

ON ALGEBRAIC GROUPS DEFINED BY NORM FORMS OF SEPARABLE EXTENSIONS

TAKASHI ONO

Let K be any field, and L a separable extension of K of finite degree. L has a structure of vector space over K , and we shall denote this space by V . The space of endomorphisms of V will be denoted by $\mathfrak{E}(V)$. Let x be any element of L , and $N(x)$ the norm of x relative to the extension L/K . N is then a function defined on V with values in K . We shall call N the norm form on V . The multiplicative groups of non-zero elements of K and L will be denoted by K^* and L^* respectively. Let H be any subgroup of K^* . Then the elements z of L^* such that $N(z) \in H$ form a subgroup of L^* , which we shall denote by G_H . On the other hand the elements s of $\mathfrak{E}(V)$ such that $N(sx) = \lambda(s)N(x)$ with $\lambda(s) \in H$ for all $x \in V$, form obviously a subgroup of $GL(V)$, which we shall denote by $\tilde{G}_H$. $\tilde{G}_H$ becomes an algebraic group if $H = K^*$ or $\{1\}$. In case $H = K^*$, $\tilde{G}_H = \tilde{G}_{K^*}$ will mean the group of linear transformations of V leaving semi-invariant the norm form of L/K and in case $H = \{1\}$, $\tilde{G}_H = \tilde{G}_{(1)}$ will mean the group of linear transformations of V leaving invariant the norm form of L/K .

The object of this paper is to investigate the structure of these groups $\tilde{G}_H$, particularly in the cases $H = K^*$ and $H = \{1\}$. Our result in most general form reads in Proposition 2, which is obtained under a sole hypothesis that K contains infinitely many elements. Theorems 1 and 2 correspond respectively to the cases $H = K^*$ and $H = \{1\}$. Theorem 2 will show in particular that $G_{(1)}$ is the algebraic component of $\tilde{G}_{(1)}$, and if L/K is normal, $\tilde{G}_{(1)}$ may be considered as a semi-direct product¹⁾ of $G_{(1)}$ and the Galois group of L/K . Theorem 3 gives the center of $\tilde{G}_H$.

The significance of the group $G_{(1)}$ as an algebraic group was indicated by Chevalley.²⁾ The groups $G_{(1)}$ and $\tilde{G}_{(1)}$ may be regarded as analogues of special

Received August 18, 1956.

¹⁾ For definition, see p. 127, footnote 3).

²⁾ Théorie des groupes de Lie: Vol. 2, Hermann, Paris, 1951, p. 170. We shall quote this book as C. II. We shall also quote Vol. 3 (1955) of the series as C. III.

orthogonal and orthogonal groups respectively. The groups G_H and $\tilde{G}_H$ have arithmetic meanings when K is the field of rational numbers, and we have in mind to investigate further arithmetic applications on later occasion.

Now, we denote by $\mathfrak{G}$ the group of automorphisms of L leaving invariant each element of K . For simplicity we shall call $\mathfrak{G}$ the automorphism group of L/K . Obviously $\mathfrak{G}$ is a subgroup of $GL(V)$. Each element $z \in L$ defines an endomorphism $\mu(z)$ of V by

$$(1) \quad \mu(z)(x) = zx, \quad x \in V.$$

The mapping μ is clearly an isomorphism of V into $\mathfrak{G}(V)$, and we have $\mu(L^*) = \mu(V) \cap GL(V)$. It follows at once that $\mu(G_H) \subset \tilde{G}_H$ and $\mathfrak{G} \subset \tilde{G}_{(1)}$. We shall set $G = G_{(1)}$ and $\tilde{G} = \tilde{G}_{(1)}$.

PROPOSITION 1. *For any $H \subset K^*$, we have $\mathfrak{G} \cap \mu(G_H) = \{\varepsilon\}$ where ε is the identity endomorphism in $\mathfrak{G}(V)$.*

Proof. Take an element $\mu(z) \in \mathfrak{G} \cap \mu(G_H)$. Then, it follows that $1 = \mu(z)(1) = z$ and $\mu(z) = \varepsilon$.

