Tôhoku Math. J.
47 (1995), 81–97

AUTOMORPHISMS OF SIMPLE CHEVALLEY GROUPS OVER Q-ALGEBRAS

YU CHEN

(Received October 8, 1993, revised May 2, 1994)

Abstract. We show that a simple adjoint Chevalley group over a Q-algebra without zero divisors and its elementary subgroup have isomorphic automorphism groups which are generated by the inner automorphisms, the graph automorphisms and the ring automorphisms. This leads to an expression for every automorphism as the composite of a ring automorphism and an automorphism of an algebraic group, which is analogous to the Borel-Tits theorem and the Margulis theorem for the automorphisms of rational subgroups of algebraic groups over certain fields.

Introduction. Let G be a simple Chevalley-Demazure group scheme of adjoint type. The main purpose of this paper is to describe the automorphisms of the Chevalley group $G(R)$ and its elementary subgroup $E(R)$ provided that the rank of G is greater than one, where R is an associative and commutative algebra over the rational number field Q without zero divisors. The first study of this problem goes back to the work of Schreier and Van der Waerden [13] where they gave a description of the automorphisms of the projective group PSL_n over an algebraically closed field. The automorphisms of adjoint simple Chevalley groups were determined first by Steinberg [14] for finite fields and then by Humphreys [12] for infinite fields. We refer to [11] for a historical survey on homomorphisms of algebraic groups and Chevalley groups. In this paper we discuss the automorphisms of all subgroups between $G(R)$ and $E(R)$. It turns out that such an automorphism can be always expressed in a unique way as a product of an automorphism induced by the conjugation of an element in $G(R)$, a graph automorphism and a ring automorphism (see § 1 for the definition). We find that each automorphism of a subgroup between $G(R)$ and $E(R)$ is a restriction of an automorphism of $G(R)$ and, meanwhile, keeps $E(R)$ invariant (see Theorem 1). This leads to an isomorphism between the automorphism group of $G(R)$ and the automorphism group of $E(R)$. The structure of the automorphism group of $G(R)$ and $E(R)$ is given by Theorem 2. We show in Theorem 3 that every automorphism of a subgroup between $G(R)$ and $E(R)$ is a composite of a ring automorphism and an automorphism as an algebraic group, which is an analogue of the Borel-Tits theorem [4] and the Margulis theorem [17]. When the rank of G is equal to one, the automorphisms of $G(R)$ are known only for some special rings R and we refer to [6, §1] for a brief review of recent developments in this particular case.

1991 *Mathematics Subject Classification*. Primary 20E36; Secondary 20G35, 20F28.

1. Terminology and main results. Let $\mathfrak{g}_C$ be a complex simple Lie algebra with a root system Φ. Using the adjoint representation of $\mathfrak{g}_C$ and a Chevalley basis, we can construct an affine group scheme G over $\boldsymbol{Z}$, which is called the Chevalley-Demazure group scheme of adjoint type (cf. [9]). In particular, for each commutative ring R with a unit, we obtain a group $G(R)$ which is called the Chevalley group over R of adjoint type. For each root $a \in \Phi$, there is a canonical (exponential) map u_a from the additive group R^+ into $G(R)$ (cf. [1, §1.3]). We denote by $U_a(R)$ the set of images $u_a(r)$ for all $r \in R$. The elementary subgroup $E(R)$ is defined to be the subgroup of $G(R)$ generated by $U_a(R)$ for all $a \in \Phi$. For example, if Φ is of type A_{n-1}, the corresponding Chevalley group of adjoint type is then $PSL_n(R)$ and its elementary subgroup $E(R)$ is the subgroup of $PSL_n(R)$ generated by the images of all $n \times n$ elementary matrices over R under the natural homomorphism from $SL_n(R)$ to $PSL_n(R)$. It is known that $E(R) = PSL_n(R)$ when R is a semilocal ring (cf. [2]). The structure of the groups between $G(R)$ and $E(R)$ is not yet clear for us for an arbitrary ring R. However, we have following result:

THEOREM 1. *Let R be an associative and commutative $\boldsymbol{Q}$-algebra without zero divisors. Suppose $G(R)$ is a simple Chevalley group of adjoint type and the rank of G is greater than* 1. *Let H be a subgroup of* G(R) *which contains $E(R)$. Then every automorphism of H can be extended uniquely to an automorphism of $G(R)$ and the restriction of each automorphism of H to $E(R)$ is an automorphism of $E(R)$. In particular, the automorphism group of $G(R)$ is isomorphic to the automorphism group of $E(R)$.*

We need some description about certain particular automorphisms of $G(R)$ and $E(R)$ before further stating our main results. Let K be a universal domain containing $\boldsymbol{Q}$. In the following, R stands for a $\boldsymbol{Q}$-subalgebra of K and G is a simple Chevalley-Demazure group scheme of adjoint type.

Let Δ be a set of fundamental roots of Φ and γ an automorphism of Φ which keeps Δ invariant. It is easily seen from [10, exp. XXIII, §5.5] that γ gives rise to an automorphism of G and, hence, an automorphism $\tilde{\gamma}$ of $G(R)$ such that

$$\tilde{\gamma}(u_a(r)) = u_{\gamma(a)}(r), \qquad \text{for all} \quad a \in \Delta \text{ or } -\Delta\,, \quad r \in R\,. \tag{1.1}$$

$\tilde{\gamma}$ is called a graph automorphism of $G(R)$ related to γ. Since $E(R)$ is generated by $U_a(R)$ for all $a \in \Delta$ or $-\Delta$, the restriction of $\tilde{\gamma}$ on $E(R)$ is also an automorphism of $E(R)$. We call an automorphism of $E(R)$ of the form (1.1) a graph automorphism of $E(R)$ related to γ.

Let φ be an automorphism of R. Since G is a covariant group functor on the category of commutative rings with unity, φ gives rise to an automorphism of group $G(R)$, which is called a ring automorphism of $G(R)$ related to φ. A ring automorphism of $E(R)$ related to φ is an automorphism $\tilde{\varphi}$ defined by

$$\tilde{\varphi}(u_a(r)) = u_a(\varphi(r))\,, \qquad \text{for all} \quad a \in \Phi \text{ and } r \in R\,. \tag{1.2}$$

The ring automorphism of $G(R)$ related to φ coincides with $\tilde{\varphi}$ on $E(R)$ (see the proof of Proposition 4.2), hence we denote it also by $\tilde{\varphi}$ without any confusion.

For each element $g \in G(R)$, we denote by $\operatorname{Int} g$ the inner automorphism of $G(R)$ induced by the conjugation by g. Since G is of adjoint type, $G(R)$ is centreless and we may identify $G(R)$ with the subgroup of $\operatorname{Aut} G(R)$ generated by $\operatorname{Int} g$ for all $g \in G(R)$.

