Tôhoku Math. Journ.
37 (1985), 423-454.

ON FULL SUBGROUPS OF CHEVALLEY GROUPS*

LEONID N. VASERSTEIN

(Received July 16, 1984)

Introduction. Let G be a split algebraic absolutely almost simple group defined over a field k. For a split maximal k-subtorus T of G let $\Sigma = \Sigma(G, T)$ denote the root system of G with respect to T. Let $\{x_\varepsilon, \varepsilon \in \Sigma\}$ be a system of isomorphisms, normalized as usual (see, for example, Steinberg [4]), from the additive group onto the root subgroups with respect to T.

We say (in the spirit of O'Meara [2, 3]) that a subgroup H of $G(k)$ is *full* if for every g in $G(k)$ and ε in Σ there exists a non-zero $c = c(g, \varepsilon)$ in k such that $g^{-1}x_\varepsilon(c)g \in H$. Thus, H is full if and only if its intersection with any root subgroup (relative to any maximal split k-torus) contains at least two elements.

For a subset R of k we denote by $G^E(R)$ the subgroup of $G(k)$ generated by all $x_\varepsilon(a)$, where $\varepsilon \in \Sigma$ and $a \in R$. Here "E" stands for "elementary".

A subset R of k is called *full* (cf., Vaserstein [7]) if for every y in k there is a non-zero r in R such that $yr \in R$. For a subring R it means that k is its field of fractions. Note that in this paper a ring is not required to have identity.

The results of the present paper are modeled on the results of Vaserstein [7], the methods are also similar. However the situation for groups of type C_n in characteristic 2 turns out to be more complicated.

We assume throughout (except in the last section) that the rank of G is greater than one. If $\mathrm{rank}(G) = 1$, i.e., G is of type A_1, then the conclusions of Theorems 1-5 below are false, see [7] and the last section, where we also discuss possible generalizations of our results.

The following Theorems 1-5 summarize our main results. More precise and detailed statements are given in the corresponding sections.

THEOREM 1. *For every full subring R of k, the subgroup $G^E(R)$ of $G(k)$ is full.*

THEOREM 2. ("Arithmeticity Theorem"). *Every full subgroup H of $G(k)$ contains $G^E(A)$ for some full subring A of k with the exception of*

* This research was supported in part by NSF grants.

the case when G *is of type* $\boldsymbol{C}_n$ $(n \geqq 2)$, $\mathrm{char}(k) = 2$ *and the dimension of* k *over* k^2 *is uncountable.*

Here, for a field k of characteristic 2, k^2 denotes the subfield of k, consisting of all squares. In the exceptional case we will show that not every full subgroup H contains $G^E(A)$ for a full subring A (see Sections 8 and 9 for details).

THEOREM 3. *If* H *is a full subgroup of* $G(k)$ *and* $g_1, \cdots, g_m$ *are in* $G(k)$ *then the intersection of all* $g_i H g_i^{-1}$ *is a full subgroup of* $G(k)$.

THEOREM 4. *Assume that* k *does not consist of* 2 *elements when* G *is of type* $\boldsymbol{B}_2$ *or* $\boldsymbol{G}_2$. *If* H *is a full subgroup of* $G(k)$ *and* M *is a subgroup of* $G(k)$ *normalized by* H *then either* $H \cap M$ *is full or* M *lies in the center of* G.

Theorems 1–4 for $G = SL_n$ were proved by Vaserstein [7]. According to [10], Serezhkin considered subgroups H of $G(k) = SL_n(k)$, $n \geqq 3$, more general than full subgroups. Assuming that H is irreducible (in the standard representation) he proves that a conjugate of H either contains $G^E(A) = E_n(A)$ for a full subring A of k or is contained in $HSp_n(k)$, the group of symplectic similitudes. Since a full H is irreducible and $HSp_n(k)$ is not full, this result combined with our Theorem 8.4 gives Theorem 2 for $G = SL_n$, $n \geqq 3$. He also tried to prove Theorem 2 for $G = Sp_{2n}$ with $\mathrm{char}(k) \neq 2$, see [11].

THEOREM 5. *Let* H *be a subgroup of* $G(k)$. *Set* $R_\varepsilon(H) := \{t \in k \colon x_\varepsilon(t) \in H\}$. *Suppose that* $R_\varepsilon := R_\varepsilon(H) \neq 0$ *for every root* ε *in* Σ. *Suppose further that* G *is not of type* $\boldsymbol{B}_n$, $\boldsymbol{C}_n$, *or* $\boldsymbol{F}_4$ *when* $\mathrm{char}(k) = 2$, *and that* G *is not of type* $\boldsymbol{G}_2$ *when* $\mathrm{char}(k) = 3$. *Then there is a non-zero subring* A *of* k *such that* $R_\varepsilon A \subset R_\varepsilon$ *(i.e.* R_ε *is an* A*-module) and* $(AR_\varepsilon)(AR_{-\varepsilon}) \subset A$ *for every root* ε *in* Σ.

We do not assume here that H is full. Here and throughout the paper $BC := \{bc \colon b \in B, c \in C\}$ for any subsets $B, C \subset k$. About the cases excluded from Theorem 5, see the next section.

The groups H in Theorem 5 are similar to "tableau", "carpet" or "net" groups considered in many papers including Riehm [12], [13], James [14], Borevich [15], Vavilov [16]. The main two differences are that our $R_\varepsilon(H)$ need not be ideals of A and are not allowed to be 0.

ACKNOWLEDGEMENTS. I thank S. Simpson and T. Jech for giving the reference [1] and D. James and a referee for many corrections. The work was started in the fall of 1981 jointly with B. Weisfeiler, and later he made a few corrections.

NOTATIONS AND CONVENTIONS. If all roots in Σ have the same length, we set $\Sigma_l := \Sigma_s := \Sigma$. Otherwise there are roots of only two lengths in Σ (see, for example, [4]). We denote then by Σ_l (resp., Σ_s) the set of long (resp., short) roots in Σ. Always, Σ_l is a subsystem of Σ.

Let $e(\Sigma)$ be the square ratio of lengths of long and short roots. Recall that $e(\Sigma) = 1$ when Σ is of type $\boldsymbol{A}_n$, $\boldsymbol{D}_n$, or $\boldsymbol{E}_n$; $e(\Sigma) = 2$ when Σ is of type $\boldsymbol{B}_n$, $\boldsymbol{C}_n$ or $\boldsymbol{F}_4$; $e(\Sigma) = 3$ when Σ is of type $\boldsymbol{G}_2$.

We say that a subset of Σ is *connected* if it is not a union of two orthogonal non-empty subsets.

If α, β are in Σ and $\alpha \neq \beta \neq -\alpha$, then we have a commutation relation of the form $[x_\alpha(t), x_\beta(u)] = \prod x_{i\alpha+j\beta}(\pm p_{\alpha,\beta,i,j} t^i u^j)$ for all t, u in k, where the product is taken over all roots $i\alpha + j\beta$ in Σ with natural $i, j \geqq 1$, the factors in the product are ordered lexicographically (i and, for fixed i, also j increase from the left to the right), $p_{\alpha,\beta,i,j}$ are natural numbers, and the signs $\pm$ do not depend on t and u but only on α, β, i, j (once the parametrizations x_φ were chosen). When $\alpha + \beta$ is not a root, the product is taken over an empty set and equals 1.

For a subset $A \subset k$ and an integer n we set $A^n := \{a^n : a \in A\}$. For $A, B \subset k$ we set $AB := \{ab : a \in A,\ b \in B\}$.

We define p as follows: if $\mathrm{char}(k) \neq e(\Sigma)$, then $p := 1$; otherwise, $p := \mathrm{char}(k) = e(\Sigma)$.

For a subgroup H of $G(k)$ and a root ε in Σ we set $R_\varepsilon(H) := \{t \in k : x_\varepsilon(t) \in H\}$.

1. A generalization of Theorem 5.

1.1. THEOREM. *Let H be a subgroup of $G(k)$ such that $R_\varepsilon(H) \neq \{0\}$ for every root ε in Σ. Set $R_\varepsilon := R_\varepsilon(H)$. Then there exist additive subgroups A and B of k and (for every root ε) non-zero a_ε, b_ε in k such that:*

(i) *$a_\delta B \subset R_\delta \subset b_\delta B$, $R_\delta A^p \subset R_\delta$, and $AR_\delta R_{-\delta} \subset A$ for every long root δ in Σ;*

(ii) *$a_\gamma A \subset B_\gamma \subset b_\gamma A$, $R_\gamma B \subset R_\gamma$, and $B'(R_\gamma R_{-\gamma})^p \subset B$ for every short root γ in Σ, where $B' := BB$ when $\mathrm{char}(k) = 2 = e(\Sigma) - 1$, $B' := e(\Sigma)!\, B$ when $\mathrm{char}(k) = 0$, and $B' := B$ otherwise;*

(iii) *$AB \subset A$, $BA^p \subset B$, and $A^p \subset B \subset A$;*

(iv) *B is a subring of k (i.e. $BB \subset B$) when Σ_l is connected; A is a subring of k when Σ_s is connected.*

The case $p = 1$ of this theorem contains Theorem 5 (indeed, (iii) with $p = 1$ implies that $A = B$ is a subring, and to obtain $AAR_\gamma R_{-\gamma} \subset A$ when $\mathrm{char}(k) = 0$, we replace A by $e(\Sigma)!A$). Note that $R_\varepsilon A \subset R_\varepsilon$ and $AAR_\varepsilon R_{-\varepsilon} \subset A$

imply $c_\varepsilon A \subset R_\varepsilon \subset c_{-\varepsilon}^{-1} A$ for any c_ε in R_ε and $c_{-\varepsilon} \neq 0$ in $AAR_{-\varepsilon}$. When $p \neq 1$ and k is not algebraic over its prime subfield, the conclusion of Theorem 5 is false for some H with $R_\varepsilon(H) \neq 0$ for all ε in Σ, see Theorem 6.1 below (namely, for $H = G^E(k_0, k_0^p)$ with subfields $k_0^p \subset k_0 \subset k$).

We will prove Theorem 1.1 in Sections 2, 3–4, and 5 in cases $e(\Sigma) = 1, 2$ and 3 respectively. The following technical lemmas will be used in our proof of Theorem 1.1.

1.2. LEMMA. *Let $m \geqq 2$ be an integer; $A, B \subset k$; $AB \subset A$, $A^m B \subset B$. Then:*

(i) *if a is in the multiplicative set generated by A and b is in the multiplicative set generated by B, then $Ba^m \subset B$ and $Ab \subset A$; therefore, for $A_1 := Aa$, $B_1 := Bb$ we have $A_1B_1 \subset A_1$, $A_1^m B_1 \subset B_1$;*

(ii) *if $a \in A$, $b \in B$, then for $A_2 := Aa^{m-1}b$, $B_2 := Ba^m b$ we have $A_2B_2 \subset A_2$, $A_2^m B_2 \subset B_2$, and $B_2 \subset A_2$;*

(iii) *if $b \in B \subset A$, then for $A_3 := Ab$, $B_3 := Bb^{m-1}$ we have $A_3B_3 \subset A_3$, $A_3^m B_3 \subset B_3$, and $A_3^m \subset B_3 \subset A_3$;*

(iv) *if $B \neq 0 \neq cAA \subset A$ for some c in k, then there is a non-zero a_0 in A such that $(a_0^{m-1}A)(a_0^{m-1}A) \subset a_0^{m-1}A$;*

(v) *if $A \neq 0 \neq cBB \subset B$ for some c in k, then there is a non-zero b_0 in B such that $(b_0^{m-1}B)(b_0^{m-1}B) \subset b_0^{m-1}B$.*

PROOF. (i) We write $a = a_1 \cdots a_n$ with $a_i \in A$. Then $Ba_1^m \subset BA^m \subset B$ and, by induction on n, $Ba^m = B(a_1 \cdots a_{n-1})^m a_n^m \subset Ba_n^m \subset B$. Similarly $Ab \subset A$.

(ii) Since $a^{m-1}b = a^{m-2}ab \in a^{m-2}AB \subset a^{m-2}A$ and $a^m b \in A^m B \subset B$, by (i) we have $A_2B_2 = A_2$ and $A_2^m B_2 \subset B_2$. Moreover, $B_2 = Ba^m b = (Ba)a^{m-1}b \subset Aa^{m-1}b = A_2$.

(iii) Again, the first two inclusions follow from (i), which implies also that $b^{m-2}B \subset A$. Hence $B_3 = b^{m-1}B \subset Ab = A_3$. Finally, $A_3^m = A^m b^m = A^m bb^{m-1} \subset A^m Bb^{m-1} \subset Bb^{m-1} = B_3$.

(iv) We have $(cA)(cA) \subset cA$, that is, cA is a multiplicative set in k. In particular, $(cA)^{2m} \subset ((cA)(cA))^m \subset (cA)^m$, so $B(cA)^{2m}A \subset B(cA)^m A = c^m BA^m A \subset c^m BA \subset c^m A$.

On the other hand, $B(cA)^{2m}A = c^{2m}(BA^{2m})A \subset c^{2m}BA \subset c^{2m}A$.

Therefore $c^m A \cap c^{2m} A \neq 0$, i.e., there are non-zero a_0 and a in A such that $c^m = a_0/a$. Then $a_0^{m-1} = a_0^{m-2}a_0 = a_0^{m-2}ac^m = (a_0c)^{m-2}(ac)c \in (cA)^{m-2}(cA)c \subset (cA)c = c^2A$. Hence $A(a_0^{m-1}A) \subset A(c^2A)A = Ac(cAA) \subset AcA \subset A$. Multiplying both sides by a_0^{m-1}, we get $(a_0^{m-1}A)(a_0^{m-1}A) \subset a_0^{m-1}A$.

(v) From $(cB)(cB) \subset cB$ we deduce that $A(cB)^2 \subset AcB = cAB \subset cA$. On the other hand, $A(cB)^2 = c^2AB^2 \subset c^2(AB)B \subset c^2AB \subset c^2A$.

Therefore, $cA \cap c^2A \supset A(cB)^2 \neq 0$, hence $a_0 = ac$ for some non-zero a,

a_0 in A. Pick a non-zero b' in B. Then $0 \neq b := a^m b' \in A^m B \subset B$, $0 \neq b_0 := a_0^m b' \in A^m B \subset B$, and $b_0 = c^m b$.

We have $b_0^{m-1} = c^m b b_0^{m-2} = (bc)(b_0 c)^{m-2} c \in (Bc)(Bc)^{m-2} c \subset (Bc)c = Bc^2$. Therefore, $B(b_0^{m-1}B) \subset B(Bc^2)B = Bc(BcB) \subset BcB \subset B$. Multiplying this with b_0^{m-1}, we get $(b_0^{m-1}B)(b_0^{m-1}B) \subset b_0^{m-1}B$.

1.3. LEMMA. *Let n, m, N be natural numbers. Let non-empty $A, B, R_i \subset k$, and $c_i, d_i \in k$ for $i = 1, \cdots, N$. Assume that $0 \neq AB^n \subset A$, $A^m B \subset B$, $0 \neq c_i A \subset R_i \subset d_i A$ $(i = 1, \cdots, N)$. Then there is a non-zero b in B such that $d_i A(bB)^n \subset c_i A$ and, therefore, $R_i(bB)^n \subset R_i$ for $i = 1, \cdots, N$.*

PROOF. From $c_i A \subset d_i A$ it follows that $A(c_i/d_i) \subset A$. Therefore $A(c_i/d_i)^r \subset A$ for every integer $r \geqq 0$. Pick non-zero a_0 in A and b' in B. Set $a_i := a_0 c_i/d_i \in A$, $b_i := b' a_i^m \in BA^m \subset B$ for $i = 1, \cdots, N$, and $b_0 := b' a_0^m \in B$.

We have: $(c_i/d_i)^m = (a_i/a_0)^m = b_i/b_0$ and $b_i^n A \subset b_i^n A/b_0^n = A(b_i/b_0)^n = A(c_i/d_i)^{mn} \subset Ac_i/d_i$ for $i = 1, \cdots, N$.

Let a be the product of all a_i, $i = 1, \cdots, N$, and $b := b'a^m \in BA^m \subset B$. We have: $bB = b_1 B$ when $N = 1$, and $bB \subset b_i A^m B \subset b_i B$ for $i = 1, \cdots, N$ when $N > 1$.

Therefore, $A(bB)^n \subset A(b_i B)^n = AB^n b_i^n \subset Ab_i^n \subset Ac_i/d_i$. Hence $d_i A(bB)^n \subset Ac_i$ and $R_i(bB)^n \subset d_i A(bB)^n \subset Ac_i \subset R_i$ for $i = 1, \cdots, N$.

2. Proof of Theorem 1.1 for groups G of type $\boldsymbol{A}_n$ $(n \geqq 2)$, $\boldsymbol{D}_n$ $(n \geqq 3)$, and $\boldsymbol{E}_n$ $(n = 6, 7, 8)$. Recall that H is a subgroup of $G(k)$ and that the $R_\varepsilon := R_\varepsilon(H) := \{t \in k \colon x_\varepsilon(t) \in H\}$ are assumed to be non-zero for all roots ε in Σ. In this section we consider the case when $\Sigma = \Sigma_l = \Sigma_s$.

2.1. LEMMA. (i) *If $\gamma, \delta, \gamma + \delta \in \Sigma$ then $R_\gamma R_\delta \subset R_{\gamma+\delta}$;*

(ii) *for any α, β in Σ there exists a non-zero $c_{\alpha,\beta}$ in k such that $c_{\alpha,\beta} R_\beta \subset R_\alpha$.*

PROOF. (i) We have $[x_\gamma(t), x_\delta(u)] = x_{\gamma+\delta}(\pm tu)$ for all t, u in k (see, e.g., [4, Examples to Lemma 14]). Taking here $t \in R_\gamma$, $u \in R_\delta$ we see that $R_\gamma R_\delta \subset R_{\gamma+\delta}$.