PROPOSITION 2. *Assume that K is an infinite field. Then, for any $H \subset K^*$, we have $\tilde{G}_H = \mu(G_H)\mathfrak{G}$.*

Proof. Let N be a Galois extension of K containing L . We denote by $\mathfrak{H}$ and $\mathfrak{R}$ the Galois groups of N/K and N/L respectively. Let $\sigma(\omega)$, $\omega \in N$, $\sigma \in \mathfrak{H}$ be a normal base of N/K . By some representatives τ_i , $1 \leq i \leq n$, of right cosets of $\mathfrak{H}$ modulo $\mathfrak{R}$, we put $\eta_i = \sum_{\sigma \in \mathfrak{R}} \sigma \tau_i(\omega)$, $1 \leq i \leq n$, where we set $\tau_1 = 1$, the identity in $\mathfrak{H}$. It follows at once that η_i form a base of L/K . Let V^N be the scalar extension of V with respect to N . We define elements λ_j , $1 \leq j \leq n$, in the dual space $(V^N)^*$ by putting $\lambda_j(\eta_i) = \tau_j(\eta_i)$, $1 \leq i, j \leq n$. Since $\det(\tau_j(\eta_i)) \neq 0$, λ_j , $1 \leq j \leq n$, form a base of $(V^N)^*$. For $x = \sum_i x_i \eta_i \in V$, we have $N(x) = \prod_j (\sum_i x_i \tau_j(\eta_i)) = \prod_j \lambda_j(x)$. We set $(\eta(s)\lambda)(x) = \lambda(sx)$ for $s \in \mathfrak{G}(V^N)$, $\lambda \in (V^N)^*$, $x \in V^N$. Then clearly we have $\eta(s)\lambda \in (V^N)^*$ and we get $\eta(s)\lambda_j = \sum_k a_{kj} \lambda_k$ with $a_{kj} \in N$. Now let s be any element of $\tilde{G}_H$. Then, we have $\prod_j (\sum_k a_{kj} \lambda_k)(x) = \lambda(s) \prod_j \lambda_j(x)$ for all $x \in V$. As K contains infinitely many elements, this implies that $\prod_j (\sum_k a_{kj} \lambda_k) = \lambda(s) \prod_j \lambda_j$ in the symmetric algebra on V^N . Thus, by a well known theorem on the decomposition of polynomials, there exists an integer $k(j)$ for each j such that $k(j) \neq k(j')$ if $j \neq j'$, and

$a_{kj} \neq 0$ if and only if $k = k(j)$. Therefore we have $\eta(s)\lambda_j = a_j \lambda_{k(j)}$, $a_j \in N^*$. In particular for $j=1$, we get $s(\eta_i) = \lambda_1(s\eta_i) = (\eta(s)\lambda_1)(\eta_i) = a_1 \tau_{k(1)}(\eta_i)$, $1 \leq i \leq n$. Since we have $\sum_i \tau_{k(1)}(\eta_i) = \sum_{\sigma \in \mathfrak{G}} \omega^\sigma \in K^*$ and $s(\eta_i) \in L$, this implies that $a_1 \in L$ and we see that $\tau_{k(1)} \in \mathfrak{G}$. As we have $N(sx) = N(a_1 \tau_{k(1)}(x)) = N(a_1)N(x)$, it follows that $N(a_1) = A(s) \in H$. Thus we have $s = \mu(a_1)\tau_{k(1)} \in \mu(G_H)\mathfrak{G}$. q.e.d.