THEOREM 2. *Suppose the rank of G is greater than one. Let H be $G(R)$ or $E(R)$. Then* $\operatorname{Aut} H$ *is generated by $G(R)$, the graph automorphisms and the ring automorphisms. More precisely,*

(i) *every automorphism $\alpha \in \operatorname{Aut} H$ has an expression*

$$\alpha = \operatorname{Int} g \cdot \tilde{\gamma} \cdot \tilde{\varphi}\,, \tag{1.3}$$

where $g \in G(R)$, $\tilde{\gamma}$ is a graph automorphism and *$\tilde{\varphi}$ is a ring automorphism. Moreover, the factors $g, \tilde{\gamma}$* and *$\tilde{\varphi}$ are uniquely determined by α;*

(ii) *let A be the subgroup of* $\operatorname{Aut} H$ *generated by $G(R)$ and the graph automorphisms, and let B be the subgroup of* $\operatorname{Aut} H$ *generated by $G(R)$ and the ring automorphisms. Then we have normal sequences*

$$G(R) \lhd A \lhd \operatorname{Aut} H \tag{1.4}$$

and

$$G(R) \lhd B \lhd \operatorname{Aut} H\,; \tag{1.5}$$

(iii) *we have following isomorphisms:*

$$\operatorname{Aut} H/A \cong B/G(R) \cong \operatorname{Aut} R \tag{1.6}$$

and

$$\operatorname{Aut} H/B \cong A/G(R) \cong S\,, \tag{1.7}$$

where S is the group of order two if G is of type A_n, D_n $(n \geqslant 5)$ or E_6, S is the symmetric group on three objects if G is of type D_4 and S is trivial for all other cases. In particular

$$\operatorname{Aut} H/G(R) \cong \operatorname{Aut} R \times S\,. \tag{1.8}$$

THEOREM 3. *Suppose the rank of G is greater than one. Let H be a subgroup of $G(R)$ which contains $E(R)$. If α is an automorphism of H, then there exist an automorphism $\varphi \in \operatorname{Aut} R$ and an automorphism β of the algebraic group $G(K)$ such that*

$$\alpha(g) = \beta(\tilde{\varphi}(g))\,, \qquad \textit{for all} \quad g \in H\,, \tag{1.9}$$

where β and φ are uniquely determined by α.

2. Notation and some lemmas. Throughout this paper G stands for a simple Chevalley-Demazure scheme of adjoint type and we assume that the rank of G is greater than one, K is a universal domain containing $\boldsymbol{Q}$ and R is a $\boldsymbol{Q}$-subalgebra of K. If M and P are subgroups of a group H, we denote by $C_P(M)$ and $N_P(M)$ the centralizer and the normalizer of M in P, respectively. The centre of H is denoted by $C(H)$. $[M, P]$

stands for the subgroup of H generated by the elements of the form $xyx^{-1}y^{-1}$ for all $x \in M$ and for all $y \in P$. A subgroup of H which is generated by subsets $X_1, X_2, \ldots$ is expressed by $\langle X_1, X_2, \ldots \rangle$. If H is an algebraic group, we denote by $L(H)$ the Lie algebra of H and if M is an abstract subgroup of H, we denote by $\mathrm{cl}(M)$ the Zariski closure of M in H and by $\mathrm{cl}(M)^\circ$ the connected component of $\mathrm{cl}(M)$ that contains the identity element.

LEMMA 2.1. *Suppose H is a connected algebraic group of one dimension. Then every infinite subgroup of H is Zariski dense in H.*

PROOF. Let M be an infinite subgroup of H. Since the quotient group $\mathrm{cl}(M)/\mathrm{cl}(M)^\circ$ is finite, $\mathrm{cl}(M)^\circ$ is infinite. This means that $\dim \mathrm{cl}(M)^\circ \geqslant 1$. On the other hand, the inclusions $\mathrm{cl}(M)^\circ \subseteq \mathrm{cl}(M) \subseteq H$ implies that $\dim \mathrm{cl}(M)^\circ \leqslant \dim H = 1$. Thus $\dim \mathrm{cl}(M)^\circ = 1$ and the above inclusions yield immediately that $\mathrm{cl}(M) = H$.

For each root $a \in \Phi$ we simply denote by U_a the group $U_a(K)$, and let U (resp. U^-) be the subgroup of $G(K)$ generated by U_a for all $a \in \Phi^+$ (resp. $-a \in \Phi^+$). Let B (resp. B^-) be the Borel subgroup of $G(K)$ which contains U (resp. U^-) as its unipotent radical. Then $B \cap B^-$ is a maximal torus of $G(K)$, which is denoted by T. Note that

$$U_a(R) = U_a \cap E(R)\,, \qquad \text{for all} \quad a \in \Phi\,.$$

It is obvious that $U \cap E(R)$ (resp. $U^- \cap E(R)$) is generated by $U_a(R)$ for all $a \in \Phi^+$ (resp. $-a \in \Phi^+$). We denote by $U(R)$ the group $U \cap E(R)$ and by $U^-(R)$ the group $U^- \cap E(R)$.

COROLLARY 2.2. (i) *$T \cap E(R)$ is Zariski dense in T;*
(ii) *$U(R)$ is Zariski dense in U and $U^-(R)$ is Zariski dense in U^-;*
(iii) *$B \cap E(R)$ is Zariski dense in B.*

PROOF. (i) Let $\Delta = \{a_1, a_2, \ldots, a_n\}$ and denote by T_i for the group $T \cap \langle U_{a_i}, U_{-a_i} \rangle$ for all $1 \leqslant i \leqslant n$. Then T_i is a one dimensional subtorus of T for all $1 \leqslant i \leqslant n$ and $T = \prod_{i=1}^n T_i$. Let $T_i(R)$, $1 \leqslant i \leqslant n$, be the set of R-rational points of T_i, which is Zariski dense in T_i by Lemma 2.1, since R is infinite. Moreover, it is easily seen that $T \cap E(R) \supseteq \prod_{i=1}^n T_i(R)$. Therefore we have

$$T \supseteq \mathrm{cl}(T \cap E(R)) \supseteq \prod_{i=1}^{n} \mathrm{cl}(T_i(R)) = T\,,$$

which implies that $\mathrm{cl}(T \cap E(R)) = T$.

(ii) Since $U(R)$ is generated by $U_a(R)$ for all $a \in \Phi^+$, which is Zariski dense in U_a by Lemma 2.1, we have

$$\mathrm{cl}(U(R)) = \mathrm{cl}(\langle U_a(R) \mid \forall a \in \Phi^+ \rangle) = \langle \mathrm{cl}(U_a(R)) \mid \forall a \in \Phi^+ \rangle = \langle U_a \mid \forall a \in \Phi^+ \rangle = U\,.$$

Replacing the positive roots by the negative roots, we then obtain the Zariski density of $U^-(R)$ in U^-.

(iii) Consider inclusions $B \supseteq B \cap E(R) \supseteq (T \cap E(R)) \cdot U(R)$. By taking their Zariski closures, we obtain from (i) and (ii)

$$B \supseteq \mathrm{cl}(B \cap E(R)) \supseteq \mathrm{cl}((T \cap E(R)) \cdot U(R)) = T \cdot U = B$$

from which follows (iii).

PROPOSITION 2.3. *Let H be a subgroup of $G(R)$ which contains $E(R)$. Then*

$$E(R) = \bigcap_{E(\boldsymbol{Q}) \subseteq N \lhd H} N .$$

PROOF. Let M be the intersection of all normal subgroups of H which contains $E(\boldsymbol{Q})$. Then $M \subseteq E(R)$ since $E(R)$ is a normal subgroup of H by [16]. On the other hand, for each $a \in \Phi$ and each $x \in \boldsymbol{Q}^*$, let

$$h_a(x) = u_a(x)u_{-a}(-x^{-1})u_a(x)u_{-a}(1)u_a(-1)u_{-a}(1) \in T \cap E(\boldsymbol{Q}) .$$

We have

$$h_a(x)u_a(r)h_a(x)^{-1} = u_a(x^2 r) , \qquad \text{for all} \quad x \in \boldsymbol{Q}^* \text{ and } r \in R .$$

Choosing such $x \in \boldsymbol{Q}^*$ that $x^2 \neq 1$, we obtain

$$u_a(r) = h_a(x)u_a((x^2-1)^{-1}r)h_a(x)^{-1}u_a((x^2-1)^{-1}r)^{-1} \in M , \qquad \text{for all} \quad r \in R \text{ and } a \in \Phi ,$$

since M is a normal subgroup of H. This implies that $M \supseteq E(R)$. Therefore $M = E(R)$.

Let $\mathfrak{g}$ be a $\boldsymbol{Z}$-form of the simple complex Lie algebra $\mathfrak{g}_{\boldsymbol{C}}$ and denote by $\mathfrak{g}_R$ the R-Lie algebra $\mathfrak{g} \otimes_{\boldsymbol{Z}} R$. Let $\mathrm{ad}\colon \mathfrak{g}_K \to \mathrm{Mat}_n(K)$ be the adjoint representation of $\mathfrak{g}_K$, where n is the dimension of $\mathfrak{g}_K$.