(ii) There exist $\gamma_1, \cdots, \gamma_m$ in Σ such that $\beta + \gamma_1 + \cdots + \gamma_i \in \Sigma$ for all $i \leqq m$ and $\alpha = \beta + \gamma_1 + \cdots + \gamma_m$. Let us proceed by induction on m. If $m = 0$, then $R_\alpha = R_\beta$ and we can take $c_{\alpha,\beta} = 1$. For $m \geqq 1$, we set $\gamma := \gamma_m$, $\delta = \beta + \gamma_1 + \cdots + \gamma_{m-1}$. Pick a non-zero c_γ in R_γ. Applying (i) and the inductive assumption to δ, we have: $R_{\gamma+\delta} = R_\alpha \supset R_\gamma R_\delta \supset c_{\delta,\beta} R_\beta R_\gamma \supset c_\gamma c_{\delta,\beta} R_\beta = c_{\alpha,\beta} R$ with $c_{\alpha,\beta} := c_\gamma c_{\delta,\beta} \neq 0$.

Now we can complete our proof of Theorem 1.1 in the case $\Sigma = \Sigma_l$.

For every pair α, β of roots in Σ we fix a non-zero $c_{\alpha,\beta} \in k$ such that $c_{\alpha,\beta} R_\beta \subset R_\alpha$ (see, Lemma 2.1 (ii)).

Pick roots α, β, γ in Σ such that $\gamma = \alpha - \beta$. By Lemma 2.1, $R_\alpha \supset R_\beta R_\gamma \supset c_{\beta,\alpha} R_\alpha c_{\gamma,\alpha} R_\alpha = c R_\alpha R_\alpha$, where $c := c_{\beta,\alpha} c_{\gamma,\alpha} \neq 0$, hence $A := cR_\alpha \supset cR_\alpha cR_\alpha = AA$ is a subring of k.

For any root ε in Σ set $a_\varepsilon := c^{-1} c_{\varepsilon,\alpha}$, $b_\varepsilon := c^{-1} c_{\alpha,\varepsilon}^{-1} \neq 0$, hence $R_\varepsilon \supset c_{\varepsilon,\alpha} R_\alpha = c_{\varepsilon,\alpha} c^{-1} A = a_\varepsilon A$ and $R_\varepsilon \subset c_{\alpha,\varepsilon}^{-1} R_\alpha = c^{-1} c_{\alpha,\varepsilon}^{-1} A = b_\varepsilon A$.

By Lemma 1.3 (with $A = B$, $m = n = 1$, $N := \operatorname{card}(\Sigma)$), $(aA) R_\varepsilon \subset R_\varepsilon$ for all ε in Σ with some non-zero a in A. Replace A by aA and a_ε, b_ε by $a_\varepsilon a^{-1}$, $b_\varepsilon a^{-1}$ respectively. Then $AR_\varepsilon \subset R_\varepsilon$ for all ε in Σ and still $a_\varepsilon A \subset R_\varepsilon \subset b_\varepsilon A$ for all ε.

Now for every ε in Σ we can find δ in Σ such that $\varepsilon + \delta \in \Sigma$. Then $R_\delta R_\varepsilon R_{-\varepsilon} \subset R_{\delta+\varepsilon} R_{-\varepsilon} \subset R_\delta$ by Lemma 2.1 (i). Take the product R of all R_δ over $\delta \in \Sigma$. Then $RR_\varepsilon R_{-\varepsilon} \subset R$ for all ε in Σ.

Since $R_\varepsilon \subset b_\varepsilon A$ for all ε, we have $R \subset bA$, where $b \neq 0$ is the product of all b_ε. Replacing A by its subring generated by Rb^{-1}, we have $R_\varepsilon A \subset R_\varepsilon$ and $AR_\varepsilon R_{-\varepsilon} \subset A$ for every root ε in Σ.

3. Proof of Theorem 1.1 for G of type B_2. Since G is split over k, it is isogenous to the symplectic group of a non-singular alternating form in dimension 4.

The root system (see, Figure 1) consists of 8 roots. Four of them ($\pm\alpha$, $\pm(\alpha + 2\beta)$) are long, and four ($\pm\beta$, $\pm(\alpha + \beta)$) are short.

Let us call a pair (γ, δ) of roots *admissible*, if $\gamma \in \Sigma_s$, $\delta \in \Sigma_l$, and $\delta - \gamma \in \Sigma_s$. In other words, γ is short and δ makes an angle $\pm 45°$ with γ. Every root is contained therefore in exactly two admissible pairs.

As in Theorem 1.1, $R_\varepsilon := R_\varepsilon(H) \neq \{0\}$. For any pair (γ, δ) of roots we set $R_{\gamma,\delta} := R_{\gamma,\delta}(H) := \{(t, u) \in k \oplus k\colon x_\gamma(t) x_\delta(u) \in H\}$. Let $R'_{\gamma,\delta}$ (resp., $R''_{\gamma,\delta}$) be the projection of $R_{\gamma,\delta}$ on the first (resp., second) factor. Clearly,

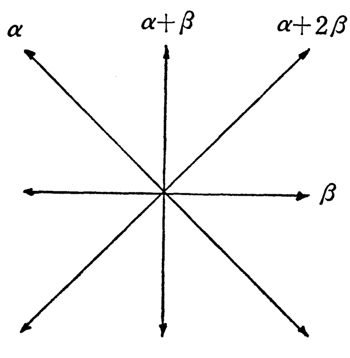

FIGURE 1. System of roots of type B_2.

$R'_{\gamma,\delta} \supset R_\gamma$ and $R''_{\gamma,\delta} \supset R_\delta$.

3.1 LEMMA. *Let* (γ, δ) *be an admissible pair of roots,* $a \in R_{2\gamma-\delta}$, $b \in R_{\delta-2\gamma}$, $(c, d) \in R_{\gamma,\delta}$, *and* $t_1, t_2 \in R_{\gamma-\delta}$. *Then* (i) $(abc, ab^2c^2) \in R_{\gamma,\delta}$; (ii) $2t_1t_2d \in R_{2\gamma-\delta}$.

PROOF. Set $\varepsilon := \delta - 2\gamma$.

(i) Since both $x_\varepsilon(k)$ and $x_{-\varepsilon}(k)$ commute with $x_\delta(k)$, we have: $H \ni [x_{-\varepsilon}(a), [x_\varepsilon(b), x_\gamma(c)x_\delta(d)]] = [x_{-\varepsilon}(a), x_{\delta-\gamma}(\pm bc)x_\delta(\pm bc^2)] = x_\gamma(\pm abc)x_\delta(\pm ab^2c^2)$. Since $R_{\pm\varepsilon}$ are additive subgroups of k, we can, changing if necessary signs of a and b, obtain that $R_{\gamma,\delta} \ni (abc, ab^2c^2)$, as claimed.

(ii) We have $H \ni y(t) := [x_{\gamma-\delta}(t), x_\gamma(c)x_\delta(d)] = x_\gamma(\pm td)x_{2\gamma-\delta}(\pm t^2d \pm 2ct)$ for any t in $R_{\gamma-\beta}$, hence $H \ni y(t_1 + t_2)y(-t_1)y(-t_2) = x_{2\gamma-\delta}(\pm 2t_1t_2d)$. Thus, $R_{2\gamma-\delta} = -R_{2\gamma-\delta} \ni 2t_1t_2d$.

3.2. COROLLARY. *In the notation of Lemma* 3.1:

(i) $R_\gamma \supset 2R_\varepsilon R_{-\varepsilon} R'_{\gamma,\delta}$ *and* $R_\delta \supset 8R_\varepsilon R_\varepsilon R_{-\varepsilon} R_\gamma R'_{\gamma,\delta}$, *where* $\varepsilon := \delta - 2\gamma$;

(ii) $R_\delta C_{\gamma-\delta} C_{\gamma-\delta} \subset R_\delta \supset 4R_\delta C_{\gamma-\delta} C_{\gamma-\delta} C_{\gamma-\delta}$, *where* $C_{\gamma-\delta} := 2R_{\gamma-\delta}R_{\delta-\gamma}$.

PROOF. (i) Let a, b, c, d be as in Lemma 3.1, and $c' \in R_\gamma$, $b' \in R_\varepsilon$. By Lemma 3.1, $R_{\gamma,\delta} \ni z(c) := (abc, ab^2c^2) \in k \oplus k$. Since $x_\gamma(k)$ and $x_\delta(k)$ commute, $R_{\gamma,\delta}$ is an additive subgroup of $k \oplus k$. Therefore, $R_{\gamma,\delta} \ni z(c) - z(-c) = (2abc, 0)$, so $R_\delta \supset 2R_{-\varepsilon} R_\varepsilon R'_{\gamma,\delta}$, which proves the first inclusion.

Similarly, $R_{\gamma,\delta} \ni z(c) + z(-c) = (0, 2ab^2c^2)$, hence $R_\delta \ni 2ab^2c^2$. Therefore $R_\delta \ni 2ab^2(c + c')^2 - 2ab^2c^2 - 2ab^2c'^2 = 4ab^2cc'$ and $R_\delta \ni 4a(b + b')^2cc' - 4ab^2cc' - 4ab'^2cc' = 8abb'cc'$. This establishes the second inclusion in Corollary 3.2(i).

(ii) By Lemma 3.1 (ii), $R''_{\gamma,\delta}(2R_{\gamma-\delta}R_{\gamma-\delta}) \subset R_{2\gamma-\delta}$. Replacing here (γ, δ) by the admissible pair $(\gamma, 2\gamma - \delta)$, we get $R''_{\gamma,2\gamma-\delta}(2R_{\delta-\gamma}R_{\delta-\gamma}) \subset R_\delta$. Combining the last two inclusions we get $R''_{\gamma,\delta}C_{\gamma-\delta}C_{\gamma-\delta} \subset R_{2\gamma-\delta}(2R_{\delta-\gamma}R_{\delta-\gamma}) \subset R_\delta$.

To prove the second inclusion in (ii) we take arbitrary u in $R_{\gamma-\delta}$, v in $R_{\delta-\gamma}$, and t in R_δ. Then $H \ni [[x_\delta(t), x_{\gamma-\delta}(u)], x_{\delta-\gamma}(v)] = x_\gamma(\pm tu^2v)x_\delta(\pm 2tuv \pm tu^2v^2)$, hence (changing if necessary signs of t and u) $R''_{\gamma,\delta} \ni 2tuv + u^2v^2t$. Since $R''_{\gamma,\delta} \supset R_\delta \supset R_\delta C_{\gamma-\delta}C_{\gamma-\delta} \ni 4u^2v^2t$, it follows that $R''_{\gamma,\delta} \ni 8tuv$. Thus, $R''_{\gamma,\delta} \supset 4R_\delta C_{\gamma-\delta}$. Combining this with $R''_{\gamma,\delta}C_{\gamma-\delta}C_{\gamma-\delta} \subset R_\delta$, we get Corollary 3.2 (ii).

PROOF OF THEOREM 1.1 FOR TYPE B_2 WHEN $\mathrm{char}(k) \neq 2$. For every root φ in Σ we pick a non-zero c_φ in R_φ.

By Corollary 3.2 (i), $R_\gamma \supset c_{\gamma,\varepsilon}R_\varepsilon$, $R_\gamma \supset c_{\gamma,-\varepsilon}R_{-\varepsilon}$, where $c_{\gamma,\varepsilon} := 2c_\gamma c_{-\varepsilon}$, $c_{\gamma,-\varepsilon} := 2c_\gamma c_\varepsilon$. Similarly, $R_\delta \supset c_{\delta,\varepsilon}R_\varepsilon$, $c_{\delta,-\varepsilon}R_{-\varepsilon}$, $c_{\delta,\gamma}R_\gamma$ with $c_{\delta,\varepsilon} := 8c_{-\varepsilon}c_\gamma^2c_\varepsilon$, $c_{\delta,-\varepsilon} := 8c_\varepsilon^2c_\gamma^2$, $c_{\delta,\gamma} := 8c_\varepsilon^2c_{-\varepsilon}c_\gamma$.

Applying the above inclusions (with other admissible pairs of roots) successively, one easily establishes that for any φ, ψ in Σ there is a non-zero $c_{\varphi,\psi}$ in k such that $R_\varphi \supset c_{\varphi,\psi} R_\psi$. Fix such $c_{\varphi,\psi}$.

Let A be the subring of k generated by $2R_\alpha R_{-\alpha}$. We have $A \supset 2c_{-\alpha}R_\alpha$. Applying Corollary 3.2 (i) with $\gamma := \beta$, $\delta := \alpha + 2\beta$, $\varepsilon := \delta - 2\gamma = \alpha$, we get $R_\beta \supset AR_\beta$ hence $R_\beta \supset c_\beta A$. Therefore $a_\varphi A \subset R_\varphi \subset b_\varphi A$ for every root φ in Σ, where $a_\varphi := c_{\varphi,\beta}c_\beta$, $b_\varphi := (2c_{-\alpha}c_{\alpha,\varphi})^{-1}$. Using Lemma 1.3 with $m = n = 1$, $A = B$, we find a non-zero a in A such that all R_φ are aA-modules.

Replacing A by aA and changing a_φ, b_φ accordingly, we have $R_\varphi A \subset R_\varphi$ for all φ and still $a_\varphi A \subset R_\varphi \subset b_\varphi A$ for all φ with non-zero a_φ, b_φ.

By Lemma 3.1 (i), $R_\varepsilon R_{-\varepsilon} R'_{\gamma,\delta} \subset R'_{\gamma,\delta}$ for any admissible pair (γ, δ), where $\varepsilon := \delta - 2\gamma$. Consider the product A_1 of all $R'_{\gamma,\delta}$. Then $A_1 R_\varepsilon R_{-\varepsilon} \subset A_1$ for every long root ε in Σ. Using Corollary 3.2 (i) and $AA \subset A$, we see that $0 \neq cA_1 \subset A$ for some c in k. Replacing A by its subring generated by cAA_1, we get $AR_\delta R_{-\delta} \subset A$ for all δ in Σ_l. We still have $R_\varepsilon A \subset R_\varepsilon$ for all ε in Σ and $R_\varepsilon \subset b'_\varepsilon A$ for all ε in Σ with some $b'_\varepsilon \neq 0$ in k.

Let now (γ, δ) be an admissible pair. Using $R_\varepsilon \subset b'_\varepsilon A$ for $\varepsilon = \delta - \gamma$ and $\varepsilon = \gamma - \delta$, we get $uC_{\gamma-\delta} \subset A$, where $u := (b'_{\gamma-\delta}b'_{\delta-\gamma})^{-1} \neq 0$. Multiplying the inclusions in Corollary 3.2 (ii) by u^2 and u^3 accordingly, we get $R_\delta \cap R_\delta u^2 \neq 0 \neq R_\delta \cap 4R_\delta u^3$. Since $R_\delta \subset bA$ for some b in k (it follows from $AR_\delta R_{-\delta} \subset A \neq 0$), $uA \cap A \neq 0$. Therefore, $0 \neq vC_{\gamma-\delta} \subset A$ for some v in A. We have $(R_\delta \cup R_\delta C_{\gamma-\delta})C_{\gamma-\delta} \subset R_\delta \cup R_\delta C_{\gamma-\delta}$ and $R_\delta \cup R_\delta C_{\gamma-\delta} \subset bA \cup bAC_{\gamma-\delta} \subset b(A \cup C_{\gamma-\delta}) \subset bv^{-1}A$, hence $w_{\gamma,\delta}(R_\delta \cup R_\delta C_{\gamma-\delta}) \subset A$, where $w_{\gamma,\delta} := vb^{-1}$.

Let A_2 be the product of all $w_{\gamma,\delta}(R_\delta \cup R_\delta C_{\gamma-\delta})$. Then $A_2 C_\gamma \subset A_2 \subset A$ for all γ in Σ_s. Replacing A by its subring generated by AA_2, we get $AC_\gamma \subset A$ for all γ in Σ_s. We still have $A(R_\delta R_{-\delta}) \subset A$ for all δ in Σ_l and $R_\varepsilon A \subset R_\varepsilon$ for all ε in Σ.

Thus, Theorem 1.1 is proved for G of type $\boldsymbol{B}_2$ when $\mathrm{char}(k) \neq 2$. For the rest of this section we assume that $\mathrm{char}(k) = 2$. Then $[x_{\pm\beta}(k), x_{\pm(\alpha+\beta)}(k)] = 1$.

3.3. LEMMA. *Let (γ, δ) be an admissible pair of roots. Then $(rs, rs^2) \in R_{\delta-\gamma,\delta}$ for any s in $R'_{\gamma,\delta}$ and r in $R''_{\delta-\gamma,\delta-2\gamma}$. In particular,*

(i) $R'_{\delta-\gamma,\delta} \supset R'_{\gamma,\delta} R''_{\delta-\gamma,\delta-2\gamma}$

(ii) $R''_{\delta-\gamma,\delta} \supset R''_{\delta-\gamma,\delta-2\gamma}(R'_{\gamma,\delta})^2$.

PROOF. Let $(s, t) \in R_{\gamma,\delta}$, $(q, r) \in R_{\delta-\gamma,\delta-2\gamma}$. Then $H \ni [x_\gamma(s)x_\delta(t), x_{\delta-\gamma}(q) \times x_{\delta-2\gamma}(r)] = [x_\gamma(s), x_{\delta-\gamma}(q)x_{\delta-2\gamma}(r)] = [x_\gamma(s), x_{\delta-2\gamma}(r)] = x_{\delta-\gamma}(sr)x_\delta(rs^2)$, as claimed.

3.4. NOTATION. For a long root δ in Σ denote by A_δ the subring of k generated by $R''_{\delta-\gamma,\delta-2\gamma}R''_{\gamma,2\gamma-\delta}$, where $(\delta-\gamma, \delta-2\gamma)$ and $(\gamma, 2\gamma-\delta)$ are the admissible pairs (γ', δ') such that $2\gamma' - \delta' = \delta$. For a short root γ in Σ we denote by A_γ the subring of k generated by $R'_{\delta-\gamma,\delta}R'_{\gamma-\delta,2\gamma-\delta}$, where $(\delta-\gamma, \delta)$ and $(\gamma-\delta, 2\gamma-\delta)$ are the admissible pairs (γ', δ') with

$\delta' - \gamma' = \gamma$.