As an immediate consequence of the two propositions, we get the following

COROLLARY. *If K contains infinitely many elements, $\tilde{G}_H$ is a semi-direct product of $\mu(G_H)$ and $\mathfrak{G}^3$.*

Suppose now K is infinite. We shall restrict our attention to the case where H is algebraic, i.e. $H = K^*$ or $H = \{1\}$. The mapping μ , which is a linear isomorphism of V onto $\mu(V)$, gives also a homeomorphism of V onto $\mu(V)$ in the sense of Zariski-topology, and every closed set in $\mu(V)$ is also closed in $\mathfrak{E}(V)$ since $\mu(V)$, being a linear subspace of $\mathfrak{E}(V)$, is closed in $\mathfrak{E}(V)$. Also each irreducible set of V is mapped on an irreducible set of $\mu(V)$ and vice versa, and every irreducible set in $\mu(V)$ is irreducible in $\mathfrak{E}(V)$.⁴ Since $\mu(L^*) = \mu(V) \cap GL(V)$, $\mu(L^*)$ is an algebraic group on V and is irreducible as an open subset in $\mu(V)$. By Proposition 2, the group $\tilde{G}_K^*$ has $\mu(G_K^*) = \mu(L^*)$ as a subgroup of a finite index. Thus we get by the above corollary the following

THEOREM 1. *Let K be an infinite field and L/K a separable extension of finite degree. Then, the group $\tilde{G}_K^*$ of all linear transformations of L over K which leave semi-invariant the norm form of L/K is algebraic on the vector space L over K and $\mu(L^*)$ is the algebraic component of $\tilde{G}_K^*$, μ being defined by (1). Furthermore $\tilde{G}_K^*$ is the semi-direct product of $\mu(L^*)$ and $\mathfrak{G}$, where $\mathfrak{G}$ is the automorphism group of L/K .*

Next, we shall consider the group $\tilde{G}$, i.e. the group of all linear transformations of V leaving invariant the norm form of L/K . Of course $\tilde{G}$ is an algebraic group on V . G being closed in V , $\mu(G)$ is also algebraic. We define a rational representation $\tilde{N}$ of $\mu(L^*)$ by $\tilde{N}(\mu(x)) = N(x)$, $x \in L^*$. Let H be the smallest algebraic group containing $\tilde{N}(\mu(L^*))$. Then, H is irreducible

³) We say that a group G is a semi-direct product of a normal subgroup N and a subgroup H if we have $G = N \cdot H$ and $N \cap H = \{e\}$, e being the identity in G . We see that $\mu(G_H)$ is normal in $\tilde{G}_H$ by the relation $\sigma\mu(z)\sigma^{-1} = \mu(\sigma(z))$, $z \in L$, $\sigma \in \mathfrak{G}$,