Lemma 2.4. *Let z be an element of $\mathfrak{g}_K$ such that $\mathrm{ad}(z) \in \mathrm{Mat}_n(R)$. Then $z \in \mathfrak{g}_R$.*

PROOF. We write the Cheavalley base of $\mathfrak{g}_{\boldsymbol{C}}$ as $\{e_1, e_2, \ldots, e_n\}$. Then $\mathrm{ad}(e_i \otimes 1) \in \mathrm{Mat}_n(\boldsymbol{Z})$ for all $1 \leqslant i \leqslant n$. Suppose z has an expression $\sum_{i=1}^n e_i \otimes x_i$, where $x_i \in K$ for all $1 \leqslant i \leqslant n$. Then

$$\mathrm{ad}(z) = \sum_{i=1}^{n} \mathrm{ad}(e_i \otimes x_i) . \tag{2.1}$$

On the other hand, suppose

$$\mathrm{ad}(z) = (z_{st}) \in \mathrm{Mat}_n(R) , \quad z_{st} \in R , \qquad \text{for} \quad s, t \in \{1, 2, \ldots, n\}$$

and

$$\mathrm{ad}(e_i \otimes 1) = (e_{i,st}) \in \mathrm{Mat}_n(\boldsymbol{Z}) , \quad e_{i,st} \in \boldsymbol{Z} , \qquad \text{for} \quad i, s, t \in \{1, 2, \ldots, n\} .$$

Then the equation (2.1) implies following n^2 equations.

$$z_{11} = x_1 e_{1,11} + x_2 e_{2,11} + \cdots + x_n e_{n,11}$$

$$z_{12} = x_1 e_{1,12} + x_2 e_{2,12} + \cdots + x_n e_{n,12}$$
$$\vdots$$
$$z_{nn} = x_1 e_{1,nn} + x_2 e_{2,nn} + \cdots + x_n e_{n,nn}\,.$$

Since $\mathrm{ad}(e_1 \otimes 1)$, $\mathrm{ad}(e_2 \otimes 1), \ldots, \mathrm{ad}(e_n \otimes 1)$ are linearly independent, there are n linearly independent equations in the above system. Hence the unique solution for $x_1, x_2, \ldots, x_n$ satisfying the above equations is given by Cramer's rule as the quotients of the determinants of certain $n \times n$ matrices in $\mathrm{Mat}_n(R)$ factored by the determinant of an $n \times n$ matrix in $\mathrm{Mat}_n(\boldsymbol{Z})$. Consequently, we obtain that $\{x_1, x_2, \ldots, x_n\} \subseteq R$. Hence z lies in $\mathfrak{g}_R$.

LEMMA 2.5. *Suppose $g \in G(K)$. If $gu_a(1)g^{-1} \in G(R)$ for all $a \in \Phi$, then $g \in G(R)$.*

PROOF. Let $\{e_a, h_{a_i} \mid \forall a \in \Phi, \forall a_i \in \Delta\}$ be a Chevalley basis of $\mathfrak{g}_C$, where $[e_{a_i}, e_{-a_i}] = h_{a_i}$. Considering $G(K)$ as a subgroup of $GL_n(\mathfrak{g}_K)$ via the adjoint representation of $G(K)$, we have (cf. [15])

$$u_a(1) = \exp \mathrm{ad}(e_a \otimes 1)\,, \qquad \text{for} \quad a \in \Phi$$

and

$$gu_a(1)g^{-1} = \exp \mathrm{ad}(g \cdot (e_a \otimes 1))\,, \qquad \text{for} \quad a \in \Phi\,, \tag{2.2}$$

where exp is the canonical exponential map which sends the nilpotent elements in $\mathrm{Mat}_n(K)$ to the unipotent elements in $GL_n(K)$. Recall that the logarithm map log sends the unipotent subset of $\mathrm{Mat}_n(R)$ to the nilpotent subset of $\mathrm{Mat}_n(R)$ and the composite $\log \cdot \exp$ is the identity map on the nilpotent subset (cf. [5, Chap. II. §6.1]). Applying log on both sides of (2.2), we obtain

$$\log(gu_a(1)g^{-1}) = \mathrm{ad}(g \cdot (e_a \otimes 1)) \in \mathrm{Mat}_n(R)\,, \qquad \text{for all} \quad a \in \Phi\,.$$

Thus it follows from Lemma 2.4 that $g \cdot (e_a \otimes 1)$ lies in $\mathfrak{g}_R$ for all $a \in \Phi$. Moreover, we have

$$g \cdot (h_{a_i} \otimes 1) = [g \cdot (e_{a_i} \otimes 1), g \cdot (e_{-a_i} \otimes 1)] \in \mathfrak{g}_R\,, \qquad \text{for all} \quad a_i \in \Delta\,.$$

Hence $g \in GL_n(\mathfrak{g}_R)$ and we then obtain $g \in G(K) \cap GL_n(\mathfrak{g}_R) = G(R)$.

Let $\mathfrak{g}_K$ be a simple Lie algebra over K and Φ a root system of $\mathfrak{g}_K$. Denote by $\mathfrak{g}_a$ the root subspace of $\mathfrak{g}_K$ related to a root $a \in \Phi$. Let $\mathfrak{u}$ be the subalgebra of $\mathfrak{g}_K$ generated by $\mathfrak{g}_a$ for all $a \in \Phi^+$. If $\mathfrak{d}$ is a subalgebra of $\mathfrak{g}_K$, denote by $C_\mathfrak{u}(\mathfrak{d})$ the centralizer of $\mathfrak{d}$ in $\mathfrak{u}$. The following properties of $\mathfrak{u}$ are obvious:

LEMMA 2.6. *Suppose $a \in \Phi^+$. Let $I = \{b \in \Phi^+ \mid a + b \notin \Phi^+\}$ and $J = \{c \in \Phi^+ \mid c + b \notin \Phi^+, \forall b \in I\}$, then*

(i) $C_\mathfrak{u}(\mathfrak{g}_a) = \sum_{b \in I} \mathfrak{g}_b\,;$

(ii) $C_{\mathfrak{u}}(C_{\mathfrak{u}}(\mathfrak{g}_a)) = \sum_{c \in J} \mathfrak{g}_c$.

Moreover, $c+d \notin \Phi^+$ *for all* $c, d \in J$, *hence* $C_{\mathfrak{u}}(C_{\mathfrak{u}}(\mathfrak{g}_a))$ *is a commutative subalgebra.*

LEMMA 2.7. *Let I be as in Lemma* 2.6 *and* $a \in \Phi^+$. *Then* $C_U(U_a)$ *is generated by* U_b *for all* $b \in I$. *In particular,* $C_U(U_a)$ *is connected for all* $a \in \Phi^+$.

PROOF. Let H be the subgroup of $G(K)$ generated by U_b for all positive roots b such that $a+b \notin \Phi$. It is obvious by the commutator formula [15] that

$$H \subseteq C_U(U_a). \tag{2.3}$$

On the other hand, since $L(U) = \mathfrak{u}$ and

$$\mathfrak{g}_b = L(U_b) \subseteq L(H), \qquad \text{for all} \quad b \in \Phi^+, \quad a+b \notin \Phi,$$

we have

$$\dim C_U(U_a) = \dim C_{\mathfrak{u}}(\mathfrak{g}_a) = \dim \sum_{b \in I} \mathfrak{g}_b \leqslant \dim L(H) = \dim H.$$

This implies, together with (2.3), that $\dim C_U(U_a) = \dim H$. Moreover, both $C_U(U_a)$ and H are connected because the former is unipotent and invariant under the conjugation of the maximal torus T, while the latter is generated by connected subgroups. Hence we obtain $C_U(U_a) = H$.