3.5. COROLLARY. *Let* (γ, δ) *be an admissible pair. Then:*
(i) $R'_{\delta-\gamma,\delta}$ *and* $R'_{\gamma,\delta}$ *are* A_δ*-modules;*
(ii) $R''_{\gamma,\delta}$ *and* $R''_{\gamma,2\gamma-\delta}$ *are* A^2_γ*-modules;*
(iii) A_δ *and* $A_{2\gamma-\delta}$ *are* A^2_γ*-modules;*
(iv) A_γ *and* $A_{\delta-\gamma}$ *are* A_δ*-modules.*

PROOF. Applying Lemma 3.3 (i) to the pair $(\delta - \gamma, \delta)$ instead of (γ, δ) we obtain $R'_{\gamma,\delta} \supset R'_{\delta-\gamma,\delta} R''_{\gamma,2\gamma-\delta}$. When we substitute this in the inclusion 3.3 (i), we obtain $R'_{\delta-\gamma,\delta} \supset R'_{\delta-\gamma,\delta}(R''_{\delta-\gamma,\delta-2\gamma} R''_{\gamma,2\gamma-\delta})$. Thus, $R'_{\delta-\gamma,\delta}$ is an A_δ-module. Replacing here $(\delta - \gamma, \delta)$ by (γ, δ) we prove (i).

To prove (ii) we apply Lemma 3.3 (ii) to the pair $(-\gamma, \delta - 2\gamma)$ instead of (γ, δ). We get $R''_{\delta-\gamma,\delta-2\gamma} \supset R''_{\delta-\gamma,\delta}(R'_{-\gamma,\delta-2\gamma})^2$. Substituting this in 3.3 (ii) we obtain $R''_{\delta-\gamma,\delta} \supset R''_{\delta-\gamma,\delta}(R'_{-\gamma,\delta-2\gamma} R'_{\gamma,\delta})^2$. Thus $R''_{\delta-\gamma,\delta}$ is an $A^2_{\delta-\gamma}$-module. Replacing here $(\delta - \gamma, \delta)$ by $(\delta - \gamma, \delta - 2\gamma)$ we see that $R''_{\delta-\gamma,\delta-2\gamma}$ is also an $A^2_{\delta-\gamma}$-module. Now it remains to replace $\delta - \gamma$ by γ (and keep δ the same) to obtain (ii).

Statements (iii) and (iv) are direct consequeces of (ii) and (i) respectively and the definition of the rings A_ε (see Notation 3.4).

3.6. LEMMA. *Let* (γ, δ) *be an admissible pair. Then there exist non-zero* c_1 *and* c_2 *in* k *such that*
(i) $R_\delta \supset c_1^2 R''_{\delta-\gamma,\delta-2\gamma}(R'_{\gamma,\delta})^2$.
(ii) $R_{\delta-\gamma} \supset c_2 R''_{\delta-\gamma,\delta-2\gamma} R'_{\gamma,\delta}$.

PROOF. Assume first that $\mathrm{card}(A_\varepsilon) = 2$ for some root ε in Σ. Since A_ε is a ring this implies that $A_\varepsilon = \{0, 1\}$. By Corollary 3.5 (iii) and (iv), A_ε is a module over A^2_φ, where φ is the root making an angle 45° with ε. Since $A_\varepsilon = \{0, 1\}$, it follows that $A^2_\varphi = \{0, 1\}$, hence $A_\varphi = \{0, 1\}$. Applying now the same argument to A_φ instead of A_ε and repeating it 7 times, we obtain that $A_\psi = \{0, 1\}$ for all roots ψ in Σ. The definition of A_ψ now implies that $\mathrm{card}(R'_{\gamma,\delta}) = \mathrm{card}(R''_{\gamma,\delta}) = 2$ for all admissible pairs (γ, δ). Since $R'_{\gamma,\delta} \supset R_\gamma \neq 0$ and $R''_{\gamma,\delta} \supset R_\delta \neq 0$ we see that $R'_{\gamma,\delta} = R_\gamma$ and $R''_{\gamma,\delta} = R_\delta$ for all admissible pairs (γ, δ). Therefore Lemma 3.3 reduces to our claim with $c_1 = c_2 = 1$.

Now we can assume that $\mathrm{card}(A_{\delta-\gamma}) > 2$. Pick $a \neq 0, 1$ in $A_{\delta-\gamma}$ and $b \neq 0$ in A_δ. By Corollary 3.5 (iii), $ba^2 \in A_\delta(A_{\delta-\gamma})^2 \subset A_\delta$. By Corollary 3.5 (i) and (ii), for any r in $R''_{\delta-\gamma,\delta-2\gamma}$ and any s in $R'_{\gamma,\delta}$, we have: ra^2, $ra^4 \in R''_{\delta-\gamma,\delta-2\gamma}$ and sb, $sba^2 \in R'_{\gamma,\delta}$.

Set $y(u, t) := (ut, tu^2) \in k \oplus k$. By Lemma 3.3, $y(u, t) \in R_{\delta-\gamma,\delta}$ if $u \in R'_{\gamma,\delta}$, $t \in R''_{\delta-\gamma,\delta-2\gamma}$. Therefore $y(sba^2, r)$, $y(sk, ra^2)$, $y(sb, ra^4) \in R_{\delta-\gamma,\delta}$. Since $x_{\delta-\gamma}(k)$

and $x_\delta(k)$ commute, $R_{\delta-\gamma,\delta}$ is an additive subgroup of $k \oplus k$. Therefore, $R_{\delta-\gamma,\delta} \ni y(sba^2, r) + y(sb, ra^2) = (0, rs^2a^2b^2(1+a)^2)$ and $R_{\delta-\gamma,\delta} \ni y(sba^2, r) + y(sb, ra^4) = (rsba^2(1+a^2), 0)$. Thus, our claim holds with $c_1 := ab(1+a) \neq 0$ and $c_2 := ba^2(1+a^2) \neq 0$.

3.7. COROLLARY. *For each pair (φ, ψ) of roots of the same length there exists a non-zero $c_{\varphi,\psi}$ in k such that*

(i) $R_\varphi \supset c_{\varphi,\psi}^2 R_\psi$ *if* $\varphi, \psi \in \Sigma_l$,

(ii) $R_\varphi \supset c_{\varphi,\psi} R_\psi$ *if* $\varphi, \psi \in \Sigma_s$.

PROOF. (i) Lemma 3.6 (i) applied to (γ, δ) gives $R_\delta \supset c_1^2 c_\gamma^2 R_{\delta-2\gamma}$, where $0 \neq c_\gamma \in R_\gamma \subset R'_{\gamma,\delta}$ (we used also the inclusion $R_{\delta-2\gamma} \subset R''_{\delta-\gamma,\delta-2\gamma}$).

This shows that $c_{\delta,\delta-2\gamma}$ exists (and can be taken to be $c_1 c_\gamma$). Note that δ was an arbitrary long root and $\delta - 2\gamma$ makes an angle $\pm 90°$ with δ if γ makes an angle $\pm 45°$ with δ. Thus, repeating the argument 3 times, we obtain (i).

(ii) We apply Lemma 3.6 (ii) to $(\delta - \gamma, \delta)$ to get that $R_\gamma \supset c_2 c_{2\gamma-\delta} R_{\delta-\gamma} =: c_{\gamma,\delta-\gamma} R_{\delta-\gamma}$. Similarly, $R_{\delta-\gamma} \supset c_{\delta-\gamma,-\gamma} R_{-\gamma}$, $R_{-\gamma} \supset c_{-\gamma,\gamma-\delta} R_{\gamma-\delta}$, $R_{\gamma-\delta} \supset c_{\gamma-\delta,\gamma} R_\gamma$.

Now we are prepared to complete our Proof of Theorem 1.1 for G of type $\boldsymbol{B}_2$.

PROOF OF THEOREM 1.1 FOR G OF TYPE $\boldsymbol{B}_2$ WHEN $\mathrm{char}(k) = 2$. For every root φ we pick a non-zero c_φ in R_φ.

By Lemma 3.6 and Corollary 3.7, $R_\alpha \supset c_1^2 R_{\alpha+2\beta}(R_{-\beta})^2 \supset c_1^2 c_{\alpha+2\beta,\alpha}^2 c_{-\beta,\alpha+\beta}^2 R_\alpha (R_{\alpha+\beta})^2$ and $R_{\alpha+\beta} \supset c_2 R_{\alpha+2\beta} R_{-\beta} \supset c_2 c_{\alpha+2\beta,\alpha}^2 c_{-\beta,\alpha+\beta} R_\alpha R_{\alpha+\beta}$.

Set $d_1 =: c_1 c_{\alpha+2\beta,\alpha} c_{-\beta,\alpha+\beta}$, $d_2 := c_2 c_{\alpha+2\beta,\alpha}^2 c_{-\beta,\alpha+\beta}$, $A := d_1 R_{\alpha+\beta}$, $B := d_2 R_\alpha$. Then the above inclusions become $d_2^{-1} B \supset d_2^{-1} B A^2$ and $d_1^{-1} A \supset d_1^{-1} AB$. Thus, $B \supset BA^2$, $A \supset AB$.

By Corollary 3.7, $d_2^{-1} c_{\delta,\alpha}^2 B \subset R_\delta \subset c_{\alpha,\beta}^{-2} d_2^{-1} B$ for $\delta \in \Sigma_l$ and $d_1^{-1} c_{\gamma,\alpha+\beta} A \subset R_\gamma \subset c_{\alpha+\beta,\gamma}^{-1} d_1^{-1} A$ for $\gamma \in \Sigma_s$. This proves the existence of a_ε, b_ε for all ε in Σ.

Consider now $A' := AA_\alpha A_{\alpha+2\beta} A_{-\alpha} A_{-\alpha-2\beta}$, $B' := B(A_\beta A_{\alpha+\beta} A_{-\beta} A_{-\alpha-\beta})^2$. Using Corollary 3.5 (iii) and (iv), we see that $B' \supset B'A'^2$ and $A' \supset A'B'$. It is clear that $A' \supset a_1 A$ and $B' \supset a_2 B$ for some non-zero a_i in k. Using Corollary 3.5 (i), (ii), Lemma 3.6, and the inclusions $B \supset BA^2$, $A \supset AB$, we see that $A' \subset b_1 A$ and $B' \subset b_2 B$ for non-zero b_i in k, $i = 1, 2$.

Replacing A, B by A', B', we get $AA_\delta \subset A$, $BA_\gamma^2 \subset B$ for all $\delta \in \Sigma_l$, $\gamma \in \Sigma_s$, and we still have $A^2 B \subset B$, $AB \subset A$ and (after appropriate change of a_ε, b_ε) $Aa_\gamma \subset R_\gamma \subset Ab_\gamma$, $Ba_\delta \subset R_\delta \subset Bb_\delta$ for all $\gamma \in \Sigma_s$, $\delta \in \Sigma_l$.

Using Lemma 1.3 with $N = 4$, $n = 1$, $m = 2$ and with $N = 4$, $n = 2$, $m = 1$, we find non-zero $a \in A$, $b \in B$ such that $R_\delta(aA)^2 \subset R_\delta$ and $B_\gamma(bB) \subset R_\gamma$ for all $\delta \in \Sigma_l$, $\gamma \in \Sigma_s$. Replacing A, B by aA, bB (and changing accordingly a_ε, b_ε) we gain the additional property: $R_\delta A^2 \subset R_\delta$, $R_\gamma B \subset R_\gamma$ for all $\gamma \in \Sigma_s$,

$\delta \in \Sigma_l$.

Now it is time to use Lemma 1.2 (ii) and then (iii) with $m = 2$ to obtain new A, B satisfying $A^2 \subset B \subset A$.

We do not loose the property that $AA_\delta \subset A$ and $BA_\gamma^2 \subset B$ for all $\delta \in \Sigma_l$, $\gamma \in \Sigma_s$. Since $A_\gamma \supset R_{\delta-2\gamma}R_{2\gamma-\delta}$ and $A_\gamma \supset R_{\delta-\gamma}R_{\gamma-\delta}$, we have, in particular, that $AR_\delta R_{-\delta} \subset A$ and $BR_\gamma^2 R_{-\gamma}^2 \subset B$ for all $\gamma \in \Sigma_s$, $\delta \in \Sigma_l$.

4. Proof of Theorem 1.1 for G of type $\boldsymbol{B}_n$ ($n \geqq 3$), $\boldsymbol{C}_n$ ($n \geqq 3$), and $\boldsymbol{F}_4$.

4.1. LEMMA. *Let φ, $\psi \in \Sigma$ have the same length. Then there exists a non-zero $c_{\varphi,\psi}$ in k such that $R_\varphi \supset c_{\varphi,\psi} R_\psi$. When G is of type $\boldsymbol{C}_n$, φ, $\psi \in \Sigma_l$, and $p = 2$, we can choose $c_{\varphi,\psi}$ in k^2.*

PROOF. If both φ and ψ lie in a subsystem of type $\boldsymbol{A}_2$ or $\boldsymbol{B}_2$, the first claim was established in Lemma 2.1 (ii) and Theorem 1.1 for G of type $\boldsymbol{B}_2$, respectively. In the general case there exist roots $\gamma_1, \cdots, \gamma_m$ in Σ of the same length as φ and ψ such that $\varphi = \gamma_1$, $\psi = \gamma_m$ and γ_i, γ_{i+1} lie in a subsystem Σ_i of type $\boldsymbol{A}_2$ or $\boldsymbol{B}_2$ for $i = 1, 2, \cdots, m-1$. Since the claim holds in every Σ_i, it holds in Σ as well, by induction on m. When G is of type $\boldsymbol{C}_n$, φ, $\psi \in \Sigma_l$, and $p = 2$, we can use Lemma 3.7 (i).

4.2. Now we pick $\alpha \in \Sigma_l$ and $\beta \in \Sigma_s$ which are simple roots in a subsystem of type $\boldsymbol{B}_2$. By Theorem 1.1, there are additive subgroups A and B of k and elements a_α, b_α, a_β, b_β of k such that $a_\alpha B \subset R_\alpha \subset b_\alpha B$, $a_\beta A \subset R_\beta \subset b_\beta A$ and, moreover,

$$AR_\alpha R_{-\alpha} \subset A\ , \qquad B(e(\Sigma)/p)(R_\beta R_{-\beta})^p \subset B, \tag{4.3}$$

$$AB \subset A\ , \qquad BA^p \subset B\ , \tag{4.4}$$

where $e(\Sigma) = 2$, and $p = 1$ or 2 (are integers depending on $\mathrm{char}(k)$).

By Lemma 4.1, $a_\delta B \subset R_\delta \subset b_\delta B$ and $a_\gamma A \subset R_\gamma \subset b_\gamma A$ for all $\delta \in \Sigma_l$ and $\gamma \in \Sigma_s$, where $a_\gamma := a_\beta c_{\gamma,\beta} \neq 0$, $b_\gamma := b_\beta c_{\beta,\gamma}^{-1}$, $a_\delta := a_\alpha c_{\delta,\alpha} \neq 0$, $b_\delta := b_\alpha c_{\alpha,\delta}^{-1}$.

Applying Lemma 1.3 with $N := \mathrm{card}(\Sigma_s)$, $n = 1$, $m = p$ and with $N := \mathrm{card}(\Sigma_l)$, $n = p$, $m = 1$, we find non-zero a in A and b in B such that $R_\delta(aA)^p \subset R_\delta$ and $R_\gamma(bB) \subset R_\gamma$ for all δ in Σ_l and γ in Σ_s.

Replacing A and B by Aa and Bb and changing a_ε and b_ε, we have (4.3), (4.4), and:

$$a_\delta B \subset R_\delta \subset b_\delta B \quad \text{and} \quad R_\delta A^p \subset R_\delta \quad \text{for all} \quad \delta \text{ in } \Sigma_l\ ; \tag{4.5}$$

$$a_\gamma A \subset R_\gamma \subset b_\gamma A \quad \text{and} \quad R_\gamma B \subset R_\gamma \quad \text{for all} \quad \gamma \text{ in } \Sigma_s\ . \tag{4.6}$$

Since every short root γ in Σ can be included as a simple root in a subsystem of type $\boldsymbol{B}_2$ or $\boldsymbol{A}_2$, we have $B_\gamma(2/p)(R_\gamma R_{-\gamma})^p \subset B_\gamma$ for an additive subgroup B_γ of k such that $u_\gamma B \subset B_\gamma \subset v_\gamma B$ with non-zero u_γ, v_γ in k (for

$\gamma = \beta$ we can take $B_\gamma = B$, see (4.3)). It follows that $B_\gamma C_\gamma \subset B_\gamma$, where C_γ is the subring of k generated by $(2/p)(R_\gamma R_{-\gamma})^p$. Let C_s be the product of all C_γ, $\gamma \in \Sigma_s$. Then $(BC_s)C_\gamma \subset BC_s$ for all γ in Σ_s. Replacing B by its additive subgroup generated by $BC_s c$ for some $c \neq 0$ (and changing a_δ, b_δ), we get $BC_\gamma \subset B$ for all γ in Σ_s, and we still have (4.3)-(4.6).

Similarly, for every long root δ in Σ there are non-zero u_δ, v_δ in k and an additive subgroup A_δ of k such that $A_\delta(R_\delta R_{-\delta}) \subset A_\delta$ and $u_\delta A \subset A_\delta \subset v_\delta A$, hence $A_\delta C_\delta \subset A_\delta$, where C_δ is the subring of k generated by $R_\delta R_{-\delta}$. Let C_l be the product of all C_δ, $\delta \in \Sigma_l$. Then $(AC_l)C_\delta \subset (AC_l)$ for all δ in Σ_l. Moreover, $u_l A \subset AC_l \subset v_l A$ for non-zero u_l, v_l in k. Replacing A by the additive subgroup generated by $AC_l v_l^{-1}$ (and changing a_γ, b_γ), we get $AC_\delta \subset A$ for all δ in Σ_l and we still have (4.3)-(4.6) and $BC_\gamma \subset B$ for all γ in Σ_s.

If Σ_l is connected (type $\boldsymbol{B}_n$, $n \geqq 3$, or $\boldsymbol{F}_4$), then there are long roots φ and ψ in Σ such that $\varphi + \psi$ is also in Σ_l. We have $[x_\varphi(t), x_\psi(u)] = x_{\varphi+\psi}(\pm tu)$ for all t, u in k, hence $R_{\varphi+\psi} \supset R_\varphi R_\psi$. By (4.5), $Bb_{\varphi+\psi} \supset R_{\varphi+\psi} \supset R_\varphi R_\psi \supset a_\varphi a_\psi BB$, so $cBB \subset B$ with $c := a_\varphi a_\psi / b_{\varphi+\psi} \neq 0$. By Lemma 1.2 (v) with $m := 2$, we can find a non-zero b_0 in B such that $(b_0 B)(b_0 B) \subset (b_0 B)$. Replacing B by $b_0 B$ (and changing a_δ, b_δ), we can assume that $BB \subset B$ (when Σ_l is connected).