⁴) Cf. C. III. Chap. VI §1,

and $H = \{1\}$ or $H = K^*$. But as K is infinite, $\tilde{N}(\mu(L^*)) \cong \{1\}$ and we have $H = K^*$. Since $\mu(G)$ is the kernel of the representation $\tilde{N}$, it follows that $\dim_K \mu(G) \leq n-1$, where $n = [L : K]$.⁵⁾ On the other hand, we shall define a homomorphism ρ of L^* into itself by $\rho(x) = x^{-n}N(x)$, $x \in L^*$. Obviously we have $\rho(L^*) \subset G$ and ρ induces a rational representation $\tilde{\rho}$ of $\mu(L^*)$ in $\mu(G)$ by $\tilde{\rho}(\mu(x)) = \mu(\rho(x))$, $x \in L^*$. We denote by H the smallest algebraic group containing $\tilde{\rho}(\mu(L^*))$. If we take an algebraically closed field M containing K , then we have $H^M = (\tilde{\rho})^M(\mu(L^*)^M)$.⁶⁾ We denote by μ^M the unique extension of μ to $V^M = L^M$. Let $(L^M)^*$ be the group of all invertible elements of L^M which is considered as an algebra over M . It follows that $\mu^M((L^M)^*) = \mu^M(L^M) \cap GL(V^M) = \overline{\mu(L)} \cap GL(V^M) = \overline{\mu(L^*)} \cap GL(V^M) = \mu(L^*)^M$, where $\overline{\mu(L)}$ and $\overline{\mu(L^*)}$ mean the closures of $\mu(L)$ and $\mu(L^*)$ in V^M respectively. Let ρ^M be the unique extension of ρ to $(L^M)^*$. It follows that $\dim_K H = \dim_M H^M = \dim_M (\tilde{\rho})^M(\mu(L^*)^M) = \dim_M \mu^M(\rho^M((L^M)^*)) = \dim_M \rho^M((L^M)^*)$. Since L/K is separable and M is algebraically closed, we have $V^M = L^M = Me_1 + \dots + Me_n$ with primitive idempotents e_i , $1 \leq i \leq n$. Let $x = \sum_i x_i e_i$ be in the kernel of the homomorphism ρ^M . From the relation $N^M(x) = x^n$,⁷⁾ it follows that $(x_1 \dots x_n)1 = (x_1 \dots x_n)(e_1 + \dots + e_n) = x_1^n e_1 + \dots + x_n^n e_n$ and that $x_1^n = \dots = x_n^n$. Therefore the kernel of ρ^M is of 1-dimension over M , as it has M^* as a subgroup of finite index, and so the kernel of $(\tilde{\rho})^M$ is also of 1-dimension over M . M being algebraically closed, it follows that $\dim_K H = \dim_M (\tilde{\rho})^M(\mu(L^*)^M) = n-1$.⁸⁾ Since H is contained in $\mu(G)$, we get at once $\dim_K \mu(G) \geq n-1$. Hence, we have $\dim_K \mu(G) = n-1$. Now, let $\mu(G_1)$ be the algebraic component of $\mu(G)$ and let $G = G_1 + \dots + G_r$ be the decomposition of G into the cosets modulo G_1 . Thus each G_i is irreducible and $\dim_K G_i = n-1$. Let $\mathfrak{P}_i$, $1 \leq i \leq r$, be prime ideals of the polynomial ring $K[X_1, \dots, X_n]$ associated to G_i respectively. As is well known each $\mathfrak{P}_i$ is principal: $\mathfrak{P}_i = (P_i(X))$, $X = (X_1, \dots, X_n)$. Obviously the ideal $\mathfrak{I} = \mathfrak{P}_1 \cap \dots \cap \mathfrak{P}_r = \mathfrak{P}_1 \cdot \dots \cdot \mathfrak{P}_r$ is associated to G . On the other hand, every element in G satisfies the equation $F(X) = \prod_j (\sum_i X_i \tau_j(\eta_i)) - 1 = 0$, where

⁵⁾ C. II. Chap. II. § 6. Prop. 8. If the characteristic of K is zero, we get $\dim_K \mu(G) = n-1$ by C. II. Chap. II. § 14. Théorème 12.

⁶⁾ C. II. Chap. II. § 5. Prop. 4, § 7. Prop. 2. Cor. 1.

⁷⁾ N^M means the extension of N to V^M . It is also the norm of the algebra L^M over M with respect to the regular representation.

⁸⁾ C. II. Chap. II. § 6. Prop. 8. Cor.

τ_j, η_i have the same meaning as in Proposition 2. Since $F(X) + 1$ splits into the product of different n linear factors in the algebraic closure of K , $F(X)$ is an irreducible polynomial. Since $F(X) \in \mathfrak{A}$, we have $r = 1$ and it follows that $\mathfrak{A} = \mathfrak{P}_1 = (F(X))$ is the associated ideal to G . Thus G , or $\mu(G)$, is irreducible and we get the following

THEOREM 2. *Let K be an infinite field, and L/K a separable extension of finite degree n . Then, the group $\tilde{G}$ of all linear transformations of L over K which leave invariant the norm form of L/K is an algebraic group of dimension $n-1$ and $\mu(G)$ is the algebraic component of $\tilde{G}$, μ being defined by (1). Furthermore $\tilde{G}$ is the semi-direct product of $\mu(G)$ and $\mathfrak{G}$, where $\mathfrak{G}$ is the automorphism group of L/K .*

Lastly, we shall determine the center of the $\tilde{G}_H$ defined over an arbitrary field K .