LEMMA 2.8. *Let J be as in Lemma* 2.6. *If a is a positive root, then*

$$C_U(C_U(U_a)) = \prod_{c \in J} U_c. \tag{2.4}$$

PROOF. Since $C_U(U_a)$ is connected by Lemma 2.7, we obtain from Lemma 2.6 that for each $a \in \Phi^+$

$$L(C_U C_U(U_a)) = C_{\mathfrak{u}}(L(C_U(U_a))) = C_{\mathfrak{u}}(C_{\mathfrak{u}}(\mathfrak{g}_a)) = \sum_{c \in J} \mathfrak{g}_c.$$

Note that $C_U C_U(U_a)$ is unipotent and invariant under the conjugation of T. Hence it is connected. Thus by the one-to-one correspondence between connected subgroups and the related Lie subalgebras we obtain (2.4) immediately from the above identities.

LEMMA 2.9. *Let a be a positive root. Then* $C_{U(R)}(U_a(Q))$ *is Zariski dense in* $C_U(U_a)$.

PROOF. It follows from Lemma 2.7 that $U_b(R) \subseteq C_{U(R)}(U_a(Q))$ for all $b \in I$. Since $U_a(Q)$ is Zariski dense in U_a by Lemma 2.1, we then have

$$\langle U_b(R) \mid \forall b \in I \rangle \subseteq C_{U(R)}(U_a(Q)) = C_{U(R)}(U_a) \subseteq C_U(U_a). \tag{2.5}$$

Moreover, the Zariski density of $U_b(R)$ in U_b for all $b \in \Phi^+$ implies

$$\mathrm{cl}(\langle U_b(R) \mid \forall b \in I \rangle) = \langle \mathrm{cl}(U_b(R)) \mid \forall b \in I \rangle = \langle U_b \mid \forall b \in I \rangle = C_U(U_a).$$

Hence, taking the Zariski closures of the subgroups in (2.5), we obtain

$$\mathrm{cl}(C_{U(R)}(U_a(\boldsymbol{Q})))=C_U(U_a)\,.$$

3. Automorphisms of $E(R)$. In this section we describe the automorphisms of $E(R)$, which will play a key role in the proofs of our main results.

LEMMA 3.1. *Let H be an absolutely almost simple algebraic group over K. If there exists a homomorphism from $E(\boldsymbol{Q})$ to H with Zariski dense image, then*

$$\dim H=\dim G(K)\,.$$

For the proof of Lemma 3.1, see [7, Cor. 2.4].

PROPOSITION 3.2. *Every nontrivial homomorphism from $E(\boldsymbol{Q})$ to $G(K)$ has a Zariski dense image.*

PROOF. Let $\alpha: E(\boldsymbol{Q})\to G(K)$ be a non trivial homomorphism. We first show that the Zariski closure of $\alpha(E(\boldsymbol{Q}))$ in $G(K)$ is connected. Let δ be the natural homomorphism from $\mathrm{cl}(\alpha(E(\boldsymbol{Q})))$ to its quotient group $\mathrm{cl}(\alpha(E(\boldsymbol{Q})))/\mathrm{cl}(\alpha(E(\boldsymbol{Q})))^\circ$. Consider a composite of homomorphisms $\delta\alpha=\beta: E(\boldsymbol{Q})\to\mathrm{cl}(\alpha(E(\boldsymbol{Q})))/\mathrm{cl}(\alpha(E(\boldsymbol{Q})))^\circ$. Then $|E(\boldsymbol{Q})/\ker\beta|<\infty$ since $\mathrm{cl}(\alpha(E(\boldsymbol{Q})))/\mathrm{cl}(\alpha(E(\boldsymbol{Q})))^\circ$ is a finite group. This implies that, since $E(\boldsymbol{Q})$ is infinite and simple, $E(\boldsymbol{Q})=\ker\beta$. Thus we have

$$\alpha(E(\boldsymbol{Q}))\subseteq\mathrm{cl}(\alpha(E(\boldsymbol{Q})))^\circ\subseteq\mathrm{cl}(\alpha(E(\boldsymbol{Q})))\,.$$

Taking the Zariski closures of the above groups simultaneously, we obtain immediately that $\mathrm{cl}(\alpha(E(\boldsymbol{Q})))^\circ=\mathrm{cl}(\alpha(E(\boldsymbol{Q})))$.

We show next that $\mathrm{cl}(\alpha(E(\boldsymbol{Q})))$ and $G(K)$ have the same dimension. Then the connectedness of $\mathrm{cl}(\alpha(E(\boldsymbol{Q})))$ yields immediately that $\mathrm{cl}(\alpha(E(\boldsymbol{Q})))=G(K)$. Since $E(\boldsymbol{Q})$ is equal to its commutator subgroup, we have

$$[\mathrm{cl}(\alpha(E(\boldsymbol{Q}))),\,\mathrm{cl}(\alpha(E(\boldsymbol{Q})))]=\mathrm{cl}([\alpha(E(\boldsymbol{Q})),\,\alpha(E(\boldsymbol{Q}))])=\mathrm{cl}(\alpha(E(\boldsymbol{Q})))\,.$$

In particular, $\mathrm{cl}(\alpha(E(\boldsymbol{Q})))$ is not a solvable group and, hence, $\mathrm{cl}(\alpha(E(\boldsymbol{Q})))/\mathscr{R}$ is a nontrivial semisimple group, where $\mathscr{R}$ is the radical. Let $\{G_i\}_{i=1}^m$ be the family of simple components of $\mathrm{cl}(\alpha(E(\boldsymbol{Q})))/\mathscr{R}$ and G_i^{ad} the adjoint simple algebraic group of the same type as G_i for $1\leqslant i\leqslant m$. Then there exists an isogeny $\varepsilon: \mathrm{cl}(\alpha(E(\boldsymbol{Q})))/\mathscr{R}\to\prod_{i=1}^m G_i^{\mathrm{ad}}$. Let π be the natural morphism from $\mathrm{cl}(\alpha(E(\boldsymbol{Q})))$ to $\mathrm{cl}(\alpha(E(\boldsymbol{Q})))/\mathscr{R}$ and p_j the projection of $\prod_{i=1}^m G_i^{\mathrm{ad}}$ to the j-th factor G_j^{ad} for $1\leqslant j\leqslant m$. Note that the image of a Zariski dense subset under the map p_j (resp. ε and π) is also a Zariski dense subset. Hence the composite $p_j\varepsilon\pi$ preserves the Zariski density. In particular, we have for $1\leqslant j\leqslant m$

$$\mathrm{cl}(p_j\varepsilon\pi\alpha E(\boldsymbol{Q}))=p_j\varepsilon\pi(\mathrm{cl}(\alpha E(\boldsymbol{Q})))=G_j^{\mathrm{ad}}\,,$$

which means that the composite $p_j\varepsilon\pi\alpha$ is a homomorphism from $E(\boldsymbol{Q})$ to G_j^{ad} with Zariski dense image. It follows from Lemma 3.1 that

$$\dim G = \dim G_j^{\mathrm{ad}} = \dim G_j \leqslant \dim \mathrm{cl}(\alpha(E(\boldsymbol{Q})))/\mathscr{R} \leqslant \dim \mathrm{cl}(\alpha(E(\boldsymbol{Q}))) \leqslant \dim G .$$

This implies that $\dim \mathrm{cl}(\alpha(E(\boldsymbol{Q}))) = \dim G(K)$. Hence $\alpha(E(\boldsymbol{Q}))$ is Zariski dense in $G(K)$.