Similarly, if Σ_s is connected (type $\boldsymbol{C}_n$, $n \geqq 3$, or $\boldsymbol{F}_4$), then there are $\varphi, \psi, \varphi + \psi \in \Sigma_s$, hence $R_{\varphi+\psi} \supset R_\varphi R_\psi$, so $A \supset cAA$ with $c := a_\varphi a_\psi / b_{\varphi+\psi} \neq 0$. By Lemma 1.2 (iv) with $m = 2$, $(a_0 A)(a_0 A) \subset a_0 A \neq 0$ for some a_0 in A. Replacing A by $a_0 A$ (and changing a_γ, b_γ) we have $AA \subset A$.

Still (4.3)-(4.6) hold and so do Theorem 1.1 (i) and (ii). To get the last part of Theorem 1.1 (iii), we use Lemma 1.2 (ii) and (iii) with $m = 2$ when $p = 2$, and we just replace both A and B by AB when $p = 1$ (and change a_ε, b_ε).

5. Proof of Theorem 1.1 for G of type $\boldsymbol{G}_2$. The root system Σ of type $\boldsymbol{G}_2$ consists of 6 short roots ($\pm\beta$, $\pm(\alpha + \beta)$, $\pm(2\beta + \alpha)$) and 6 long roots ($\pm\alpha$, $\pm(\alpha + 3\beta)$, $\pm(2\alpha + 3\beta)$), see Figure 2.

We use, sometimes without explicit reference, commutation relations given in [4, § 10, after Lemma 57].

For every root ε in Σ, we fix a non-zero c_ε in $R_\varepsilon := R_\varepsilon(H)$.

5.1. LEMMA. *There is a subring B of k such that $0 \neq R_\delta B \subset R_\delta$ and $BR_\delta R_{-\delta} \subset B$ for every δ in Σ_l.*

PROOF. It is a direct consequence of the results of Section 2 (namely, Theorem 1.1 for G of type $\boldsymbol{A}_2$) applied to the algebraic group generated by all long root subgroups (which is of type $\boldsymbol{A}_2$).

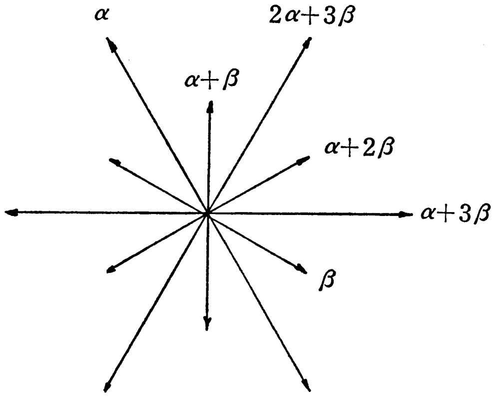

FIGURE 2. Root system of type G_2.

5.2. LEMMA. *For every short root γ in Σ there exist non-zero a_γ, b_γ, d_γ in k such that*:

(i) $3b_\gamma R_\gamma \subset B$; (ii) $a_\gamma B \subset R_\gamma$; (iii) $4d_\gamma R_\gamma^3 \subset B$.

PROOF. Let δ be a long root forming angle 30° with γ. Pick a non-zero b in B.

We have $[x_\gamma(t), x_{\delta-\gamma}(u)] = x_\delta(\pm 3tu)$ for all t, u in k. Therefore, $R_\delta \supset 3R_\gamma R_{\delta-\gamma} \supset 3c_{\delta-\gamma}R_\gamma$. By Lemma 5.1, $B \supset BR_{-\delta}R_\delta \supset bc_{-\delta}R_\delta$. Thus, (i) holds with $b_\gamma := bc_{-\delta}c_{\delta-\gamma} \neq 0$.

Part (ii) will be proved separately in the following three cases: $\mathrm{char}(k) \neq 2$; $\mathrm{card}(B) = 2$; $\mathrm{char}(k) = 2$ and $\mathrm{card}(B) > 2$.

When $\mathrm{char}(k) \neq 2$, we take any t in $R_{3\gamma-2\delta}$ and u in $R_{\delta-\gamma}$. Then $H \ni y(t, u) := [x_{3\gamma-2\delta}(t), x_{\delta-\gamma}(u)] = x_{2\gamma-\delta}(\pm tu)x_\gamma(\pm tu^2)x_\delta(\pm tu^3)x_{3\gamma-\delta}(\pm t^2u^3)$, hence $H \ni z(t, u) := y(-t, -u)^{-1}y(t, u) = x_\gamma(\pm 2tu^2)x_{3\gamma-\delta}(\pm 2t^2u^3)$ and $H \ni z(t, u)z(t, -u) = x_\gamma(\pm 4tu^2)$. Therefore, $R_\gamma \supset 4R_{3\gamma-2\delta}R^2_{\delta-\gamma} \supset 4Bc_{3\gamma-2\delta}c^2_{\delta-\gamma}$, so (ii) holds with $a_\gamma := 4c_{3\gamma-\delta}c^2_{\delta-\gamma} \neq 0$.

When $\mathrm{card}(B) = 2$, then $B = \{0, 1\}$ and we have (ii) with $a_\gamma := c_\gamma$.

When $\mathrm{char}(k) = 2$ and $\mathrm{card}(B) > 2$, we pick $b \neq 0, 1$ in B. For any a in $R_{-\delta}$, d in R_δ and u in R_γ we have: $H \ni y_1(a, d) := [x_\delta(d), [x_{-\delta}(a), x_\gamma(u)]] = [x_\delta(d), x_{\gamma-\delta}(ua)x_{2\gamma-\delta}(u^2a)x_{3\gamma-\delta}(u^3a)x_{3\gamma-2\delta}(u^3a^2)] = [x_\delta(d), x_{\gamma-\delta}(ua)][x_\delta(d), x_{3\gamma-2\delta}(u^3a^2)] = x_\gamma(uad)x_{2\gamma-\delta}(u^2a^2d)x_{3\gamma-2\delta}(u^3a^3d)x_{3\gamma-\delta}(u^3a^3d^2)x_{3\gamma-\delta}(u^3a^2d)$, hence $H \ni y_2(a, d) := y_1(ab, d)y_1(a, db^2)^{-1} = x_\gamma(uad(b+b^2))x_{3\gamma-2\delta}(u^3a^3d(b^3+b^2))x_{3\gamma-\delta}(u^3a^3d^2(b^3+b^4))$, and, finally, $H \ni y_2(ab^3, d)y_2(ab^2, db^3)y_2(ab, db^3)y_2(a, db^6) = x_\gamma(uad(b + b^2)(b^3 + b^5 + b^4 + b^6)) = x_\gamma(uadb^4(1 + b^4))$.

Thus, $R_\gamma \supset R_\gamma R_\delta R_{-\delta} b^4(1 + b^4) \supset c_\gamma(Bc_\delta)c_{-\delta}b^4(1 + b^4) = Ba_\gamma$, where $a_\gamma := c_\gamma c_\delta c_{-\delta} b^4(1 + b^4) \neq 0$.

To prove (iii) we consider the same $z(t, u) = x_\gamma(\pm 2tu^2)x_{3\gamma-\delta}(\pm 2t^2u^3) \in H$ as in the proof of (ii). Then $H \ni z(t, u)z(-t, u) = x_{3\gamma-\delta}(\pm 4t^2u^3)$. Therefore,

$R_{3\gamma-\delta}\supset 4R^2_{3\gamma-2\delta}R^3_{\delta-\gamma}\supset 4c^2_{3\gamma-2\delta}R^3_{\delta-\gamma}$. Since $bc_{\delta-3\gamma}R_{3\gamma-\delta}\subset BR_{3\gamma-\delta}R_{\delta-3\gamma}\subset B$ by Lemma 5.1, we get $4d_{\delta-\gamma}R^3_{\delta-\gamma}\subset B$ with $d := bc_{\delta-3\gamma}c^2_{3\gamma-2\delta}$. Similarly, $4d_\gamma R^3_\gamma\subset B$ with some $d_\gamma\neq 0$ in k.

5.3. LEMMA. *Let γ be a short root in Σ and δ form angle $\pm 150°$ with γ. Let $C_\gamma := 6R_\gamma R_{-\gamma}$. Then $R_\delta C_\gamma C_\gamma C_\gamma\subset R_\delta$.*

PROOF. Let $t, t_i\in R_\gamma$, $u\in R_\delta$, $s, s_i\in R_{-\gamma}$. Then $H\ni z_1(t) := [x_\delta(u), x_\gamma(t)] = x_{\delta+\gamma}(\pm tu)x_{\delta+2\gamma}(\pm t^2u)x_{\delta+3\gamma}(\pm t^3u)x_{2\delta+3\gamma}(\pm t^3u^2)$, hence $H\ni z_2(t_1) := z_1(t_1)^{-1}\times z_1(t_2)^{-1}z_1(t_1+t_2) = x_{\delta+3\gamma}(\pm 3(t_1+t_2)t_1t_2u)x_{\delta+2\gamma}(\pm 2t_1t_2u)x_{2\delta+3\gamma}(\pm u^2 3t_1t_2(t_1+t_2))\times x_{2\delta+3\gamma}(\pm 3u^2t_1t_2^2)$, hence $H\ni z_3 := z_2(t_1+t_3)z_2(t_1)^{-1}z_2(t_3)^{-1} = x_{\delta+3\gamma}(\pm 6t_1t_2t_3u)\times x_{2\delta+3\gamma}(\pm 6t_1t_2t_3u^2) = x_{\delta+3\gamma}(u')x_{2\delta+3\gamma}(\pm u'u)$, where $u' := \pm 6t_1t_2t_3u$. Similarly, $H\ni z_4(s) := [z_3, x_{-\gamma}(s)] = [x_{\delta+3\gamma}(u'), x_{-\gamma}(s)]$, hence $H\ni z_5(s_1) := z_4(s_1)^{-1}z_4(s_2)^{-1}\times z_4(s_1+s_2)$, $H\ni z_6(u) := z_5(s_1+s_3)z_5(s_1)^{-1}z_5(s_3)^{-1} = x_\delta(\pm 6s_1s_2s_3u')x_{2\delta+3\gamma}(\pm 6s_1s_2s_3u'^2)$. Finally, $H\ni z_6(u)z_6(-u)^{-1} = x_\delta(\pm 12s_1s_2s_3u')$, hence $R_\delta\ni 12s_1s_2s_3u' = \pm 72s_1s_2s_3\times t_1t_2t_3u$. Since we have this for arbitrary $t_i\in R_\gamma$, $s_i\in R_{-\gamma}$, $u\in R_\delta$, it follows that $R_\delta\supset C_\gamma C_\gamma C_\gamma R_\delta$.

PROOF OF THEOREM 1.1 FOR G OF TYPE $\boldsymbol{G}_2$ WHEN $\mathrm{char}(k)\neq 3$. By Lemma 5.2 (i), (ii), $a_\gamma B\subset R_\gamma\subset(3b_\gamma)^{-1}B$ for all short roots γ in Σ. By Lemma 1.3 with $A := B$, $n = m = 1$, $N := \mathrm{card}(\Sigma_s) = 6$, we have: $R_\gamma(bB)\subset R_\gamma$ for all short γ with some $b\neq 0$ in B. Replacing B by Bb and $(3b_\gamma b)^{-1}$ by b'_γ, we get $R_\gamma B\subset R_\gamma$, $R_\gamma\subset b'_\gamma B$ for all γ in Σ_s and we still have $R_\delta B\subset R_\delta$ and $BR_\delta R_{-\delta}\subset B$ for all δ in Σ_l.

Let γ be in Σ_s and δ make an angle $30°$ with γ. Then $3c_{\delta-2\gamma}c_{\delta-\gamma}\in 3R_{\delta-2\gamma}R_{\delta-\gamma}\subset R_{2\delta-3\gamma}$, $3c_\gamma c_{\delta-\gamma}\subset R_\delta$, and $3c_{-\gamma}c_{\delta-2\gamma}\in R_{\delta-3\gamma}$, hence $(3c_\gamma c_{\delta-\gamma})(3c_{-\gamma}c_{\delta-2\gamma})\in R_\delta R_{\delta-3\gamma}\subset R_{2\delta-3\gamma}$. So both $3c_{\delta-2\gamma}c_{\delta-\gamma}$ and $(3c_{\delta-2\gamma}c_{\delta-\gamma})(3c_\gamma c_{-\gamma})$ are in $R_{2\delta-3\gamma}$. Since $BR_{2\delta-3\gamma}R_{3\gamma-2\delta}\subset B$, we have $R_{2\delta-3\gamma}\subset Bd_1$ for some $d_1\neq 0$ in k. Writing $3c_{\delta-2\gamma}c_{\delta-\gamma} = b_1d_1$ and $(3c_{\delta-2\gamma}c_{\delta-\gamma})(3c_\gamma c_{-\gamma}) = b_2d_1$ with b_1 and b_2 in B, we see that $c_\gamma c_{-\gamma} = b_2/3b_1$. Since $c_\gamma c_{-\gamma}B\subset R_\gamma R_{-\gamma}\subset Rd_2$ for some $d_2\neq 0$ in k, we can use Lemma 1.3 with $n = m = N = 1$, $A = B$ and get $b_3R_\gamma R_{-\gamma}\subset b_3d_2B\subset c_\gamma c_{-\gamma}B$ for some $b_3\neq 0$ in B. Therefore $3b_1b_3R_\gamma R_{-\gamma}\subset 3b_1c_\gamma c_{-\gamma}B\subset b_2B\subset B$, hence $u_\gamma R_\gamma R_{-\gamma}\subset B$ for $0\neq u_\gamma := 3b_1b_3\in B$.

Let u be the product of all u_γ, $\gamma\in\Sigma_s$. Then $uR_\gamma R_{-\gamma}\subset B$ for all γ in Σ_s and $0\neq u\in B$. Replacing B by uB, we have $BBR_\gamma R_{-\gamma}\subset B$ for all γ in Σ_s. Still we have $R_\varepsilon B\subset R_\varepsilon$ for all ε in Σ and $BR_\delta R_{-\delta}\subset B$ for all δ in Σ_l.

If $\mathrm{char}(k) = 2$, we are done. Otherwise, $C_\gamma := 6R_\gamma R_{-\gamma}\neq 0$, and $R_\delta C_\gamma C_\gamma C_\gamma\subset R_\delta$ by Lemma 5.3, where δ makes angle $150°$ with γ, for any short root γ in Σ. Let $B_\gamma := R_\delta\cup R_\delta C_\gamma\cup R_\delta C_\gamma C_\gamma$. Then $B_\gamma C_\gamma\subset B_\gamma$. Since $R_\delta\subset d_3B$ for some $d_3\neq 0$ in k, we have $B^4B_\gamma\subset d_3B\cup d_3B\cup d_3B = d_3B$, hence $e_\gamma B_\gamma\subset B$ for some $e_\gamma\neq 0$ in k.

Let B' be the product of all $e_\gamma B_\gamma$, $\gamma\in\Sigma_s$. Then $B'\subset B$ and $B'C_\gamma\subset B'$

for all γ in Σ_s. Replacing B by its subring generated by BB' we have $BC_\gamma \subset B$ for all γ in Σ_s. Still we have $R_\varepsilon B \subset R_\varepsilon$ for all ε in Σ and $BR_\delta R_{-\delta} \subset B$ for all δ in Σ_l.

PROOF OF THEOREM 1.1 FOR G OF TYPE G_2 WHEN $\mathrm{char}(k) = 3$. Let B be as in Lemma 5.1. Since $3 = 0$ in k, the algebraic subgroup of G generated by all short root subgroups is also of type A_2. So $R_\gamma A \subset R_\gamma$ and $AR_\gamma R_{-\gamma} \subset A$ for some non-zero subring A of k and all short roots γ in Σ.

Using $R_\beta A \subset R_\beta$, $AR_\beta R_{-\beta} \subset A$, and Lemma 5.2 (ii), (iii) with $\gamma = \beta$, we get $A \supset c_1 B$ and $B \supset c_2 A^3$ with non-zero c_i in k.

Let B_0 (resp. A_0) be the additive subgroup of k generated by BA^3 (resp., by BA). Then $A_0 R_\varepsilon R_{-\varepsilon} \subset A_0$, $B_0 R_\delta R_{-\delta} \subset B_0 \supset B_0(R_\gamma R_{-\gamma})^3$ for all $\varepsilon \in \Sigma$, $\delta \in \Sigma_l$, $\gamma \in \Sigma_s$.

Since $(BA)^3 \subset BA^3 \subset BA$, it follows that $A_0^3 \subset B_0 \subset A_0$. From $c_1 B \subset A$ and $c_2 A^3 \subset B$ it follows that $BA \subset AAc_1^{-1} \subset Ac_1^{-1}$ and $BA^3 \subset BBc_2^{-1} \subset Bc_2^{-1}$, hence $c_2 B_0 \subset B$, $c_1 A_0 \subset A$. Since A and B are subrings of k, so are A_0 and B_0.

Using Lemma 1.3 with $N = 6$, $m = 3$, $n = 1$, $A = A_0$, $B = B_0$ and then with $N = 6$, $m = 1$, $n = 3$, $A = B_0$, $B = A_0$, we find non-zero a in A_0, b in B_0 such that $R_\gamma(bB_0) \subset R_\gamma$ and $R_\delta(aA_0)^3 \subset R_\delta$ for all $\gamma \in \Sigma_s$, $\delta \in \Sigma_l$. Let $c := a^3 b \in A_0^3 B_0 \subset B_0 B_0 \subset B_0 \subset A_0$. Then $R_\delta(A_0 c)^3 \subset R_\delta(A_0 a)^3 \subset R_\delta$ and $R_\gamma(cB_0) \subset R_\gamma(bB_0) \subset R_\gamma$. Moreover, $(A_0 c)^3 \subset B_0 c \subset A_0 c$.