PROPOSITION 3. *Let K be an arbitrary field and L/K a separable extension of degree n . Then, there exists a base ω_i , $1 \leq i \leq n$ of L/K with $N(\omega_i) = 1$.*

Proof. Suppose first that K is infinite. Let $L(G)$ be the linear closure of G in V . Clearly we have $\dim_K L(G) \geq \dim_K G = n-1$. (Theorem 2). Since G is irreducible and closed and is not a linear space, $L(G)$ must be the whole space V .⁹⁾ Next, suppose that K is a finite field with q elements. Thus, the number of elements in G is $=(q^n-1)/(q-1)$. Let r be the dimension of $L(G)$. Then, we have $(q^n-1)/(q-1) \leq q^r$. From this, it follows that $q^r(q-1) = q^{r+1} - q \geq q^n - 1 > q^n - q$ and $r+1 > n$, namely $r = n$. Therefore we have again $L(G) = V$. This proves our proposition.

THEOREM 3. *Let K be an arbitrary field and L/K a separable extension of degree n . Then the center of $\tilde{G}_H$ is the image of the group $W_H = \{a; a \in G_H, \sigma(a) = a, \sigma \in \mathfrak{G}\}$ by the isomorphism μ defined by (1).*

Proof. Let ζ be any element of the center of $\tilde{G}_H$. Let ω_i be a base of L/K with $N(\omega_i) = 1$, $1 \leq i \leq n$ (Proposition 3). As we have $G \subset G_H$, ζ must commute with $\mu(\omega_i)$ and it must commute with all $\mu(z)$, $z \in L$. Thus it follows that $(\zeta \mu(z))(1) = \zeta(z) = \mu(z)\zeta(1) = z\zeta(1)$. Hence, it follows that $\zeta(z) = \alpha z$ and $\alpha = \zeta(1) \in L^*$. On the other hand, ζ must commute with each $\sigma \in \mathfrak{G}$,

⁹⁾ C. III. Chap. VI. §1 Prop. 14.

Thus, we have $\zeta_\sigma(1) = \alpha = \sigma\zeta(1) = \sigma(\alpha)$. Since $\zeta \in \tilde{G}_H$, we get $N(\alpha) \in H$. Conversely, it is easy to see that any $\mu(a)$ with $a \in W_H$ is in the center of $\tilde{G}_H$ either by Proposition 2 or by the fact that every $a \in W_H$ is an element in K if K is finite.

COROLLARY. *Under the same assumption as in Theorem 3, suppose that L/K is a Galois extension. Then the center of $\tilde{G}_H$ is the image of $W_H = \langle a, a \in K^*, a^n \in H \rangle$.*

Remark 1. We can define the norm form for any algebraic extension L/K of finite degree by means of the regular representation. E.g. if L/K is a purely inseparable extension of degree p^f , where p is the characteristic of K , we have $N(x) = x^{p^f}$, $x \in L$ and we see at once that $\mu(G) = \tilde{G} = \{\varepsilon\}$. Thus, we have a simple example showing that the dimension of the kernel of a rational representation ρ of an algebraic group G is strictly smaller than the difference of the dimension of G and that of $\rho(G)$.¹⁰⁾

Remark 2. The conclusion of Proposition 2 does not hold in general if K is a finite field. E.g. let $K = GF(2)$, $[L:K] = 3$. Since K^* is of order 1, $\tilde{G}_H = \tilde{G} = GL(V)$. Thus, the order of $\tilde{G}$ is $=(2^3 - 1)(2^3 - 2)(2^3 - 2^2) = 168$.¹¹⁾ On the other hand, $\mu(K^*) = \mu(G)$ is of order $2^3 - 1 = 7$. By Proposition 1, the order of $\mu(L^*)\mathfrak{G} = 3 \cdot 7 = 21 < 168$. The center of $\tilde{G}$ is of order 1 (Theorem 3, Corollary). Furthermore this $\tilde{G}$ is simple as is well known.¹¹⁾ Thus, it would be of some interest to study the structure of the finite group $\tilde{G}$ for these cases.

*Mathematical Institute
Nagoya University*

¹⁰⁾ C.f. C. II. Chap. II. §6. p. 119.

¹¹⁾ Ç.f. Dickson, *Linear Groups*, pp. 77-83,