PROPOSITION 3.3. *Let H be a subgroup of $G(R)$ which contains $E(R)$. If α is an automorphism of H, then there exists an element $g \in G(R)$ such that*

$$(\mathrm{Int}\, g) \cdot \alpha(E(\boldsymbol{Q})) = E(\boldsymbol{Q}) .$$

PROOF. Since the restriction of α to $E(\boldsymbol{Q})$ is a homomorphism from $E(\boldsymbol{Q})$ to $G(K)$ with a Zariski dense image by Proposition 3.2, it follows from the Borel-Tits theorem [4] that there exist a homomorphism of fields $\varphi: \boldsymbol{Q} \to K$ and an isogeny ε from ${}^{\varphi}G(K)$, the group obtained by the base change through φ, to $G(K)$ such that

$$\alpha(h) = \varepsilon\varphi^{\circ}(h) , \qquad \text{for all} \quad h \in E(\boldsymbol{Q}) ,$$

where φ° is the canonical morphism from $G(K)$ to ${}^{\varphi}G(K)$ induced by φ (for the notations see [4]). Note that φ is in fact the natural embedding, which implies that φ° is the identity map. This yields

$$\alpha(h) = \varepsilon(h) , \qquad \text{for all} \quad h \in E(\boldsymbol{Q}) . \tag{3.1}$$

Since char $K=0$, the isogeny ε is an automorphism of the algebraic group G by [8, EXP. 23, 24], which can be written in the form (see [3, §14.9])

$$\varepsilon = (\mathrm{Int}\, g^{-1}) \cdot \tilde{\gamma} , \tag{3.2}$$

where $g \in G(R)$ and $\tilde{\gamma}$ is a graph automorphism of G related to an automorphism γ,of Φ. It is easily seen from the definition of a graph automorphism that

$$\tilde{\gamma}(E(\boldsymbol{Q})) = E(\boldsymbol{Q}) , \tag{3.3}$$

hence we have from (3.1) and (3.2)

$$(\mathrm{Int}\, g) \cdot \alpha(E(\boldsymbol{Q})) = \mathrm{Int}\, g \cdot \varepsilon(E(\boldsymbol{Q})) = E(\boldsymbol{Q}) .$$

We claim that g actually belongs to $G(R)$. This is because, for each $a \in \Phi$, we have by (3.1) and (3.3)

$$(\mathrm{Int}\, g^{-1})(u_a(1)) = (\mathrm{Int}\, g^{-1}) \cdot \tilde{\gamma}(\tilde{\gamma}^{-1}(u_a(1))) = \varepsilon(\tilde{\gamma}^{-1}(u_a(1))) = \alpha(\tilde{\gamma}^{-1}(u_a(1))) \in H \subseteq G(R) ,$$

which implies by Lemma 2.5 that g^{-1}, hence also g, lies in $G(R)$.

COROLLARY 3.4. *Suppose α is an automorphism of $E(R)$. Then there exist an element $g \in G(R)$ and a graph automorphism $\tilde{\gamma}$ of $E(R)$ such that*

$$\tilde{\gamma} \cdot (\mathrm{Int}\, g) \cdot \alpha(q) = q , \qquad \text{for all} \quad q \in E(\boldsymbol{Q}) .$$

PROOF. Since each graph automorphism of $G(R)$ induces by the restriction a graph automorphism of $E(R)$. This result follows from (3.1) and (3.2) where $\tilde{\gamma}$ is replaced by $\tilde{\gamma}^{-1}$.

LEMMA 3.5. *If α is an automorphism of $E(R)$ which fixes each element in $E(\boldsymbol{Q})$, then* $\alpha(U(R))=U(R)$.

PROOF. We have $\alpha(B\cap E(R))\supseteq B\cap E(\boldsymbol{Q})$. Taking the Zariski closures of the above subgroups in $G(K)$, we obtain from Corollary 2.2, (iii) that

$$\mathrm{cl}(\alpha(B\cap E(R)))\supseteq \mathrm{cl}(B\cap E(\boldsymbol{Q}))=B\,.$$

Note that B is a maximal solvable subgroup and that $\mathrm{cl}(\alpha(B(R))$ is solvable since so is $\alpha(B(R))$. Thus we have $\mathrm{cl}(\alpha(B\cap E(R)))=B$. In particular, this implies

$$\alpha(U(R))\subseteq B\,. \tag{3.4}$$

Let $a\in\Phi^+$. We can choose an element $h\in T\cap E(\boldsymbol{Q})$ such that $\alpha(h)\neq 1$ since $T\cap E(\boldsymbol{Q})$ is Zariski dense in T by Lemma 2.2, (i). Then we have

$$hu_a(r)h^{-1}u_a(r)^{-1}=u_a((a(h)-1)r)\,,\qquad \text{for all}\quad a\in\Phi^+ \text{ and } r\in R\,, \tag{3.5}$$

which implies that $U_a(R)\subseteq[T\cap E(\boldsymbol{Q}),\, U(\boldsymbol{R})]$ for all $a\in\Phi^+$. Thus we obtain by (3.4)

$$\alpha(U(R))\subseteq[\alpha(T\cap E(\boldsymbol{Q})),\, \alpha(U(R))]\subseteq[T,\, B]\cap E(R)=U\cap E(R)=U(R)\,.$$

This implies that $\alpha(U(R))=U(R)$ since α is an isomorphism.

LEMMA 3.6. *Let α be as in Lemma* 3.5. *Then*

$$\alpha(U_a(R))=U_a(R)\,,\qquad \textit{for all}\quad a\in\Phi^+\,. \tag{3.6}$$

PROOF. Suppose a is a positive root. Since $U_a(R)$ is contained in $C_{U(R)}C_{U(R)}(U_a(\boldsymbol{Q}))$, we have by Lemmas 3.5, 2.9 and 2.8 that

$$\begin{aligned}\alpha(U_a(R))&\subseteq C_{U(R)}C_{U(R)}(\alpha(U_a(\boldsymbol{Q})))=C_{U(R)}C_{U(R)}(U_a(\boldsymbol{Q}))\\&=U(R)\cap C_UC_{U(R)}(U_a(\boldsymbol{Q}))=U(R)\cap C_UC_U(U_a)=U(R)\cap\prod_{c\in J}U_c\,,\end{aligned} \tag{3.7}$$

where J is as in Lemma 2.6. Suppose $J=\{c_1, c_2, \dots, c_r\}$ where $c_1=a$. If $r=1$, then $\alpha(U_a(R))\subseteq U(R)\cap U_a=U_a(R)$, from which follows (3.6) since α is an automorphism. Suppose $r\geq 2$. Then $a\neq c_r$ and $(\ker c_r)^\circ\setminus\ker a$ is an open subset of $(\ker c_r)^\circ$. Note that, since $(\ker c_r)^\circ$ splits over $\boldsymbol{Q}$ (cf. [3, CH. III, Cor. 8.7]), $(\ker c_r)^\circ\cap E(\boldsymbol{Q})$ is Zariski dense in $(\ker c_r)^\circ$ by [4, Cor. 6.8]. Hence

$$\{(\ker c_r)^\circ\setminus\ker a\}\cap E(\boldsymbol{Q})=\{(\ker c_r)^\circ\cap E(\boldsymbol{Q})\}\cap\{(\ker c_r)^\circ\setminus\ker a\}\neq\varnothing\,.$$

Let $h\in\{(\ker c_r)^\circ\setminus\ker a\}\cap E(\boldsymbol{Q})$. Then (3.5) and Lemma 2.8 yield

$$U_a(R)=[\langle h\rangle,\, U_a(R)]\quad\text{and}\quad\left[\langle h\rangle,\, \prod_{i=1}^{r}U_{c_i}\right]\subseteq\prod_{i=1}^{r-1}U_{c_i}\,.$$

Thus it follows from (3.7)

$$\alpha(U_a(R)) = [\langle h\rangle, \alpha(U_a(R))] \subseteq \prod_{i=1}^{r-1} U_{c_i} .$$

This gives rise to (3.6) immediately if $r=2$. When $r\geq 3$, we obtain (3.6) by repeating analogous procedures as above.