Replacing A and B by $A_0 c$ and $B_0 c$, we get $A^3 \subset B \subset A$, $BB \subset B$, $AA \subset A$, $R_\delta A^3 \subset R_\delta$ for all $\delta \in \Sigma_l$ and $R_\gamma B \subset R_\gamma$ for all $\gamma \in \Sigma_s$. Moreover, $B(R_\gamma R_{-\gamma})^3 \subset B$ and $A(R_\varepsilon R_{-\varepsilon}) \subset A$ for all γ in Σ_s and ε in Σ.

6. Existence of groups described by Theorem 1.1. For any subsets A and B of k let $G^E(A, B)$ denote the subgroup of $G(k)$ generated by all $x_\gamma(a)$ and $x_\delta(b)$ with δ in Σ_l, γ in Σ_s, a in A, and b in B. In particular, $G^E(A, A) = G^E(A)$, Evidently, $R_\gamma(G^E(A, B)) \supset A$ and $R_\delta(G^E(A, B)) \supset B$ for all γ in Σ_s and δ in Σ_l.

6.1. THEOREM. *Let A and B be additive subgroups of k satisfying Theorem* 1.1 (iii), (iv). *Then $R_\gamma(G^E(A, B)) = A$ and $R_\delta((G^E(A, B)) = B$ for all long roots δ in Σ and short roots γ in Σ.*

To prove this theorem, we will exhibit a certain subgroup $G(A, B)$ of $G(k)$ such that $G(A, B) \supset G^E(A, B)$ and $R_\gamma(G(A, B)) = A$ and $R_\delta(G(A, B)) = B$ for all $\gamma \in \Sigma_s$ and $\delta \in \Sigma_l$.

We use here that G defined in the introduction over k may be defined as a Chevalley group scheme over the integers $\boldsymbol{Z}$ (see [17]). There is a matrix representation $G \subset SL_N$ such that G is defined by polynomial equations in the matrix entries with integral coefficients.

Given any commutative ring R (with or without 1) we define $G(R)$ as the group of all ring morphisms from the ring of regular functions on G vanishing at the identity of G to the ring R. If R is an ideal of a ring R' then $G(R)$ is the kernel of $G(R') \to G(R'/R)$. If R is a subring of k, the group $G(R)$ can be also defined as $G(k) \cap SL_N(R)$, where $SL_N(R)$ is the group of all matrices $(a_{i,j})$ with the determinant 1 such that $a_{i,j}$, $a_{i,i} - 1 \in R$ for all $i \neq j$.

The monomorphisms x_ε ($\varepsilon \in \Sigma$) are also defined over $\boldsymbol{Z}$. Moreover, the corresponding maps of the rings of regular functions are ring morphisms *onto* the polynomial ring $\boldsymbol{Z}[t]$. Therefore we have

6.2. LEMMA. *For any subring R of k and any root ε in Σ, we have $G^E(R) \subset G(R)$ and $R_\varepsilon(G(R)) = R$.*

This lemma implies Theorem 6.1 in the case $A = B$. In particular, the theorem holds when $p = 1$. To prove it when $p \neq 1$, we consider a few cases separately.

PROOF OF THEOREM 6.1 FOR G OF TYPES $\boldsymbol{F}_4$ AND $\boldsymbol{G}_2$. We assume that $\mathrm{char}(k) = 2$ in the case of type $\boldsymbol{F}_4$ and $\mathrm{char}(k) = 3$ in the case of type $\boldsymbol{G}_2$. Then there is a bijection $\rho\colon \Sigma \to \Sigma$ and a non-central isogeny (defined over $\boldsymbol{Z}/p\boldsymbol{Z}$) $\iota\colon G \to G$ such that $\rho(\Sigma_l) = \Sigma_s$, $\rho(\Sigma_s) = \Sigma_l$, $\iota x_\delta(t) = x_{\rho\delta}(\pm t)$, and $\iota x_\gamma(t) = x_{\rho\gamma}(\pm t^p)$) for all $\delta \in \Sigma_l$, $\gamma \in \Sigma_s$, and $t \in k$ (see, for example, [4]).

For any subrings A and B of k such that $A^p \subset B \subset A$, let $G(A, B)$ be the set of all g in $G(A)$ such that $\iota(g) \in G(B)$. Then $G(A, B) \supset G^E(A, B)$, $R_\delta(G(A, B)) = B$ (since $B \subset A$), and $R_\gamma(G(A, B)) = A$ (since $A^p \subset B$), for all $\gamma \in \Sigma_s$ and $\delta \in \Sigma_l$.

Therefore $R_\delta(G^E(A, B)) = B$ and $R_\gamma(G^E(A, B)) = A$.

6.3. "PSEUDO-ORTHOGONAL" GROUPS. To prove Theorem 6.1 for G of types $\boldsymbol{B}_n$ and $\boldsymbol{C}_n$ (with $p = 2$) we use some of ($*$, ε, A)-orthogonal groups of [8].

Namely, let $n \geqq 1$, Q a n by n integral matrix, A a commutative ring (with or without 1), B an A^2-submodule of A containing $2A$. Then let $O(Q; A, B)$ denote the set of matrices g in $GL_n(A)$ such that $g^*Qg - Q \in \mathscr{D}$, where $*$ means transposition and $\mathscr{D}$ is the set of all symmetric matrices over A with the diagonal entries in B.

Since $\mathscr{D}$ is an additive subgroup and $a^*ba \in \mathscr{D}$ for any $b \in \mathscr{D}$ and any matrix a over A, the set $O(Q; A, B)$ is a subgroup of $GL_n(A)$.

6.4. PROOF OF THEOREM 6.1 FOR G OF TYPES $\boldsymbol{B}_2$ WITH $AA \subset A$ AND $\boldsymbol{C}_n$ ($n \geqq 3$). Consider the ring of $2n$ by $2n$ integral matrices with the usual matrix units $e_{i,j}$ and the matrix $Q := \sum_{i=1}^{n} e_{i,2n+1-i}$. The group

$Sp_{2n} = \{g \in SL_{2n}: g^*(Q - Q^*)g = Q - Q^*\}$ can be considered as an affine group scheme over $\boldsymbol{Z}$. It is a simply connected almost simple Chevalley group scheme of type $\boldsymbol{C}_n$ ($\boldsymbol{C}_2 = \boldsymbol{B}_2$ when $n = 2$). The root elements with respect to the torus of diagonal matrices are $y_{i,2n+1-i}(t) := 1_{2n} + te_{i,2n+1-i}$ (correspond to the long roots) and $y_{i,j}(t) := 1_{2n} + te_{i,j} \pm te_{2n+1-j,2n+1-i}$ with $i + j < 2n + 1$ (correspond to the short roots).

Let now A and B be as in Theorem 6.1 and $\operatorname{char}(k) = 2$.

For any G of type $\boldsymbol{C}_n$ there is a bijection ρ from Σ to the set $\{(i, j): 1 \leqq i, j \leqq 2n, i + j \leqq 2n + 1\}$ and a central isogeny $\iota: Sp_{2n} \to G$ over $\boldsymbol{Z}$ such that $\iota y_{\rho\varepsilon}(t) = x_\varepsilon(t)$ for all ε in and all t. The kernel of ι is either trivial or isomorphic to the algebraic group of square roots of 1.

Let now A and B be as in Theorem 6.1, $AA \subset A$, and $\operatorname{char}(k) = 2$. Set $G(A, B) := \iota(Sp_{2n}(A, B))$, where $Sp_{2n}(A, B) := O(Q; A, B)$ (see 6.3). Then $G(A, B) \supset G^E(A, B)$, $R_\gamma(G(A, B)) = \{t \in k: y_{\rho\gamma}(t) \in O(Q; A, B)\} = A$, and $R_\delta(G(A, B)) = \{t \in k: y_{\rho\delta}(t) \in O(Q; A, B)\} = B$ for all γ in Σ_s and δ in Σ_l.

6.5. Proof of Theorem 6.1 for G of type $\boldsymbol{B}_2$ with $BB \subset B$ and type $\boldsymbol{B}_n$ ($n \geqq 3$). Let $Q := \sum_{i=1}^n e_{i,2n+1-i} + e_{2n+1,2n+1}$. For any commutative ring R, let $SO_{2n+1}(R) := O(Q; R, 0) \cap SL_{2n+1}(R)$ (see 6.3).

Then SO_{2n+1} can be considered as an affine group scheme over $\boldsymbol{Z}$. It is a simple Chevalley group of type $\boldsymbol{B}_n$. The root elements with respect to the torus of diagonal matrices are

$$z_{i,2n+1-i}(t) := 1_{2n+1} - t^2 e_{i,2n+1-i} + te_{2n+1,2n+1-i} - 2te_{i,2n+1}$$

(correspond to the short roots) and

$$z_{i,j}(t) := 1_{2n+1} + te_{i,j} - te_{2n+1-j,2n+1-i} \quad \text{with} \quad i + j < 2n + 1$$

(correspond to the long roots).

For any G of type $\boldsymbol{B}_n$ there is a bijection ρ from Σ to the set $\{(i, j): 1 \leqq i, j \leqq 2n, i + j \leqq 2n + 1\}$ and a central isogeny $\iota: G \to SO_{2n+1}$ over $\boldsymbol{Z}$ such that $\iota z_{\rho\varepsilon}(t) = x_\varepsilon(t)$ for all ε in Σ and all t. The kernel of ι is either trivial or isomorphic to the algebraic group of square roots of 1.

For any commutative ring R of characteristic 2, every matrix in $SO_{2n+1}(R)$ has the form $\begin{pmatrix} g & 0 \\ u & 1 \end{pmatrix}$, where g is in $Sp_{2n}(R)$ and u is a $2n$-row over R. It gives a non-central isogeny $\iota': SO_{2n+1} \to Sp_{2n}$ over $\boldsymbol{Z}/2\boldsymbol{Z}$. We have

$$\iota' z_{i,j}(t) = \begin{cases} y_{i,j}(t) & \text{when} \quad i + j < 2n + 1 \\ y_{i,j}(t^2) & \text{when} \quad i + j = 2n + 1 \end{cases}$$

for all t in k.

Let now A and B be as in Theorem 6.1 and $p = 2$. $\operatorname{char}(k) = 2$ and

$BB \subset B$. Set $G(A, B) := \{g \in G(A): \iota'\iota(g) \in Sp_{2n}(B, A^2)\}$ (see 6.4).

Then $G(A, B) \supset G^E(A, B)$, $R_\gamma(G(A, B)) = A$, and $R_\delta(G(A, B)) = B$ for all γ in Σ_s and δ in Σ_l.

6.6. PROOF OF THEOREM 6.1 FOR G OF TYPE $\boldsymbol{B}_2$ WITH $p = 2$. Let A' (resp. B') be the subring of k generated by A (resp. B). By 6.4, there is a subgroup H_1 of $G(k)$ such that $H_1 \supset G^E(A', B)$, $R_\gamma(H_1) = A'$, and $R_\delta(H_1) = B$ for all γ in Σ_s and δ in Σ_l. By 6.5, there is a subgroup H_2 of $G(k)$ such that $H_2 \supset G^E(A, B')$, $R_\gamma(H_2) = A$, and $R_\delta(H_2) = B'$ for all γ in Σ_s and δ in Σ_l.

Set $G(A, B) := H_1 \cap H_2$. Then $G(A, B) \supset G^E(A, B)$, $R_\gamma(G(A, B)) = A$, and $R_\delta(G(A, B)) = B$ for all γ in Σ_s and δ in Σ_l.

7. Full subsets of k. The following lemmas will be used in next sections.

7.1. LEMMA. (i) *If R is a full subset of k, then so is tR for any non-zero t in k;*

(ii) *if C is a full subring of k and $t_1, \cdots, t_m$ are non-zero elements of k, then there exists a non-zero c in C such that $t_i C \supset cC$ for $i = 1, \cdots, m$.*

PROOF. The statement (i) is evident; (ii) is contained in [7, Lemma 4].

7.2. LEMMA. *Let A and B be subsets of k such that A is full, $BA^2 \subset B$, and $Bk^2 = k$. Then:*

(i) *B is a full subset of k;*

(ii) *for any non-zero $t_1, \cdots, t_m$ in k, the intersection B' of all Bt_i is full and $B'k^2 = k$.*

PROOF. (i) Fix a non-zero b_0 in B. Given any t in k, we can write $tb_0 = bu^2$ with b in B and u in k. Since A is full in k, we can write $u = a_1/a_2$ with a_i in A and $a_2 \neq 0$. Then $t = ba_1^2/b_0 a_2^2$ with both ba_1^2 and $b_0 a_2^2$ in B. Thus, B is full.

(ii) Let z be in k. Since $Bk^2 = k$, we can write $z/t_i = b_i u_i^2$ for $i = 1, \cdots, m$ with b_i in B and u_i in k. Since A is full, $u_i = v_i/w_i$ with v_i, w_i in A. Let w be the product of all w_i. Then $zw^2 = t_i b_i v_i^2 (w/w_i)^2 \in t_i B$ for all $i = 1, \cdots, m$, so $zw^2 \in B'$, hence $z \in B'k^2$. Thus, $k = B'k^2$. It is clear that $B'A^2 \subset B'$. By (i), B' is full.

7.3. LEMMA. *Let F be a field but not an algebraic extension of a finite field. Then there exists a full subring A of k and a non-trivial homomorphism N of the multiplicative group of F into the additive group $\boldsymbol{Q}$ of the rational numbers such that $N(a) \geqq 0$ for all a in A.*

PROOF. Let X be a trancendence basis of F over its prime subfield

F_0. Let A_0 be the integers when X is empty, and $A_0 = F_0[X]$, the polynomial ring, otherwise. Let A be the integral closure of A_0 in F, i.e. the set of all roots in F of all monic polynomials in t with coefficients in A_0.

Fix $x \in X$ when X is not empty and set $x = 2 \in A_0$ otherwise. We define $N_0(a) = n$ for $0 \neq a \in A_0$, if x^n is the maximal power of x dividing a in A_0. We define $N_0(a_1/a_2) := N_0(a_1) - N_0(a_2)$ for non-zero a_i in A_0.

For any z in F, $z \neq 0$, let $f_z(t)$ be the monic polynomial in t, with coefficients in the field of fractions of A_0, of the minimal degree $\deg(z)$ such that $f_z(z) = 0$. We define $N(z) := N_0(f_z(0))/\deg(z)$; it is a rational number.

If $a \in A$, then $f_a(t) \in A_0[t]$, so $f_a(0) \in A$ hence $N(a) = N_0(f_a(0))/\deg(a) \geqq 0$.

For any non-zero z, z' in F we have $f_z(0)^{d/\deg(z)} f_{z'}(0)^{d/\deg(z')} = f_{zz'}(0)^{d/\deg(zz')}$ with some $d \neq 0$ divisible by $\deg(z)$, $\deg(z')$, $\deg(zz')$, so $N(zz') = N(z) + N(z')$. The homomorphism N is not trivial, because $N(x) = 1 \neq 0$.

Let us check now that A is full in F. For any $z \neq 0$ in F we can find a non-zero a_0 in A_0 such that $a_0 f_z(t) \in A_0[t]$. Let a be the leading coefficient of $a_0 f_z(t)$. Then $0 \neq a \in A$ and $a^{\deg(z)-1} f_z(t/a) a_0$ is a monic polynomial in t with coefficients from A_0 with a root za, so $za \in A$. Thus, A is full and Lemma 7.3 is proved.

For the rest of this section, $\mathrm{char}(k) = 2$.

7.4. NOTATION. For any finite subset $S \subset k$, let v_S denote the product of all y in S. In particular, $v_S = 1$ for the empty subset S.

7.5. LEMMA. *There is a set $Y_0 \subset k$ such that the all v_S, finite $S \subset Y_0$, form a basis for the vector space k over k^2.*

PROOF. We call a subset $Y \subset k$ algebraically almost independent (AAI), if all v_S, S a finite subset of Y, are linearly independent over k^2. (Note that k is an algebraic extension of k^2.) It is clear, that the union of any chain of AAI subsets of k is again AAI. Also the empty subset of k is AAI. By Zorn's lemma, there is a maximal AAI $Y_0 \subset k$.

Let V be the linear subspace of k over k^2 spanned by all v_S with finite $S \subset Y_0$. We have to prove that $V = k$.

Since Y_0 is a maximal AAI subset, for every $z \notin Y_0$ in k we have a linear relation (because $Y_0 \cup \{z\}$ is not AAI): $\sum a_S v_S + z \sum b_S v_S = 0$ with coefficients a_S, b_S in k^2, only finitely many of them $\neq 0$, both sums are taken over all finite $S \subset Y_0$, and the second sum $\neq 0$ (because Y_0 is AAI). Then $z = \sum a_S v_S / \sum b_S v_S = (\sum a_S v_S)(\sum b_S v_S)/a^2 \in VVk^2 \subset Vk^2 \subset V$, where $a := \sum b_S v_S \in V \subset k$. Thus, $V = k$.

7.6. LEMMA. *The following two statements are equivalent:*
(a) *$R = k$ for every full vector subspace $R \subset k$ over k^2;*
(b) *the dimension of k over k^2 is 1 or 2.*

PROOF. *Implication* (b) $\Rightarrow$ (a). Since R is full in k, $R \ni y_1 \neq 0$. If $k^2 = k$, then $R = Rk^2 = Rk \supset y_1 k = k$. When $k \neq k^2$, $R \ni y_2$ outside $y_1 k^2$ (otherwise, only elements of k^2 can be written as r_1/r_2 with $r_i \in R = y_1 k^2$). Therefore, $k^2 y_1 + k^2 y_2 = k$ when the dimension of k over k^2 is 2.

Implication (a) $\Rightarrow$ (b). We assume that the dimension of k over k^2 is larger than 2 and will find a full vector subspace $R \neq k$. First, we find Y_0 as in Lemma 7.5. Pick distinct x, y in Y_0, and let Y be the complement of $\{x, y\}$ in Y_0. Consider the linear subspace V spanned by all v_S with finite $S \subset Y$; V is a subfield of k, containing k^2.

Put $R := V + xV + yV$; $R \neq k$, because xy is outside R. We have to prove that R is full in k. Every z in $k - R$ can be written as $z = c_0(xy + c_1 x + c_2 y + c_3)$ with $c_i \in V$, $c_0 \neq 0$. Then $0 \neq r_1 := x + c_2 \in R$, $r_2 := c_0(yr_1^2 + x(c_3 + c_1 c_2) + c_1 r_1^2 + c_2(c_3 + c_1 c_2)) \in R$, and $z = r_2/r_1$.

