a_\alpha))(\prod_{\alpha\in\Phi} x_\alpha(a'_\alpha))^{-1} = t \prod_{\alpha\in\Phi} x_\alpha(b_\alpha)$$

for some $t \in T(R)$ and $a'_\alpha \in R$. Consider an element

$$h' = t^{-1}(\prod_{\alpha\in\Phi} x_\alpha(a_\alpha))(\prod_{\alpha\in\Phi} x_\alpha(a'_\alpha))^{-1} = \prod_{\alpha\in\Phi} x_\alpha(b_\alpha).$$

It lies in the group H, because H contains h, $T(R)$, and $x_\alpha(a')$ for each root α. On the other hand, we have

$$h' = t^{-1}(\prod_{\alpha\in\Phi} x_\alpha(a_\alpha))(\prod_{\alpha\in\Phi} x_\alpha(a'_\alpha))^{-1} \equiv t^{-1} \prod_{\alpha\in\Phi} x_\alpha(a_\alpha - a'_\alpha) \mod I^{2r+q}$$

by Lemma 15, because $x_\alpha(a_\alpha)x_\alpha(a'_\alpha)^{-1} = x_\alpha(a_\alpha - a'_\alpha)$, and we permute only elements of type $x_\alpha(a_\alpha - a'_\alpha)$, where $a_\alpha - a'_\alpha \in I^{r+q}$, and elements of type $x_\alpha(a'_\alpha)$, where $a'_\alpha \in I^r$. Since Gauss decomposition is unique for the big cell of the group $G(\Phi, R/I^{2r+q})$, we have $b_\alpha \equiv a_\alpha - a'_\alpha \mod I^{2r+q}$ for each root α, and, in particular, $b_\alpha \equiv a_\alpha - a'_\alpha \mod I^{r+q+1}$ and $b_\alpha \in I^{r+q}$. Apply Sublemma 16.5 to the element h'. Then for each root α there is an element a''_α such that $a''_\alpha \equiv b_\alpha \mod I^{r+q+1}$ and $x_\alpha(a''_\alpha) \in H$. Thus we have

$$x_\alpha(a'_\alpha + a''_\alpha) = x_\alpha(a'_\alpha)x_\alpha(a''_\alpha) \in H$$

with $a'_\alpha + a''_\alpha \equiv a_\alpha \mod I^{r+q+1}$. □

Proof of Main Lemma 16. This follows from Sublemma 16.6 for $r = s = 1$, $I = \langle a_\alpha \mid \alpha \in \Phi\rangle$, and for q large enough, because some power of I is equal to zero. □

§ 11 Determining of a function φ

In this section we determine a function φ corresponding to a given connected subgroup scheme H in $G(\Phi)$ that contains T and check that φ satisfies the condition $(*)$.

Lemma 17. *Under the assumptions of Lemma 14, the following equality holds:* $H = G(S)\prod_{\beta\in\Phi}(H\cap x_\beta(\alpha_{p^N}))$.

Proof. By Lemmas 14 and 7, it is enough to prove the equality

$$H\cap (T_N\prod_{\beta\in\Phi} x_\beta(\alpha_{p^N})) = T_N\prod_{\beta\in\Phi}(H\cap x_\beta(\alpha_{p^N})),$$

which follows immediately from Main Lemma 16. □

Any subgroup scheme of the scheme α_{p^N} is a scheme α_{p^M} for some $M\leq N$. Define a function $\varphi:\Phi\to\mathbb{N}\cup\{0,\infty\}$ as follows:
if $\beta\in S$, set $\varphi(\beta)=\infty$;
otherwise $\varphi(\beta)$ is determined by $H\cap x_\beta(\alpha_{p^N}) = x_\beta(\alpha_{p^{\varphi(\beta)}})$.

Lemma 18. $x_\beta(G_a)\cap H = x_\beta(\alpha_{p^{\varphi(\beta)}})$.

Proof. The inclusion $x_\beta(G_a)\cap H\supseteq x_\beta(\alpha_{p^{\varphi(\beta)}})$ is obvious. Let us prove the other inclusion. The case $\beta\in S$ (in other words, $\varphi(\beta)=\infty$) is trivial, because we have the inclusions $x_\beta(G_a)\subseteq G(S)\subseteq H$.