LEMMA 3.7. *Let* α *be as in Lemma* 3.5. *Then*

$$\alpha(U_a(R)) = U_a(R) , \qquad \text{for all} \quad a \in \Phi .$$

PROOF. Thanks to Lemma 3.6, it is sufficient to show that for all $a\in\Phi^+$

$$\alpha(U_{-a}(R)) = U_{-a}(R) .$$

Write $w_a = u_a(1)u_{-a}(-1)u_a(1)$ for each $a\in\Phi^+$. Then $w_a U_a(R) w_a^{-1} = U_{-a}(R)$. Note that $\alpha(w_a)=w_a$ for all $a\in\Phi^+$. Thus we obtain by Lemma 3.6

$$\alpha(U_{-a}(R)) = w_a(\alpha(U_a(R)))w_a^{-1} = U_{-a}(R) .$$

Let α be as in Lemma 3.5. Since α keeps $U_a(R)$ invariant for all $a\in\Phi$, we can assign a map Φ_a: $R\to R$ to each $a\in\Phi$, which is defined by

$$\alpha(u_a(r)) = u_a(\varphi_a(r)) .$$

φ_a is obviously well-defined and is an automorphism of the additive group R^+.

LEMMA 3.8. *Let* $a\in\Phi$. *Then* φ_a *is an automorphism of* R *and* $\varphi_a=\varphi_b$ *for all* $b\in\Phi$.

PROOF. We first consider the case where a is a fundamental root. Since the rank of G is greater than one, there exists a positive root b such that $a+b\in\Phi$. Let $h\colon \Phi^+\to \boldsymbol{Z}$ be the height function of Φ^+. Then we have by the commutator formula [10, EXP. XXII, §5]

$$u_a(r)u_b(s)u_a(r)^{-1}u_b(s)^{-1} = u_{a+b}(n_{a,b}rs)u , \qquad \text{for} \quad r, s\in R ,$$

where $n_{a,b}$ is an integer determined uniquely by the roots a and b, while u is a product of elements $u_c(t)$ for $t\in R$ and $c\in\Phi^+$ such that $h(c)<h(a+b)$. Applying α on both sides, we obtain

$$u_a(\varphi_a(r))u_b(\varphi_b(s))u_a(\varphi_a(r))^{-1}u_b(\varphi_b(s))^{-1} = u_{a+b}(n_{a,b}\varphi_{a+b}(rs))u' ,$$

where u' is also a product of elements of the form $u_c(t)$ for $c\in\Phi^+$ with $h(c)>h(a+b)$. On the other hand, it follows from the commutator formula that

$$u_a(\varphi_a(r))u_b(\varphi_b(s))u_a(\varphi_a(r))^{-1}u_b(\varphi_b(s))^{-1} = u_{a+b}(n_{a,b}\varphi_a(r)\varphi_b(s))u'' ,$$

where u'' is a product of elements of the form $u_c(t)$ with $h(c)>h(a+b)$. Comparing these two identities, we obtain

(3.8) $$\varphi_{a+b}(rs) = \varphi_a(r)\varphi_b(s) , \qquad \text{for all} \quad r, s\in R .$$

Taking r and s to be 1 respectively, we have

$$\varphi_{a+b}=\varphi_a=\varphi_b .$$

If $c\in\Delta$, then there is a sequence of fundamental roots

$$a=a_1, a_2, \dots, a_m=c$$

such that $a_i+a_{i+1}\in\Phi$ for all $1\leqslant i\leqslant m-1$. Thus we have by the above argument that $\varphi_a=\varphi_c$ for all $c\in\Delta$. Let φ stand for φ_a for all $a\in\Delta$. It follows from (3.8) that $\varphi(rs)=\varphi(r)\varphi(s)$ for all $r, s\in R$, which means that φ is a ring homomorphism and hence φ is an automorphism of R.

We show next that $\varphi_a=\varphi$ for all $a\in\Phi^+$. We use induction on the height of the roots. If a is not a fundamental root, suppose that $\varphi_c=\varphi$ for all $c\in\Phi$ with $h(c)<h(a)$. We can write the root a in the form $b+c$ for some $b, c\in\Phi^+$ with both $h(b)$ and $h(c)$ being smaller than $h(a)$. We then have

$$u_b(r)u_c(s)u_b(r)^{-1}u_c(s)^{-1}=u_a(n_{b,c}rs)v , \qquad \text{for all} \quad r, s\in R ,$$

where $n_{b,c}$ is an integer which depends only on b and c, while v is a product of elements $u_d(t)$ for some $t\in R$ and $d\in\Phi^+$ with $h(d)>h(a)$. Applying α on both sides and using the induction hypothesis, we obtain

$$u_b(\varphi(r))u_c(\varphi(s))u_b(\varphi(r))^{-1}u_c(\varphi(s))^{-1}=u_a(n_{b.c}\varphi_a(rs))v' ,$$

where v' is a product of elements which involves only those positive roots whose height is greater than $h(a)$. On the other hand, we have by the commutator formula that

$$u_b(\varphi(r))u_c(\varphi(s))u_b(\varphi(r))^{-1}u_c(\varphi(s))^{-1}=u_a(n_{b,c}\varphi(r)\varphi(s))v'' ,$$

where v'' is a product of elements involving only the positive roots whose height is greater than $h(a)$. Comparing the above two identities, we obtain that $\varphi_a(rs)=\varphi(r)\varphi(s)$ for all $r, s\in R$. Taking $s=1$, we then have the identity $\varphi_a=\varphi$.

Finally we show that $\varphi_a=\varphi$ for every negative root a, hence $\varphi_b=\varphi$ for all $b\in\Phi$. Let a be a negative root. Then for any $r\in R$

$$u_a(r)=w_{-a}u_{-a}(-r)w_{-a}^{-1} .$$

Applying α on both sides, we have

$$u_a(\varphi_a(r))=w_{-a}u_{-a}(-\varphi(r))w_{-a}^{-1}=u_a(\varphi(r)) .$$

Thus $\varphi_a=\varphi$. This completes our proof.

THEOREM 3.9. *Every automorphism α of $E(R)$ has an expression*

$$\alpha=(\operatorname{Int} g)\cdot\tilde{\gamma}\cdot\tilde{\varphi} , \tag{3.9}$$

where $g\in G(R)$, $\tilde{\gamma}$ is a graph automorphism and $\tilde{\varphi}$ is a ring automorphism. Moreover, the factors g, $\tilde{\gamma}$ and *$\tilde{\varphi}$ are uniquely determined by α.*

PROOF. It follows from Corollary 3.4 that there exist an element $g \in G(R)$ and a graph automorphism $\tilde{\gamma}$ of $E(R)$ such that the restriction of $\tilde{\gamma}^{-1} \cdot (\mathrm{Int}\, g^{-1}) \cdot \alpha$ to $E(\boldsymbol{Q})$ is the identity map on $E(\boldsymbol{Q})$. This means by Lemmas 3.7 and 3.8 that $\tilde{\gamma}^{-1}(\mathrm{Int}\, g^{-1}) \cdot \alpha$ is a ring automorphism $\tilde{\varphi}$ for some $\varphi \in \mathrm{Aut}\, R$, from which follows the expression (3.9).