7.7. LEMMA. (i) *If the dimension of k over k^2 is finite or countable, then, for any full subring C of k and any C^2-submodule B of k such that $Bk^2 = k$, B contains a full subring of k.*

(ii) *If the dimension of k over k^2 is uncountable, then there is a full subring A of k and an A^2-submodule B in A such that $Bk^2 = k$, $B \supset A^2$, and B does not contain any full subset of k closed under multiplication.*

PROOF. (i) Let $X \subset B$ be a basis for k over k^2. For every finite $S \subset X$ we can find a non-zero a_S in C such that $v_S a_S^2 \in B \cap C$ (see, Notation 7.4).

If X is finite, let c be the product of all a_S^2. Then $0 \neq c \in C^2$ and $v_S c \in B \cap C$ for all $S \subset X$ (recall that $BC^2 \subset B$). The C^2-submodule R of B generated by all $v_S c^2$ is a subring of k (namely, $(v_S c^2)(v_{S'} c^2) = (v_{S+S'} c^2)(v_{S \cap S'} c)^2 \in v_{S+S'} c^2 C^2 \subset R$, where $S + S' := S \cup S' - S \cap S'$).

We claim that R is full. Indeed, every y in k can be written as $y = \sum x t_x^2$ with t_x in k, where the summation is taken over x in X. Since C is full, we can find a non-zero a_0 in C such that $t_x a_0 \in C$ for all x in X (see, Lemma 7.1 (ii)). Then $yc^2 a_0^2 \in R$ and $0 \neq c^2 a_0^2 \in R$. So R is full.

If X is infinite, let us enumerate it, $X = \{u_1, u_2, \cdots\}$. For any $i \geqq 1$, let a_i be the product of all a_T with $T \subset \{u_1, \cdots, u_i\}$. Then, for any finite $S \subset X$, we have $\prod_{u_i \in S} (u_i a_i^2) = v_S \prod_{u_i \in S} a_i^2 \in B$, because $\prod a_i \in a_S C$ and $BC^2 \subset B$.

Therefore, the C^2-submodule R of B generated by a_0^2 and all $u_i a_i^2$

with u_i in X lies in B. As before, we see that R is full in k.

(ii) Find Y_0 as in Lemma 7.5. Since the dimension of k over k^2 is uncountable Y_0 is uncountable. By Jech [1], there is a function $r: Y_0 \times Y_0 \to \boldsymbol{Q}$ (with values in the rational numbers) with the property that for every function t: $Y_0 \to \boldsymbol{Q}$ there are x, y in Y_0 such that $r(x, y) > t(x)$ and $r(x, y) > t(y)$.

Find A and N as in Lemma 7.3 with $F = k$. For any finite $S \subset Y_0$ choose a non-zero a_S in A such that $v_S a_S \in A$ and $N(a_S) > 2r(x, y)$ in the case $S = \{x, y\}$ consisting of two distinct elements. Define B as the A^2-submodule in k generated by all $v_S a_S^2$ and A^2.

Let us check that $Bk^2 = k$. If we write any z in k as $\sum b_S^2 v_S$ with b_S in k and only finitely many $b_S \neq 0$, then we see that $za^2 \in R$ for some non-zero a in A hence $z \in Bk^2$.

Let now C be a full subset of k closed under multiplication. Since it is full in k, every x in Y_0 can be written as $x = c/c_x = cc_x/c_x^2$, where c and c_x are in C. So $C \ni cc_x = xc_x^2$ with $0 \neq c_x \in C$. Let $t(x) := N(c_x)$.

By the choice r: $Y_0 \times Y_0 \to \boldsymbol{Q}$ above, there are x, y in Y_0 such that $r(x, y) > t(x), t(y)$. For these x, y we have $N(c_x c_y) = N(c_x) + N(c_y) = t(x) + t(y) < 2r(x, y)$ and $C \supset CC \ni xc_x^2 yc_y^2 = xy(c_x c_y)^2$, so $xy(c_x c_y)^2$ is not in B by the definition of B, but it is in C. Thus, C is not contained in B.

8. Proof of Theorem 1.

8.1. LEMMA. *Let A and B be additive subgroups of k such that $A^p \subset B \subset A$, $BA^p \subset B$, $BA \subset A$, where p is as in Section 1. Assume that $BB \subset B$ when Σ_l is connected. Let $u \in k$, $b \in B$, and $\varphi, \varepsilon \in \Sigma$. Assume that $bu \in B^2$. Set $D_\varepsilon := B$ when ε is long and $D_\varepsilon := A$ otherwise. For any t in k we set $y(t) := [x_\varphi(u), x_\varepsilon(t)]$. Then*:

(i) $y(t) \in G^E(A, B)$ *if* $\varphi + \varepsilon \neq 0$ *and* t *is in* $b^4 D_\varepsilon$;

(ii) $y(t) \in G^E(A, B)$ *if* t *is in* $b^{16}(b-1)^2(b^2-1)D_\varepsilon$.

PROOF. We can assume that $y(t) \neq 1$ for some t in k (otherwise the statement is trivial). Pick a connected subsystem $\Sigma' \subset \Sigma$ of rank 2 containing both φ and ε. Then $\varphi + \varepsilon$ is in Σ' or else $\varphi + \varepsilon = 0$. We will prove (i) (and then (ii)) for the three possible cases, when Σ' is of type A_2, B_2, or G_2, separately.

Type $\boldsymbol{A}_2$ with $\varepsilon + \varphi \neq 0$. Then $y(b^2 t) = x_{\varepsilon+\varphi}(\pm b^2 tu) = [x_\varphi(b), x_\varepsilon(tbu)] \in G^E(A, B)$ for all t in D_ε, because $b \in B \subset D_\varphi$ and $tbu \in D_\varepsilon B^2 \subset D_\varepsilon$ for all t in D_ε. Thus, $y(b^2 D_\varepsilon) \subset G^E(A, B)$, hence $y(b^4 D_\varepsilon) \subset y(b^2 D) \subset G^E(A, B)$.

Type $\boldsymbol{B}_2$ with $\varepsilon + \varphi \neq 0$. If $\varepsilon, \varphi \in \Sigma_s$, then $y(t) = x_{\varepsilon+\varphi}(\pm 2tu) \in G^E(B)$ provided $t \in bA = bD_\varepsilon$. In particular, we can take any t in $b^4 D_\varepsilon = b^4 A \subset bA$ (the last inclusion follows from $BA \subset A$).

If $\varepsilon \in \Sigma_s$ and $\varphi \in \Sigma_l$, then $y(t) = x_{\varphi+\varepsilon}(\pm tu)x_{\varphi+2\varepsilon}(\pm t^2u) \in G^E(A, B)$ provided $t \in bA = bD_\varepsilon$ (because $Abu \subset AB^2 \subset A$ and $(bA)^2u = bA^2bu \subset BA^2B^2 \subset B = D_{\varphi+2\varepsilon}$). In particular, $y(t) \in G^E(A, B)$ for any t in $b^4A \subset bA$.

If $\varepsilon \in \Sigma_l$ and $\varphi \in \Sigma_s$, then $y(t) = x_{\varphi+\varepsilon}(\pm tu)x_{2\varphi+\varepsilon}(\pm tu^2) \in G^E(A, B)$ provided $t \in b^2B = b^2D_\varepsilon$ (because $(b^2B)u = bBbu \subset BBB^2 \subset A = D_{\varphi+\varepsilon}$ and $(b^2B)u^2 = B(bu)^2 \subset BB^4 \subset BB^2 \subset B = D_{2\varphi+\varepsilon}$). In particular, $y(t) \in G^E(A, B)$ for any t in $b^4D_\varepsilon = b^4B \subset b^2B$.

Type $\boldsymbol{G}_2$ with $\varphi + \varepsilon \neq 0$. If φ and ε are long, they lie in Σ_l' of type $\boldsymbol{A}_2$. Therefore, as shown above, $y(b^4D_\varepsilon) \subset y(b^2D_\varepsilon) \subset G^E(A, B)$.

If φ and ε are short and make the angle $\pm 60°$ then $y(t) = x_{\varphi+\varepsilon}(\pm 3ut) \in G^E(B)$ provided $t \in bA \supset b^4A = b^4D_\varepsilon$ (recall that $3A \subset B$).

If φ and ε are short and make the angle $\pm 120°$, then $y(t) = x_{\varphi+\varepsilon}(\pm 2tu)x_{2\varphi+\varepsilon}(\pm 3tu^2)x_{\varphi+2\varepsilon}(\pm 3t^2u) \in G^E(B) \subset G^E(A, B)$ provided $t \in b^2A \supset b^4A = b^4D_\varepsilon$ (because then $tu \in B$, $3tu^2 \subset 3A \subset B$, and $3t^2u \subset 3A \subset B$).

If φ is short and ε is long, then $y(t)^{-1} = x_{\varphi+\varepsilon}(\pm tu)x_{2\varphi+\varepsilon}(\pm u^2t)x_{3\varphi+\varepsilon}(\pm u^3t) \times x_{3\varphi+2\varepsilon}(\pm u^3t^2) \in G^E(B) \subset G^E(A, B)$ provided $t \in b^3B$ (because then $tu \in BB^2 \subset B$, $u^2t \subset B^4BB \subset B$, $u^3t \in B^6B \subset B$, $u^3t^2 \in B^3B^3B \subset B$). In particular, $y(t) \in G^E(A, B)$ when $t \in b^4B \subset b^3B$.

Finally, if φ is long and ε is short, then $y(t) = x_{\varphi+\varepsilon}(\pm tu)x_{\varphi+2\varepsilon}(\pm t^2u) \times x_{\varphi+3\varepsilon}(\pm ut^3)x_{2\varphi+3\varepsilon}(\pm u^2t^3) \in G^E(A, B)$ provided $t \in b^3A$ (because then $tu \in A = D_{\varphi+\varepsilon}$, $t^2u \in A = D_{\varphi+2\varepsilon}$, $t^3u \in B = D_{\varphi+3\varepsilon}$, and $t^3u^2 \in b^3B \subset B = D_{2\varphi+3\varepsilon}$). In particular, we can take any t in $b^4D_\varepsilon = b^4A \subset b^3A$.

Thus, (i) is proved in all cases. Since $b^4D_\varepsilon \subset D_\varepsilon$ for all ε in Σ, (i) can be stated also as follows: the subgroup $H := x_\varphi(u)^{-1}G^E(A, B)x_\varphi(u)$ contains all $x_\varepsilon(b^4D_\varepsilon)$ with $\varepsilon \neq -\varphi$. Now we want to prove (ii), i.e., $H \supset x_\varepsilon(b^{16}(b-1)^2(b^2-1)D_\varepsilon)$ for all ε. When $\varepsilon + \varphi \neq 0$, this has been proved, because $b^{16}(b-1)^2(b^2-1)D_\varepsilon \subset b^4D_\varepsilon$. So we assume that $\varepsilon = -\varphi$ and consider again separately the cases when Σ' is of type $\boldsymbol{A}_2$, $\boldsymbol{B}_2$, or $\boldsymbol{G}_2$.

Type $\boldsymbol{A}_2$ with $\varepsilon = -\varphi$. Pick α and β in Σ' such that $\alpha + \beta = \varepsilon$. From $H \supset x_\alpha(b^4D_\alpha), x_\beta(b^4D_\beta)$ it follows that $H \supset [x_\alpha(b^4D_\beta), x_\beta(b^4D_\beta)] = x_\varepsilon(b^8D_\alpha D_\beta) = x_\varepsilon(b^8D_\varepsilon D_\varepsilon) \supset x_\varepsilon(b^9D_\varepsilon) \supset x_\varepsilon(b^{16}(b-1)^2(b^2-1)D_\varepsilon)$.

Type $\boldsymbol{B}_2$ with $\varepsilon = -\varphi$. Pick α in Σ_l' and β in Σ_s' such that $\varepsilon = \alpha + \beta$ when ε is short and $\varepsilon = \alpha + 2\beta$ when ε is long. Then $H \ni z(v, w) := [x_\alpha(v), x_\beta(w)] = x_{\alpha+\beta}(\pm vw)x_{\alpha+2\beta}(\pm vw^2)$ provided $v \in b^4B = b^4D_\alpha$ and $w \in b^4A = b^4D_\beta$. Therefore, $H \ni z(b^4c, b^7)z(b^6c, b^5)^{-1} = x_{\alpha+2\beta}(\pm c(b^{18} - b^{16}))$ for all c in B and $H \ni z(b^7, db^4)z(b^5, db^5)^{-1} = x_{\alpha+\beta}(\pm d(b^{11} - b^{10}))$ for all d in A.

Thus, $R_{\alpha+2\beta}(H) \supset B(b^{18} - b^{16}) = D_{\alpha+2\beta}b^{16}(b^2-1) \supset D_{\alpha+2\beta}b^{16}(b^2-1)(b-1)^2$ and $R_{\alpha+\beta}(H) \supset A(b^{11} - b^{10}) = D_{\alpha+\beta}b^{10}(b-1) \supset D_{\alpha+\beta}b^{16}(b-1)^2(b^2-1)$.

Type $\boldsymbol{G}_2$ with $\varepsilon = -\varphi$. If ε is long, we can include ε and φ in a subsystem of type $\boldsymbol{A}_2$ (namely, Σ_l'), so $H \supset x_\varepsilon(Bb^9) = x_\varepsilon(D_\varepsilon b^9) \supset x_\varepsilon(D_\varepsilon(b -$

$1)^2(b^2 - 1)b^{16})$.

If ε is short, we find α in Σ'_l and β in Σ'_s such that $\varepsilon = \alpha + \beta$. Then $H \supset x_\alpha(b^4 B)$, $x_\beta(Ab^4)$, hence $H \ni z_1(v, w) := [x_\alpha(v), x_\beta(w)] = x_{\alpha+\beta}(\pm vw) \times x_{\alpha+2\beta}(\pm vw^2) x_{\alpha+3\beta}(\pm vw^3) x_{2\alpha+3\beta}(\pm v^2 w^3)$ for any v in $b^4 B$ and w in $b^4 A$. Therefore, for such v and w, we have $H \ni z_2(v, w) := z_1(vb^2, w) z_1(v, wb)^{-1} = x_{\alpha+\beta}(\pm vw(b^2 - b)) x_{\alpha+3\beta}(\pm vw^3(b^2 - b^3)) x_{2\alpha+3\beta}(\pm v^2 w^3(b^4 - b^3))$, so $H \ni z_3(v, w) := z_2(vb^3, w) z_2(v, wb^2)^{-1} = x_{\alpha+\beta}(\pm vw(b^2 - b)(b^3 - b^2)) x_{\alpha+3\beta}(\pm vw^3(b^2 - b^3)(b^3 - b^6))$, hence $H \ni z_3(vb^3, w) z_3(v, wb)^{-1} = x_{\alpha+\beta}(\pm vw(b^2 - b)(b^3 - b^2)(b^3 - b))$.

Thus, $R_\varepsilon(H) \supset (b^4 B)(b^4 A)(b^2 - b)(b^3 - b^2)(b^3 - b) = ABb^{12}(b-1)^2(b^2-1) \supset D_\varepsilon b^{16}(b-1)^2(b^2-1)$, because $AB \supset Ab^4 = D_\varepsilon b^4$.

8.2. COROLLARY. *Let A and B be as in Lemma 8.1. Assume that B is full and $Bk^2 = k$. Then for any g in $G^E(k)$ there is a non-zero b_g in B such that $gG^E(A, B)g^{-1} \supset G^E(Ab_g^2, Bb_g^2)$.*

PROOF. If $\mathrm{card}(B) \leqq 9$, then $B = A = k$ and $G^E(k) = G^E(A, B) \ni g$, so we can take $b_g = 1$.

Otherwise we pick some $b_1 \neq b_1^9$ in B.

Consider first the case $g = x_\varphi(u)$ with φ in Σ and u in k. Since $Bk^2 = k$ and B is full, we can find b_i in B such that $u = b_2(b_3/b_4)^2$ and $b_2 b_4 \neq 0$. For $b_5 := b_2^3 b_4^2 \in BB^2B^2 \subset BB^2 \subset B$ we have $b_5 \neq 0$ and $b_5 u = (b_3 b_2^2)^2 \in B^2$.

Let $b := b_5$ when $b_5 \neq \pm 1$ and $b := b_5 b_1^4$ otherwise. Then $bu \in B^2$ and $0 \neq b \in B$. Set $b_0 := b^8(b-1)(b^2-1) \in B$. Then $b_0 \neq 0$ and, by Lemma 8.1, $gG^E(A, B)g^{-1} =: H \supset G^E(Ab_0^2/(b^2-1),\ Bb_0^2/(b^2-1))$. Since $B(b^2-1) \subset B$ and $A(b^2-1) \subset A$, it follows that $H \supset G^E(Ab_0^2, Bb_0^2)$. Thus, we can take $b_g = b_0$ in the case $g = x_\varphi(u)$.

In the general case we write $g = g_1 \cdots g_m$ and proceed by induction on m, where every g_i is a root element. The case $m = 1$ has been considered, so let $m \geqq 2$. By induction, for $g' = g_1^{-1} g$ there is a non-zero b' in B such that $g'G^E(A, B)g'^{-1} \supset G^E(Ab'^2, Bb'^2)$. Since Ab'^2 and Bb'^2 enjoy the same properties as A and B, there is a non-zero b'' in Bb'^2, such that $g_1 G^E(Ab'^2, Bb'^2) g_1^{-1} \supset G^E(Ab'^2 b''^2, Bb'^2 b''^2)$. Set $b_g := b'^2 b'' \in b'^4 B \subset B$ to obtain the statement. $gG^E(A, B)g^{-1} \supset G^E(Ab'^2 b''^2, Bb'^2 b''^2) \supset G^E(Ab_g^2, Bb_g^2)$.