Assume that $\beta\notin S$. We have $F^N(x_\beta(G_a)\cap H)\subseteq F^N(H) = F^N(G)$, so $F^N(x_\beta(G_a)\cap H)\subseteq F^N(G)\cap F^N(x_\beta(G_a))$. Since F preserves root data and $\beta\notin S$, we have $F^N(G)\cap F^N(x_\beta(G_a)) = 1$. Therefore $x_\beta(G_a)\cap H$ lies in the kernel $\mathrm{Ker}(F^N: G(\Phi)\to F^N(G(\Phi)))$. So $x_\beta(G_a)\cap H\subseteq x_\beta(\alpha_{p^N})$. By the setting of φ, this implies $x_\beta(G_a)\cap H = x_\beta(\alpha_{p^{\varphi(\beta)}})$. □

Lemma 19. *The function φ satisfies the inequality $(*)$.*

Proof. Consider the K-algebra $R = K[a,b]/(a^{p^{\varphi(\alpha)}}, b^{p^{\varphi(\beta)}})$. Elements $x_\alpha(a)$ and $x_\beta(b)$ lie in $H(R)$. Since $H(R)$ is a group, the commutator

$$[x_\alpha(a), x_\beta(b)] = \prod_{r,s\geq 1} x_{r\alpha+s\beta}(N_{\alpha\beta rs}a^r b^s)$$

lies in $H(R)$. By Main Lemma 16, we have $x_{r\alpha+s\beta}(N_{\alpha\beta rs}ab)\in H(R)$ for any positive integers r ans s such that $r\alpha+s\beta\in\Phi$. By Lemma 18, this means that $(N_{\alpha\beta rs}ab)^{p^{\varphi(r\alpha+s\beta)}} = 0$. Obviously, this is equivalent to the condition $(*)$. □

Proof of Theorem 1. In Section § 7 we defined a scheme H_φ that corresponds to a function φ satisfying $(*)$. In Lemma 11 we prove that the schemes H_φ satisfies all the conditions of Theorem 1. Lemma 12 shows that all schemes H_φ are distinct. It remains to prove that any scheme H satisfying the conditions of Theorem 1 is a scheme H_φ for an appropriate function φ satisfying $(*)$. By Lemma 13, we may assume K is algebraically closed. In Section § 11 we determine a function φ corresponding to a given scheme H. In Lemma 19 we prove that the function φ satisfies $(*)$. By the definition of φ we have $H = H_\varphi$, and this completes the proof. □

References

[1] A. Borel, J. Tits, *Groupes réductifs.* – Inst. Hautes Études Sci. Publ. Math. 27 (1965), pp. 55-151.

[2] Z. I. Borewicz, N. A. Vavilov, *Subgroups of the general linear group over a semilocal ring containing the group of diagonal matrices.* – Proc. Steklov Inst. Math. 4 (1980), pp. 41–54.

[3] J. C. Jantzen, *Representations of algebraic groups.* – 2nd ed. – Providence, RI: Amer. Math. Soc., (2003).

[4] F. Knop, *Homogeneous varieties for semisimple groups of rank one.* – Comp. Math. 98 (1995), pp. 77-89.

[5] Schemas en groupes (SGA 3) / Séminaire de Géométrie Algébrique du Bois Marie 1962/64, SGA 3. Dirigé par M. Demazure et A.Grothendieck. – Berlin: Springer, (1970).

[6] E. A. Sopkina, *Classification of subgroup schemes in GL_n that contain a split maximal torus. (Russian)* – Zap. Nauch. Sem. POMI 321 (2005), pp.281-296. (English transl. in J. Math. Sci.)

[7] T. A. Springer, *Linear algebraic groups.* – 2nd ed. – Boston: Birkhäuser, (1998).

[8] N. A. Vavilov, *Bruhat decomposition for subgroups containing the group of diagonal matrices. II.* – J. Sov. Math. 27 (1984), pp. 2865-2874.

[9] N. Vavilov, *Intermediate Subgroups in Chevalley Groups.* – Groups of Lie type and their geometries, Como, (1993), pp. 233–280.

[10] N. A. Vavilov, *Subgroups of Chevalley groups containing a maximal torus.* – Proc. Leningrad Math. Soc. 1 (1990), pp. 64–109. (English transl. in Proc. Sanct-Petersburg Math. Soc.)

[11] N. Vavilov, E. Plotkin, *Chevalley groups over commutative rings I. Elementary calculations.* – Acta Appl. Math. 45 (1996), pp. 73–113.

[12] W. C. Waterhouse, *Introduction to affine group schemes.* – New York: Springer, 1979.

[13] Ch. Wenzel, *Classification of all parabolic subgroup-schemes of a reductive linear algebraic group over an algebraically closed field.* – Trans. Amer. Math. Soc. 337 (1993), pp. 211-218.

[14] Ch. Wenzel, *Rationality of G/P for a nonreduced parabolic subgroup-scheme P.* – Proc. Amer. Math. Soc. 117 (1993), pp. 899-904.