We show now the uniqueness of g, $\tilde{\gamma}$ and $\tilde{\varphi}$. Suppose we have

$$\alpha = (\mathrm{Int}\, g) \cdot \tilde{\gamma} \cdot \tilde{\varphi} = (\mathrm{Int}\, g_1) \cdot \tilde{\gamma}_1 \cdot \tilde{\varphi}_1 ,$$

where $g_1 \in G(R)$, $\tilde{\gamma}_1$ is the graph automorphism of $E(R)$ related to an automorphism γ_1 of Φ and $\tilde{\varphi}_1$ is the ring automorphism related to an automorphism φ_1 of R. Then

$$(3.10) \qquad (\mathrm{Int}\, g_1^{-1}) \cdot (\mathrm{Int}\, g) = \tilde{\gamma}_1 \tilde{\varphi}_1 \tilde{\varphi}^{-1} \tilde{\gamma}^{-1} .$$

Since graph automorphisms and ring automorphisms keep both $U(R)$ and $U^-(R)$ invariant, the above equation implies

$$\begin{aligned} g_1^{-1} g &\in N_{G(R)}(U(R)) \cap N_{G(R)}(U^-(R)) \\ &\subseteq N_{G(R)}(\mathrm{cl}(U(R))) \cap N_{G(R)}(\mathrm{cl}(U^-(R))) = N_{G(R)}(U) \cap N_{G(R)}(U^-) \\ &= G(R) \cap N_G(U) \cap N_G(U^-) = G(R) \cap B \cap B^- = G(R) \cap T . \end{aligned}$$

This yields, for each fundamental root $a \in \Delta$,

$$g_1^{-1} g u_a(1) (g_1^{-1} g)^{-1} = u_a(a(g_1^{-1} g)) .$$

On the other hand, we have

$$\tilde{\gamma}_1 \tilde{\varphi}_1 \tilde{\varphi}^{-1} \tilde{\gamma}^{-1}(u_a(1)) = u_{\gamma_1 \gamma^{-1}(a)}(1) , \qquad \text{for all} \quad a \in \Delta .$$

Comparing the two equations, we obtain $\gamma_1 = \gamma$ and $a(g_1^{-1} g) = 1$ for all $a \in \Delta$. In other words, $g_1^{-1} g \in \bigcap_{a \in \Delta} \ker a = C(G(K))$. This implies immediately $g = g_1$ and hence $\varphi_1 = \varphi$ by (3.10).

4. Automorphisms of $G(R)$ and its subgroups. In this section we give the proofs of the theorems stated in §1. Notation is the same as that in the previous sections.

LEMMA 4.1. *Let H be a subgroup of $G(R)$ with contains $E(R)$ and α an automorphism of H. If α fixes every element of $E(R)$, then α is the identity map on H.*

PROOF. Since $E(R)$ is a normal subgroup of H by [16], we have for all $h \in H$

$$h g h^{-1} = \alpha(h g h^{-1}) = \alpha(h) g \alpha(h)^{-1} , \qquad \text{for all} \quad g \in E(R) .$$

This yields

$$(\alpha(h)^{-1} h) g = g (\alpha(h)^{-1} h) , \qquad \text{for all} \quad g \in E(R) , \quad h \in H ,$$

which means that, since $E(R)$ is Zariski dense in $G(K)$,

$$\alpha(h)^{-1} h \in C_H(E(R)) = C_H(G(K)) .$$

Since G is of adjoint type, $C_H(G(K))$ is trivial. Hence we obtain that $\alpha(h)=h$ for all $h\in H$.

PROPOSITION 4.2. (i) *Every automorphism of* $E(R)$ *can be extended uniquely to an automorphism of* $G(R)$;

(ii) *If* H *is a subgroup of* $G(R)$ *which contains* $E(R)$, *the restriction of each automorphism of* H *to* $E(R)$ *is an automorphism of* $E(R)$.

In particular, $\operatorname{Aut} G(R)\cong \operatorname{Aut} E(R)$.

PROOF. (i) Let α be an automorphism of $E(R)$. We know by Theorem 3.9 that α has an expression of the form $(\operatorname{Int} g)\cdot\tilde{\gamma}\cdot\tilde{\varphi}$, where $g\in G(R)$, $\tilde{\gamma}$ is a graph automorphism and $\tilde{\varphi}$ is the ring automorphism of $E(R)$ related to an automorphism $\varphi\in\operatorname{Aut} R$. It is evident that $\tilde{\gamma}$ can be extended to a graph automorphism of $G(R)$ by definition. Let $\bar{\varphi}$ be the ring automorphism of $G(R)$ related to φ. We show that the restriction of $\bar{\varphi}$ to $E(R)$ coincides with $\tilde{\varphi}$. Identifying $G(R)$ with $\operatorname{Hom}_{\boldsymbol{Q}\text{-alg}}(\boldsymbol{Q}[G], R)$, where $\boldsymbol{Q}[G]$ is the $\boldsymbol{Q}$-regular function ring of G, we can easily see that $\bar{\varphi}$ is defined by

$$\bar{\varphi}(g)(f)=\varphi(g(f))\,,\qquad \text{for}\quad g\in G(R)\quad\text{and}\quad f\in\boldsymbol{Q}[G]\,. \tag{4.1}$$

Suppose $a\in\Phi$. Let $\iota\colon U_a\to G$ be the natural embedding and $\iota^*\colon \boldsymbol{Q}[G]\to\boldsymbol{Q}[U_a]$ the homomorphism of $\boldsymbol{Q}$-algebras induced by ι in the canonical way, where $\boldsymbol{Q}[U_a]$ is the $\boldsymbol{Q}$-regular function ring of U_a. Then an element g belongs to $U_a(R)$ if and only if there exists an element $g'\in\operatorname{Hom}_{\boldsymbol{Q}\text{-alg}}(\boldsymbol{Q}[U_a], R)$ such that $g=g'\iota^*$. Thus, given $\varphi\in\operatorname{Aut} R$, we have a commutative diagram

$$\begin{tikzcd}
\boldsymbol{Q}[G] \arrow[r, "\iota^*"] \arrow[d, "\bar{\varphi}(g)"'] \arrow[dr, "g"] & \boldsymbol{Q}[U_a] \arrow[d, "g'"] \\
R \arrow[r, "\varphi"] & R
\end{tikzcd}$$

which implies immediately $\bar{\varphi}(U_a(R))=U_a(R)$, for all $a\in\Phi$. This, together with (4.1) (see also [1, §1.3]), yields

$$\bar{\varphi}(u_a(r))=u_a(\varphi(r))\,,\qquad\text{for all}\quad r\in R\quad\text{and}\quad a\in\Phi\,.$$

Comparing this identity with (1.2), we see that $\bar{\varphi}$ is an extension of $\tilde{\varphi}$. Therefore, α can be extended to an automorphism $\tilde{\alpha}$ in an obvious way. If $\bar{\alpha}\in\operatorname{Aut} G(R)$ is also an extension of α, then $\bar{\alpha}\cdot\tilde{\alpha}^{-1}$ fixes every element of $E(R)$ and, hence, $\tilde{\alpha}=\bar{\alpha}$ by Lemma 4.1. Thus the extension of α to an automorphism of $G(R)$ is unique.

(ii) Suppose α is an automorphism of H. Then it follows from Proposition 3.3 that there exists an element $g\in G(R)$ such that the homomorphism $(\operatorname{Int} g)\cdot\alpha\colon H\to G(R)$ keeps $E(\boldsymbol{Q})$ invariant. In other words, we have $E(\boldsymbol{Q})\subseteq\operatorname{Int} g\cdot\alpha(H)=gHg^{-1}$. Hence it follows from Proposition 2.3 that

$$E(R)=\bigcap_{N\in P} N=\bigcap_{N'\in P'} N'\,,$$

where P is the set of normal subgroups of H which contains $E(\boldsymbol{Q})$ while P' is the set of normal subgroups of gHg^{-1} which contains $E(\boldsymbol{Q})$. Note that $(\operatorname{Int} g)\cdot\alpha$ induces a one-to-one correspondence between P and P'. Thus we obtain

$$((\operatorname{Int} g)\cdot\alpha)(E(R))=((\operatorname{Int} g)\cdot\alpha)\Bigl(\bigcap_{N\in P} N\Bigr)=\bigcap_{N'\in P'} N'=E(R).$$

This implies, since $E(R)$ is a normal subgroup of $G(R)$ by [16], that $\alpha(E(R))=E(R)$.