8.3. LEMMA. *In the situation of Theorem 1.1, assume that B is full and $Bk^2 = k$ (both conditions evidently do not depend on the choice of A and B). Then there is a non-zero b_0 in B such that $b_0 B \subset R_\delta \subset b_0^{-1} B$ and $b_0 A \subset R_\gamma \subset b_0^{-1} A$ for all δ in Σ_l and γ in Σ_s.*

PROOF. If $BB \subset B$, then, by Lemma 7.1 (ii) with $C = B$, we can find a non-zero b_0 in the intersection of B with all $Ba_\varepsilon \cap Bb_\varepsilon^{-1}$, where $\varepsilon \in \Sigma$. Therefore, $b_0 B \subset a_\delta B \subset R_\delta \subset Bb_\delta \subset Bb_0^{-1}$ and $b_0 A \subset a_\gamma A \subset R_\gamma \subset Ab_\gamma \subset Ab_0^{-1}$ for all δ in Σ_l and γ in Σ_s.

If BB is not contained in B, then Σ is of type C_n ($n \geqq 2$), and $p = 2$. Fix a long root α in Σ. By Lemma 1.3, $b_\alpha B(aA)^2 \subset a_\alpha B \subset R_\alpha$ for some $a \neq 0$ in A. In particular, $a^4 b_\alpha B \subset R_\alpha$.

By Lemma 4.1, $R_\varphi \supset c_{\varphi,\psi} R_\psi$ with $0 \neq c_{\varphi,\psi} \in k^2$ for all φ, ψ in Σ_l. Let C be the ring generated by B. Then $B \subset C \subset A$, $CA \subset A$, and $BC^2 \subset B$.

Since C is full in k, C^2 is full in k^2. By Lemma 7.1 (ii) there is a non-zero c in C such that $c^2 \in c_{\delta,\alpha} a^4 C^2 \cap c_{\alpha,\delta} C^2$ for all δ in Σ_l and $c^2 \in a_\gamma^2 C^2 \cap b_\gamma^{-2} C^2$ for all γ in Σ_s.

So for such δ and γ we have $cA \subset (a_\gamma C)A \subset a_\gamma A \subset R_\gamma \subset b_\gamma A \subset (c^{-1}C)A \subset c^{-1}A$ and $b_\alpha c^2 B \subset b_\alpha (c_{\delta,\alpha} a^4 C^2) B \subset b_\alpha c_{\delta,\alpha} a^4 B \subset c_{\delta,\alpha} R_\alpha \subset R_\delta \subset c_{\alpha,\delta}^{-1} R_\alpha \subset Bb_\alpha / c_{\alpha,\delta} \subset Bb_\alpha (C^2 c^{-2}) \subset Bb_\alpha c^{-2}$.

Since $Bk^2 = B$ and B is full, there are non-zero b_i in B such that $b_\alpha = b_1(b_2/b_3)^2 = b_4/b_3^2$, where $b_4 := b_1 b_2^2 \in BB^2 \subset B$. Set $b_0 := b_4 c^2 b_3^2 \in BC^2B^2 \subset B$. Then $b_0 A \subset cA \subset R_\gamma \subset c^{-1}A \subset b_0^{-1}A$ for all γ in Σ_s and $b_0 B = b_\alpha b_3^4 c^2 B \subset b_\alpha e^2 B \subset R_\delta \subset Bb_\alpha c^{-2} = Bb_4^2 b_0^{-1} \subset Bb_0^{-1}$ for all δ in Σ_l.

8.4. THEOREM. *Let A and B be additive subgroups of k satisfying Theorem* 1.1 (iii), (iv). *Assume that B is full and $Bk^2 = k$. Then for any g in $G(k)$ there is a non-zero b_0 in B such that $gG^E(A, B)g^{-1} \supset G^E(Ab_0, Bb_0)$. In particular, $G^E(A, B)$ is full.*

PROOF. Every g in $G(k)$ can be written as $g = hg'$ with h in $T(k)$ and g' in $G^E(k)$ (see, Tits [5] and Borel-Tits [9, Prop. 6.2]). Set $H' := g'G^E(A, B)g'^{-1}$ and $H := gG^E(A, B)g^{-1} = hH'h^{-1}$.

By Corollary 8.2, $H' \supset G^E(Ab^2, Bb^2)$ with $0 \neq b \in B$. Since $h \in T(k)$, we have $R_\varepsilon(H) = R_\varepsilon(H')t_\varepsilon$ for all ε in Σ with non-zero t_ε in k. Therefore $R_\varepsilon(H) \supset D_\varepsilon b^2 t_\varepsilon$, where $D_\varepsilon := B$ when $\varepsilon \in \Sigma_l$ and $D_\varepsilon := A$ when $\varepsilon \in \Sigma_s$.

Applying Lemma 8.3 to H, we find additive subgroups A' and B' of k and a non-zero b' in B' such that $b'B' \subset R_\delta(H) \subset B'b'^{-1}$ and $b'A' \subset R_\gamma(H) \subset A'b'^{-1}$ for all δ in Σ_l and γ in Σ_s.

Fix α in Σ_l and β in Σ_s. Then $R_\delta(H) \supset b'B' \supset b'^2 R_\alpha(H) \supset b'^2 b^2 t_\alpha B$ and $R_\gamma(H) \supset b'A' \supset b'^2 R_\beta(H) \supset b'^2 b^2 t_\beta A$ for all δ in Σ_l and γ in Σ_s.

Since B is full and $Bk^2 = k$, there are non-zero b_1 and b_2 in B such that $b_3 := b_1 b'^2 t_\beta \in B$ and $b_4 := b_2^2 b'^2 t_\alpha \in B$. Set $b_0 := b_4 b_3^2 b^2 \in BB^2B^2 \subset BB^2 \subset B$.

Then $R_\delta(H) \supset b'^2 b^2 t_\alpha B \supset b'^2 b^2 t_\alpha (b_2^2 b_3^2 B) = b_0 B$ and $R_\gamma(H) \supset b'^2 b^2 t_\beta A \supset b'^2 b^2 t_\beta (b_3 b_4 b_1 A) = b_0 A$ for all δ in Σ_l and γ in Σ_s. Thus $H \supset G^E(Ab_0, Bb_0)$ with $0 \neq b_0 \in B$.

PROOF OF THEOREM 1. Let A be a full subring of k. Set $B := A$. Then Theorem 1.1 (iii), (iv) are satisfied. Moreover, given any u in k we can write $u = b_1/b_2$ with b_i in B and $b_2 \neq 0$, hence $u = b_1 b_2 b_2^{-2} \in Bk^2$. Thus, $Bk^2 = k$. By Theorem 8.4, $G^E(A) = G^E(A, B)$ is full.

9. Proof of Theorems 2 and 3.

9.1. LEMMA. *Let H be a full subgroup of $G(k)$. Then*
(i) *$R_\varepsilon(H)$ is full, if ε lies in a subsystem $\Sigma' \subset \Sigma$ of type $\boldsymbol{A}_2$;*
(ii) *$R_\gamma(H)$ is full for any short root γ in Σ.*

PROOF. (i) We apply an argument of [7]. Namely, we find a root φ in Σ' such that $\varphi + \varepsilon$ is in Σ' too. Fix non-zero c_1 in $R_{-\varphi}(H)$ and c_2 in $R_\varphi(H)$. Take an arbitrary t in k. Since H is full, $H \ni x_\varphi(t)x_\varepsilon(u)x_\varphi(t)^{-1} = x_{\varepsilon+\varphi}(\pm tu)x_\varepsilon(u) =: g$ for a non-zero u in k. Therefore, $H \ni [g, x_{-\varphi}(c_1)] = x_\varepsilon(\pm tuc_1)$ and $H \ni [[g, x_\varphi(c_2)], x_{-\varphi}(c_1)] = [x_{\varepsilon+\varphi}(uc_2), x_{-\varphi}(c_1)] = x_\varepsilon(\pm uc_1c_2)$. Thus, $R_\varepsilon(H)$ contains both $tuc_1 := a_1$ and $uc_1c_2 := a_2 \neq 0$. Since $a_1a_2^{-1} = tc_2^{-1}$ can be an arbitrary element of k, $R_\varepsilon(H)$ is full in k.

(ii) If Σ contains a system of type $\boldsymbol{A}_2$, then we can use (i) and, by Theorem 1.1, conclude that A and all $R_\gamma(H)$ with γ in Σ_s are full. Otherwise, Σ is of type $\boldsymbol{B}_2$.

Let δ in Σ make an angle 45° with γ. Since H is full, for any t in k there exists a non-zero u in k such that $H \ni x_{\delta-2\gamma}(t)x_\gamma(u)x_{\delta-2\gamma}(-t) = x_\gamma(u)x_{\delta-\gamma}(\pm tu)x_\delta(\pm tu^2) =: g$, where the signs $\pm$ depend on γ and δ.

Now we pick non-zero c_1 in $R_{\delta-2\gamma}(H)$ and c_2 in $R_{2\gamma-\delta}(H)$. We have successively $H \ni [x_{\delta-2\gamma}(c_1), g] = [x_{\delta-2\gamma}(c_1), x_\gamma(u)] = x_{\delta-\gamma}(\pm c_1u)x_\delta(\pm c_1u^2) =: g'$; $H \ni [x_{2\gamma-\delta}(c_2), g'] = x_\gamma(\pm c_1c_2u)x_\delta(\pm c_1^2c_2u^2)$; and $H \ni [x_{2\gamma-\delta}(c_2), g] = x_\gamma(\pm c_2tu) \times x_\delta(\pm c_2t^2u^2)$.

Thus, $R_{\gamma,\delta} \ni (c_2c_1u, \pm c_2c_1^2u^2), (c_2tu, \pm c_2t^2u^2)$, hence $R'_{\gamma,\delta} \ni c_2c_1u =: a_2$ and $R'_{\gamma,\delta} \ni c_2tu =: a_1$ (see, the beginning of Section 3 for notation). Since $a_1/a_2 = t/c_1$ is arbitrary, $R'_{\gamma,\delta}$ is full.

By Corollary 3.2 (i) it follows that $R_\gamma(H)$ is full when $2 \neq 0$ in k. If $\mathrm{char}(k)=2$, $R_{\delta-\gamma}(H)$ is full by Lemma 3.6 (ii). Replacing here (γ, δ) by $(\delta - \gamma, \delta)$, we obtain that $R_\gamma(H)$ is full.

9.2. LEMMA. *Let H be a full subgroup of $G(k)$. Then $R_\varepsilon(H)$ is full and $R_\varepsilon(H)k^2 = k$ for any root ε in Σ.*

PROOF. Find A and B as in Theorem 1.1. Since $a_\varepsilon B \subset R_\varepsilon(H)$ for every ε in Σ with $a_\varepsilon \neq 0$, the statement of Lemma 9.2 will follow from: B is full and $Bk^2 = k$. By Lemma 9.1 (ii), A is full.

If $B = A$ (for example, $p = 1$), then $BB = BA \subset A = B$, so B is a subring of k. When B is a full subring of k (for example, if $B = A$), every t in k can be written as $t = b_1/b_2 = (b_1b_2)(b_2)^{-2} \in Bk^2$ with b_i in B, $b_2 \neq 0$, hence $k = Bk^2$.

If B is not a full subring of k, then (using Lemma 9.1 (i) to exclude type $\boldsymbol{D}_n$ and $\boldsymbol{G}_2$) G is of type $\boldsymbol{C}_n$ ($n \geqq 2$) and $p = 2$.

Then we pick a subsystem $\Sigma' \subset \Sigma$ of type $\boldsymbol{B}_2$ and an admissible pair (γ, δ) in Σ'. Take an arbitrary t in k and set $g := x_\delta(t)$.

Applying Theorem 1.1 to $H' := gHg^{-1}$, we find a non-zero u in k such that $R_\gamma(H') \subset uR_{-\gamma}(H')$. Then $a_\gamma A \subset R_\gamma(H) = R_\gamma(H') \subset uR_{-\gamma}(H')$. Since A is full, $a_{-\gamma}u/a_\gamma = a_1/a_2$ with non-zero a_i in A. Then $0 \neq v := a_\gamma a_1/u = a_2 a_{-\gamma} \in Aa_\gamma/u \cap Aa_{-\gamma} \subset R_{-\gamma}(H') \cap R_{-\gamma}(H)$, hence $x_{-\gamma}(v) \in H \cap H'$.

Therefore $H = g^{-1}H'g \ni g^{-1}x_{-\gamma}(v)g =: g'$ and $H \ni g'x_{-\gamma}(v)^{-1} = [g^{-1}, x_{-\gamma}(v)] = x_{\delta-\gamma}(tv)x_{\delta-2\gamma}(tv^2)$, hence $R''_{\delta-\gamma,\delta-2\gamma} \ni tv^2$.

By Lemma 3.6 (i), $R_\delta(H) \ni c^2 t$ for some $c \neq 0$ in k (c depends on H and t), so $t \in R_\delta(H)k^2$. Thus, $R_\delta(H)k^2 = k$, i.e. $Bk^2 = k$. By Lemma 7.2 (using that B is a module over the ring generated by A^2), B is full, so $R_\varepsilon(H)$ is full for every root ε in Σ.

9.3. THEOREM. *Let H be a full subgroup of $G(k)$. Then there are additive subgroups A and B of k and a non-zero c in B such that B is full, $Bk^2 = k$, and Theorem* 1.1 (i)-(iv) *hold with $a_\varepsilon = 1$ and $b_\varepsilon = c^{-1}$ for all ε in Σ.*

PROOF. Find A and B by Theorem 1.1. By Lemma 9.2, B is full and $Bk^2 = k$. By Lemma 8.3, there is a non-zero b_0 in B such that $b_0 B \subset R_\delta \subset Bb_0^{-1}$ and $b_0 A \subset R_\gamma \subset Ab_0^{-1}$ for all δ in Σ_l and γ in Σ_s. Set $A' := Ab_0$, $B' := Bb_0$, and $c := b_0^2 \in B'$. Replacing A and B by A' and B', we obtain our statement.

9.4. COROLLARY. *Let H be a subgroup of $G(k)$. Then the following three statements are equivalent*: (a) *H is full*; (b) *$H \supset G^E(B)$ for a full additive subgroup B of k such that $BB^2 \subset B$ and $Bk^2 = k$*; (c) *$H \supset G^E(R)$ for a full subset R of k such that $Rk^2 = k$.*

PROOF. By Theorem 9.3, (a) implies (b). Clearly, (b) implies (c). Now assume (c). Find A and B as in Theorem 1.1. Since $R \subset R_\delta(H) \subset b_\delta B$ for any δ in Σ_l with $b_\delta \neq 0$, our assumption on R implies that B is full and $Bk^2 = k$. By Lemma 8.3, $H \supset G^E(Ab_0, Bb_0)$ with $0 \neq b_0 \in B$. By Theorem 8.4, H is full. Thus, (c) implies (a).

9.5. COROLLARY. *Let H be a subgroup of $G(k)$. If G is of type $\boldsymbol{C}_n$, assume that* $\operatorname{char}(k) \neq 2$. *Then the following three statements are equivalent*:

(a) *H is full;*
(b) *$H \supset G^E(B)$ for a full subring B of k;*
(c) *$H \supset G^E(R)$ for a full subset R of k.*

PROOF. By Theorem 9.3, (a) implies (b). The implication (b) $\Rightarrow$ (c) is trivial. Now assume (c). Since we excluded type $\boldsymbol{C}_n$ with $p = 2$, we can find A, B as in Theorem 1.1 with $BB \subset B$. Since $R \subset R_\delta(H) \subset b_\delta B$ with $\delta \in \Sigma_l$, $b_\delta \neq 0$, it follows that B is a full subring of k. So $Bk^2 = k$. In view of the implication 9.4 (c) $\Rightarrow$ 9.4 (a), H is full.

9.6. COROLLARY. *Assume that G is of type $\boldsymbol{C}_n$ ($n \geqq 2$) and* char$(k) =$ 2. *Then*:

(i) *every full subgroup H of $G(k)$ contains $G^E(B)$ for a full subring B of k, if and only if the dimension of k over k^2 is finite or countable*;

(ii) *$G^E(R)$ is full in $G(k)$ for every full subset R of k, if and only if the dimension over k^2 is* 1 *or* 2.

PROOF. (i) Assume first that H is full. By Theorem 9.3, $H \supset G^E(A, B)$ with full B such that $Bk^2 = k$, $BA^2 \subset B \subset A$. By Lemma 7.7 (i), B contains a full subring R of k, provided the dimension of k over k^2 is countable. So, $H \supset G^E(R)$.

Assume now that the dimension is uncountable. Then we can find A and B as in Lemma 7.7 (ii). Then for $H := G^E(A, B)$ we have $R_\delta(H) = B$ for all δ in Σ_l (see, Theorem 6.1). So, by Lemma 7.7 (ii), H does not contain $G^E(C)$ for any subring C.

(ii) Let first R be full. By Lemma 7.6, then $Rk^2 = k$ provided the dimension is 1 or 2. By Corollary 9.4, $G^E(R)$ is full.

Assume now that the dimension is larger than 2. By Lemma 7.6, we find a proper full subspace R of k. Replacing R by Ry^{-1} with $0 \neq y$ in R, we can assume that $R \ni 1$. By Theorem 6.1, $R_\delta(G^E(k, R)) = R$ for any δ in Σ_l. By Theorem 9.3, $G^E(k, R)$ is not full. So its subgroup $G^E(R)$ is not full.

REMARK. Theorem 2 is contained in Corollaries 9.5 and 9.6.

PROOF OF THEOREM 3. Let H and g_i be as in Theorem 3. By Theorem 9.3, $H \supset G^E(A, B)$, where B is full and $Bk^2 = k$. By Theorem 8.4, $H_i := g_i H g_i^{-1} \supset G^E(Ab_i, Bb_i)$ for $i = 1, \cdots, m$ with $0 \neq b_i \in B$. By Lemma 7.2 (i), the intersection B' of all Bb_i is full and $B'k^2 = k$. Since $A \supset B$, we have $H_i \supset G^E(B')$ for all $i = 1, \cdots, m$. By Corollary 9.4, $G^E(B')$ is full, so the intersection of H_i is full.

REMARK. If all $g_i \in G^E(k)$, then the intersection of all H_i contains $G^E(Ab_0, Bb_0)$ for some $b_0 \neq 0$ in B, see Corollary 8.2.