In particular, on taking H to be $G(R)$, we obtain from (i) and (ii) that the restriction of the automorphisms of $G(R)$ to $E(R)$ yields an isomorphism from $\operatorname{Aut} G(R)$ to $\operatorname{Aut} E(R)$.

THE PROOF OF THEOREM 1. Thanks to Propositon 4.2, we only need to show that every automorphism of H can be extended uniquely to an automorphism of $G(R)$. Let $\alpha\in\operatorname{Aut} H$ and write α' for the restriction of α to $E(R)$, which is an automorphism of $E(R)$ by Proposition 4.2, (ii). It follows from Proposition 4.2, (i) that α' can be extended uniquely to an automorphism $\tilde\alpha$ of $G(R)$. We claim that $\tilde\alpha$ is also an extension of α. Indeed, we have for any $g\in E(R)$

$$(\tilde\alpha\cdot\alpha^{-1})(g)=\tilde\alpha(\alpha'^{-1}(g))=\alpha'(\alpha'^{-1}(g))=g.$$

Therefore, since $E(R)$ is a normal subgroup of H by [16], we have

$$hgh^{-1}=(\tilde\alpha\cdot\alpha^{-1})(hgh^{-1})=\tilde\alpha(\alpha^{-1}(h))g(\tilde\alpha\cdot\alpha^{-1}(h))^{-1}, \qquad \text{for all} \quad g\in E(R).$$

This yields

$$\tilde\alpha(\alpha^{-1}(h))^{-1}hg=g(\tilde\alpha(\alpha^{-1}(h))^{-1}h), \qquad \text{for all} \quad g\in E(R) \text{ and } h\in H.$$

Hence

$$\tilde\alpha(\alpha^{-1}(h))^{-1}h\in C_{G(k)}(E(R))=C(G(K))=\{1\}, \qquad \text{for all} \quad h\in H.$$

Thus we obtain that $\tilde\alpha(h)=\alpha(h)$, for all $h\in H$. Suppose $\bar\alpha\in\operatorname{Aut} G(R)$ is also an extension of α. Then $\tilde\alpha\cdot\bar\alpha^{-1}$ is the identity map on H and hence is also the identity map on $E(R)$. This implies by Lemma 4.1 that $\tilde\alpha\cdot\bar\alpha^{-1}$ is the identity map on $G(R)$. Thus $\tilde\alpha=\bar\alpha$ and the extension of α to an automorphism of $G(R)$ is unique.

THE PROOF OF THEOREM 2. (i) See the proof of Proposition 4.2, (i).

(ii) It follows from the definitions of graph automorphisms and ring automorphisms that $G(R)$ is a normal subgroup of both A and B. Moreover, let S be the group of automorphisms of Φ which keep Δ invariant. Then for any $\gamma\in S$, $\varphi\in\operatorname{Aut} R$ and $a\in\pm\Delta$, we have

$$\tilde\gamma\tilde\varphi(u_a(r))=\tilde\gamma(u_a(\varphi(r)))=u_{\gamma(a)}(\varphi(r))=\tilde\varphi(u_{\gamma(a)}(r))=\tilde\varphi\tilde\gamma(u_a(r)), \qquad \text{for all} \quad r\in R.$$

This implies that $\tilde\gamma\tilde\varphi(g)=\tilde\varphi\tilde\gamma(g)$, for all $g\in E(R)$. We obtain therefore from Lemma 4.1

$$\tilde\gamma\tilde\varphi=\tilde\varphi\tilde\gamma, \qquad \text{for all} \quad \gamma\in S \text{ and } \varphi\in\operatorname{Aut} R, \tag{4.2}$$

from which follow the normal sequences (1.4) and (1.5) immediately.

(iii) The normal sequences (1.4) and (1.5), together with the uniqueness of the expression (1.3), give rise to the following structure of the automorphisms group of H:

$$A \cong G(R) \rtimes S\,; \quad B \cong G(R) \rtimes \operatorname{Aut} R\,.$$

Hence, it follows from (4.2) that

$$\operatorname{Aut} H \cong G(R) \rtimes (S \times \operatorname{Aut} R)\,,$$

from which follow the isomorphisms (1.6), (1.7) and (1.8). Finally, the structure of S is well-known (see, for instance, [10, EXP. XXI, §7.4.6]).

THE PROOF OF THEOREM 3. It follows from Theorem 1 that each automorphism $\alpha \in \operatorname{Aut} H$ is the restriction of an automorphism, say $\tilde{\alpha}$, of $G(R)$. We know from Theorem 2 that $\tilde{\alpha}$ is a product of the form $(\operatorname{Int} g) \cdot \tilde{\gamma}\tilde{\varphi}$ for some $g \in G(R)$, $\gamma \in S$ and $\varphi \in \operatorname{Aut} R$. Note that $\tilde{\gamma}$ can be extended to a graph automorphism of the algebraic group $G(K)$ in an obvious and unique way, and so does $\operatorname{Int} g$. Hence $(\operatorname{Int} g) \cdot \tilde{\gamma}$ can also be extended to an automorphism of the algebraic group $G(K)$. Denote this extension of $(\operatorname{Int} g) \cdot \tilde{\gamma}$ by β and we then have the expression (1.8). The uniqueness of β and φ is obvious.

REFERENCES

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

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

[3] A. BOREL, Linear algebraic groups, 2nd enl. ed., Springer-Verlag, New York, 1991.

[4] A. BOREL AND J. TITS, Homomorphismes "abstraits" de groupes algébrique simples, Ann. of Math. 97 (1973), 499–571.

[5] N. BOURBAKI, Groupes et algèbres de Lie, Chaps. II and III, Hermann, Paris, 1972.

[6] Y. CHEN, Homomorphisms of two dimensional linear groups over Laurent polynomial rings and Gaussian domains, Math. Proc. Cambridge Phil. Soc. 109 (1991), 287–297.

[7] Y. CHEN, Isomorphic Chevalley groups over integral domains, Rendiconti Sem. Mat. Padova (to appear).

[8] C. CHEVALLEY, Séminaire sur la classification des groupes de Lie algébriques, Notes polycopiées, Inst. H. Poincaré, Paris, 1956–58.

[9] C. CHEVALLEY, Certains schémas des groupes semi-simples, Sém. Bourbaki 13 (1960), Exp. 219, 1–16.

[10] M. DEMAZURE AND A. GROTHENDIECK, Schémas en groupes III, Lecture Notes in Math. 153, Springer-Verlag, Berlin-Heidelberg-New York, 1970.

[11] A. HAHN, D. JAMES AND B. WEISFEILER, Homomorphisms of algebraic and classical groups: a survey, Canad. Math. Soc. Conf. Proc. 4 (1984), 249–296.

[12] J. HUMPHREYS, On the automorphisms of infinite Chevalley groups, Canad. J. Math. 21 (1969), 908–911.

[13] O. SCHREIER AND B. L. VAN DER WAERDEN, Die Automorphismen der projektiven Gruppen, Abh. Math. Sem. Univ. Hamburg 6 (1928), 303–322.

[14] R. STEINBERG, Automorphisms of finite linear groups, Canad. J. Math. 12 (1960), 606–615.

[15] R. STEINBERG, Lectures on Chevalley groups, Yale Univ. Lecture Notes, 1967.

[16] G. TADDEI, Normalité des groupes élémentaire dans les groupes de Chevalley sur un anneau, Contemp. Math. 55 (1986), 693–710.

[17] J. TITS, Travaux de Margulis sur les sous-groupes discrete de Lie, Lecture Notes in Math. 567, Springer-Verlag, Berlin-Heidelberg-New York, 1977, 174–190.

DIPARTIMENTO DI MATEMATICA
UNIVERSITÀ DI TORINO
VIA CARLO ALBERTO, 10
10123 TORINO
ITALY