10. Proof of Theorem 4.

10.1. THEOREM. *Assume that k contains at least* 3 *elements, if G is of type $\boldsymbol{B}_2$ or $\boldsymbol{G}_2$. Let A and B be additive subgroups of k satisfying Theorem* 1.1 (iii), (iv). *Assume that B is full and $Bk^2 = k$. Let M be a* *non-central subgroup of* $G(k)$ *normalized by* $G^E(A, B)$. *Then* $M \supset G^E(dA, dB)$ *for a non-zero* d *in* B.

In view of Corollary 9.4, this theorem implies Theorem 4. Indeed, let M be a non-central subgroup of $G(k)$ normalized by a full subgroup H of $G(k)$. By Theorem 9.3, $H \supset G^E(A, B)$, where A and B are as in Theorem 10.1. By Theorem 10.1, there is a non-zero d in B such that $M \supset G^E(Ad, Bd)$. By Lemma 7.2 (ii), $B \cap Bd := B'$ is a full additive subgroup of k such that $B'B^2 \subset B'$ and $B'k^2 = k$. By Corollary 9.4, $G^E(B')$ is full in $G(k)$, Thus, $H \cap M \supset G^E(B')$ is full.

REMARK. If G is of type $\boldsymbol{B}_2 = \boldsymbol{C}_2$ or $\boldsymbol{G}_2$ and $k = \{0, 1\}$, then $G^E(k)$ contains a normal subgroup M of index 2 (see, for example, [4, Remark after Theorem 5]). Since $G^E(k)$ is the smallest full subgroup of $G(k)$, M is not full (and M does not sit in the center of $G(k)$).

10.2. LEMMA. *Theorem* 10.1 *holds if* k *is finite.*

PROOF. Any full subring of a finite k is k itself. In particular, if B and A are as in Theorem 10.1, then the subring of k generated by B is k. It follows easily that $A = k$ and $B = k$.

Therefore, $G^E(A, B) = G^E(k)$. By Theorem 8.4, $G^E(k)$ is normal in $G(k)$. It is well-known (see, for example, [5]) that every non-central subgroup M of $G(k)$ normalized by $G^E(k)$ contains $G^E(k)$. In particular, $M \supset G^E(k) = G^E(dA, dB)$ for any $d \neq 0$ in $B = k$.

For the rest of this section we assume that k *is infinite.*

10.3. LEMMA. *Fix an ordering on* Σ. *Let* α *be the maximal root and* U *the algebraic subgroup of* G *generated by all* $x_\varepsilon(k)$ *with positive* ε *in* Σ. *Then there are* w *in* $G^E(k)$ *and* c *in* k *such that* $UwTU$ *is Zariski open in* G *and* $wx_\alpha(t)w^{-1} = x_{-\alpha}(ct)$ *for all* t *in* k.

PROOF. Let U' be the algebraic subgroup of G generated by all $x_\varepsilon(k)$ with negative ε. Then $U'TU$ is open in G (see, for example, [4, Theorem 7 (a)]).

We pick any w in $G^E(k)$ such that $wTw^{-1} = T$ and $wU'w^{-1} = U$. Then $wx_\alpha(t)w^{-1} = x_{-\alpha}(ct)$ for some c in k.

10.4. LEMMA. *In the conditions of Theorem* 10.1, M *is Zariski dense in* G.

PROOF. Since k is infinite, so is B. Therefore $x_\varepsilon(B)$ is Zariski dense in $x_\varepsilon(k)$ for each root ε in Σ and $H := G^E(A, B) \supset G^E(B)$ is Zariski dense in G. Since H normalizes M, it follows that G normalizes the Zariski closure of M in G. Since G is almost simple and M is not central, the closure is G, so M is dense in G.

10.5. LEMMA. *In the conditions of Theorem* 10.1, *let* $\alpha \in \Sigma_l$. *Then there are* g *in* $G^E(k)$ *and* u *in* k *such that* g *commutes with* $x_\alpha(k)$ *and* $x_\alpha(b)x_{-\alpha}(ub) \in gMg^{-1}$ *for all* b *in* B.

PROOF. We can choose an ordering on Σ in such a way that α becomes the maximal root (because the maximal root is always long and the Weyl group acts transitively on the long roots). Let U, w, and c be as in Lemma 10.3.

Since $UwTU$ is open in G and M is dense in G (see, Lemma 10.4), there is some m in $UwTU \cap M$. We write $m = g^{-1}whg'$ with $g, g' \in U(k)$ and $h \in T(k)$. Since $[U, x_\alpha(k)] = 1$ and $hx_\alpha(t)h^{-1} = x_\alpha(\alpha(h)t)$ for all t in k, we have $M \ni [x_\alpha(b), m] = x_\alpha(b)g^{-1}whg'x_\alpha(-b)g'^{-1}h^{-1}w^{-1}g = x_\alpha(b)g^{-1}x_{-\alpha}(-c\alpha(h)b)g = g^{-1}(x_\alpha(b)x_{-\alpha}(-c\alpha(h)b))g$ for all b in B. Thus, $gMg^{-1} \ni x_\alpha(b)x_{-\alpha}(ub)$ for all b in B with $u := -c\alpha(h)$.

10.6. COROLLARY. *In the conditions of Lemma* 10.5, *there is a non-zero* d_α *in* k *such that* $M \supset x_\alpha(d_\alpha B)$.

PROOF. Let g and u be as in Lemma 10.5. Let $b_g \in B$ be as in Corollary 8.2. Then $gMg^{-1} =: M'$ is normalized by $gG^E(A, B)g^{-1} \supset G^E(Ab_g^2, Bb_g^2)$. Pick a $b' \neq b'^3$ in Bb_g^2.

If α belongs to a subsystem $\Sigma' \subset \Sigma$ of type $\boldsymbol{A}_2$, we find $\delta \in \Sigma'$ such that $\alpha + \delta \in \Sigma'$. Since gMg^{-1} contains $x_\alpha(b)x_\alpha(bu)$ for all b in B and is normalized by $x_\delta(Bb_g^2)$ and $x_{-\delta}(Bb_g^2)$, we have $M' \ni y := [x_\delta(b'), x_\alpha(b)x_{-\alpha}(bu)] = x_{\delta+\alpha}(\pm bb')$ and $M' \ni [x_{-\delta}(b'), y] = x_\alpha(\pm b'^2 b)$. So, $M' \supset x_\alpha(b'^2 B)$. Since $[g, x_\alpha(k)] = 1$, it follows that $M \supset x_\alpha(b'^2 B)$. Thus, we can take $d := b'^2$.

If α does not belong to a subsystem of type $\boldsymbol{A}_2$, then it belongs to a subsystem Σ' of type $\boldsymbol{B}_2$. We pick a short root β in Σ' such that $\alpha + \beta \in \Sigma'$. Then $[x_\beta(k), x_{-\alpha}(k)] = 1$.

Since M' is normalized by $x_\beta(Bb_g^2)$, we have $M' \ni z_1(v, t) := [x_\beta(v), x_\alpha(b)x_{-\alpha}(bu)] = x_{\beta+\alpha}(\pm vt)x_{2\beta+\alpha}(\pm v^2 b)$ for all v in Bb_g^2 and b in B, hence $M' \ni z_1(b'^3, b)z_1(b', b'^2 b)^{-1} = x_{\alpha+2\beta}(\pm b'^4(b'^2 - 1)b)$ for all b in B. So, $M' \supset x_{\alpha+2\beta}(Bb'^4(b'(b'^2 - 1))$.

Since M' is normalized by $x_{-\beta}(b_g^2 B)$, we have $M' \ni z_2(v, t) = [x_{-\beta}(v), x_{2\beta+\alpha}(t)] = x_{\beta+\alpha}(\pm vt)x_\alpha(\pm v^2 t)$ for all v in $b_g^2 B$ and t in $b'^4(b'^2 - 1)B$, hence $M' \ni z_2(b'^3, t)z_2(b', b'^2 t)^{-1} = x_\alpha(\pm b'^4(b'^2 - 1)t)$ for all t in $b'^4(b'^2 - 1)B$. Thus, $M' \supset x_\alpha(d_\alpha B)$ for $d_\alpha := b'^8(b'^2 - 1)^2 \neq 0$, hence $M \supset x_\alpha(d_\alpha B)$.

10.7. LEMMA. *For any* $\beta \in \Sigma_s$ *there is a non-zero* d_β *in* k *such that* $M \supset x_\beta(d_\beta A)$.

PROOF. If β is long, we can use Corollary 10.6. Otherwise, β lies in a subsystem $\Sigma' \subset \Sigma$ of type $\boldsymbol{B}_2$ or $\boldsymbol{G}_2$. Pick $b \neq b^3$ in B.

If Σ' is of type $\boldsymbol{B}_2$, we pick a short root γ in Σ' such that $\gamma + \beta \in \Sigma'_l$. Since M is normalized by $G^E(A, B)$ and $M \supset x_{\gamma+\beta}(d_{\gamma+\beta}B)$ (see, Corollary 10.6), we have $M \ni z(u, t) := [x_{-\gamma}(u), x_{\gamma+\beta}(t)] = x_\beta(\pm ut)x_{\beta-\gamma}(\pm u^2 t)$ for all u in A and t in $d_{\gamma+\beta}B$. Therefore, $M \ni z(u, b^3 d_{\gamma+\beta})z(ub, bd_{\gamma+\beta})^{-1} = x_\beta(\pm u(b^3 - b^2)d_{\gamma+\beta})$. Thus, $M \supset x_\beta(d_\beta A)$ with $d_\beta := b^2(b-1)d_{\gamma+\beta} \neq 0$.

If Σ' is of type $\boldsymbol{G}_2$, then we find a long α in Σ' such that $\alpha + \beta \in \Sigma'_s$. Since $M \supset x_{-\alpha}(d_{-\alpha}B)$ and M is normalized by $G^E(A, B) \supset x_{\alpha+\beta}(A)$, we have $M \ni z_1(t, u) := [x_{-\alpha}(t), x_{\alpha+\beta}(u)] = x_\beta(\pm tu)x_{\alpha+2\beta}(\pm tu^2)x_{2\alpha+3\beta}(\pm tu^3)x_{\alpha+3\beta}(t^2u^3)$ for all t in $d_{-\alpha}B$ and u in A.

Therefore, $M \ni z_2(t, u) := z_1(t, ub)z_1(tb^3, u)^{-1} = x_\beta(\pm tu(b - b^3)x_{\alpha+2\beta}(\pm tu^2 \times (b^2 - b^3))x_{\alpha+3\beta}(\pm t^2u^3(b^3 - b^6))$, hence, $M \ni z_3(t, u) := z_2(tb^3, u)z_2(t, ub^2)^{-1} = x_\beta(\pm tu(b - b^3)(b^3 - b^2))x_{\alpha+2\beta}(\pm tu^2(b^2 - b^3)(b^3 - b^4))$, so $M \ni z_3(tb^2, u)z_3(t, ub)^{-1} = x_\beta(\pm tu(b - b^3)(b^3 - b^2)(b^2 - b))$ for all $t \in d_{-\alpha}B$ and $u \in A$.

Thus, $M \supset x_\beta(Ad_\beta)$ with $d_\beta := d_{-\alpha}b^4(b^2 - 1)(b - 1)^2 \neq 0$.

Proof of Theorem 10.1. Now we are ready to complete our Proof of Theorem 10.1 (for infinite k).

By Theorem 1.1, Lemma 8.3, and Corollaries 10.6 and 10.7, $M \supset G^E(A', B')$ with additive subgroups A' and B' of k satisfying $A' \subset d_1 A$ and $B' \subset d_1 B$, where $0 \neq d_1, d_2 \in k$.

Since $Bk^2 = k$, we have $d_2 = b_1c^2$ with $0 \neq b_1 \in B$ and $0 \neq c \in k$. Since B is full, $c = b_2/b_3$ and $d_1 = b_4/b_5$ with non-zero b_i in B. Therefore, $A' \supset d_1A = b_4A/b_5 \supset b_4A \supset b_4^2 b_1 b_2^2 A$ (since $BA \subset B$) and $B' \supset d_2B = b_1c^2B = b_1b_2^2B/b_3^2 \supset b_1b_2^2B \supset b_4^2b_1b_2^2B$ (since $BB^2 \subset B$).

Thus, $A' \supset dA$ and $B' \supset dB$, where $0 \neq d := b_4^2b_1b_2^2 \in B$, hence $M \supset G^E(Ad, Bd)$.

11. Type A_1 and non-split groups. First we give counter examples to Theorems 1–4 for $G = SL_2$.

11.1. A counter example to Theorem 1. See [7, the last section].

11.2. A counter example to Theorems 2 and 9.3. Let k be a field such that $\mathrm{char}(k) = 2$ and $k \neq k^2$. Let $T(k)$ be the subgroup of diagonal matrices in $SL_2(k)$. Here is our choice of parametrizations of the root subgroups: $x_\alpha(t) = \begin{pmatrix} 1 & t \\ 0 & 1 \end{pmatrix}$ and $x_\beta(t) = \begin{pmatrix} 1 & 0 \\ t & 1 \end{pmatrix}$ for all t in k.

Set $H := \{hg : h \in T(k), g \in SL_2(k^2)\}$. Since $T(k)$ normalizes $SL_2(k^2)$, H is a subgroup of $SL_2(k)$. We claim that it is a full subgroup. Indeed, given any $g = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ in $SL_2(k)$, we set $u := 1/(1 + ac)$ when $ac \neq 1$ and $u := 1/(1 + z^2)$ with any $z \neq 0, 1$ when $ac = 1$. Then $v := u/(1 + auc) \in k^2$, hence

$$g\begin{pmatrix}1 & u\\ 0 & 1\end{pmatrix}g^{-1} = \begin{pmatrix}1+auc & aua\\ cuc & 1+cua\end{pmatrix}$$
$$= \begin{pmatrix}u/v & 0\\ 0 & v/u\end{pmatrix}\begin{pmatrix}1 & ava\\ ucuc/v & (u/v)^2\end{pmatrix} \in T(k)SL_2(k^2) = H\ .$$

Similarly, there is a non-zero u' in k such that $H \ni gx_\beta(u')g^{-1}$. Thus, H is full.

But $R_\alpha(H) = k^2$ is not full when $k \neq k^2$. Therefore, H does not contain $E_2(R)$ with a full subset R of k.

11.3. A COUNTER EXAMPLE TO THEOREM 3. Let k and H be as in 11.2. Take any w in k outside k^2. Set $g := x_\alpha(w)$. Then H is full, but $H \cap gHg^{-1} \cap x_\beta(k)$ is trivial, so $H \cap gHg^{-1}$ is not full.

11.4. A COUNTER EXAMPLE TO THEOREM 4. Let k and H be as in 11.2. Then $SL_2(k^2)$ is normalized by full H, but $SL_2(k^2)$ is not full and is not contained in the center of $SL_2(k)$.

Now we will discuss extensions of our results to non-split groups. Let G be an almost simple algebraic group defined over a field k. Fixing a maximal k-split torus T and a matrix representation $G \subset SL_N$, we have "root" subgroups U_ε. Given any subset R of k, we can define $G^E(R)$ to be the subgroup of $G(k)$ generated by all root elements with (non-diagonal) entries in R. We can call a subgroup H of $G(k)$ *full*, if for any g in $G(k)$ the intersection of gHg^{-1} with each root subgroup is not trivial. I believe that Theorems 1–5 hold (for this more general class of G's), if the k-rank of G is at least 2 and G is absolutely (almost) simple, and have checked this for all classical G. For some groups it follows from results of [7].

REMARK. It is easy to see that when k is a number field every arithmetic (or, more generally, S-arithmetic) subgroup of $G(k)$ is full. I believe that, conversely, every full subgroup contains an arithmetic subgroup, and have checked this for all classical G.

REMARK. Some of our groups $G^E(A, B)$ for Chevalley groups G were introduced by Abe [18] and studied by Abe-Suzuki [19].

REFERECES

[1] T. J. JECH, On a problem of L. Nachbin, Proc. Amer. Math. Soc. 79 (1980), 341–342.
[2] O. T. O'MEARA, Lectures on linear groups, Providence, R.I. 1978.
[3] O. T. O'MEARA, Symplectic groups, Providence, R.I. 1978.
[4] R. STEINBERG, Lectures on Chevalley groups, Yale University, 1967.
[5] J. TITS, Algebraic and abstract simple groups, Ann. of Math. 80 (1964), 313–329.

[6] J. TITS, Systemes generateurs de groupes de congruence, C.R. Acad. Sc. Paris, 283 (1976), A693-695.

[7] L. N. VASERSTEIN, On full subgroups in the sense of O'Meara, J. of Algebra, 75 (1982), 437-444.

[8] L. N. VASERSTEIN, Stabilization for classical groups over rings, Mat. Sbornik, 93 : 2 (1974), 268-295; Math. USSR Sb. 22 (1974), 271-303.

[9] A. BOREL AND J. TITS, Homomorphismes "abstraits" de groupes algebriques simples, Annals of Math. 97 : 3 (1973), 499-571.

[10] Zentralblatt 481 (1982) 20031; Math. Rev. 83b, 20047.

[11] Zentralblatt 466 (1981) 20022; Math. Rev. 82j, 10043.

[12] C. RIEHM, Structure of the symplectic group over a valuation ring, Amer. J. Math. 88 (1966), 106-128.

[13] C. RIEHM, Orthogonal groups over the integers of a local field. II, Amer. J. Math. 89 (1967), 549-577.

[14] D. JAMES, The structure of local integral orthogonal groups, Trans. AMS, 228 (1977), 165-186.

[15] Z. BOREVICH, A description of the subgroups of the general linear group containing the group of diagonal matrices, Zapiski LOMI, 64 (1976), 12-29 (in Russian).

[16] N. VAVILOV, On parabolic subgroups of Chevalley groups over semi-local rings, Zapiski LOMI 75 (1978), 43-58 (in Russian); Zentralblatt 488.20046.

[17] A. BOREL, Properties and linear representations of Chevalley groups, in Lecture Notes in Math. 131 (1970), 1-55, Springer-Verlag, Berlin, Heidleberg, New York.

[18] E. ABE, Chevalley groups over local rings, Tôhoku Math. J. 21 (1969), 474-494.

[19] E. ABE AND K. SUZUKI, On normal subgroups of Chevalley groups over commutative rings, Tôhoku Math. J. 28 (1976), 185-198.

DEPARTMENT OF MATHEMATICS
THE PENNSYLVANIA STATE UNIVERSITY
UNIVERSITY PARK, PA 16802,
USA