INVARIANT SUBFIELDS OF RATIONAL FUNCTION FIELDS

By Tsuneo Kanno*

Let $K$ be the rational function field $k(X_1, X_2, \ldots, X_n)$ of variables $X_1, X_2, \ldots, X_n$ over a field $k$. Let $M$ be the vector space $\sum_{i=1}^{n} k \cdot X_i$ over $k$. Let $g$ be a finite group operating on $K$, induced by a representation $\rho$ of $g$ with representation space $M$. Let $L$ be the subfield of $K$ consisting of elements which are invariant under $g$. The problem to consider here is whether $L$ is purely transcendental over $k$. This problem has been answered affirmatively in the following cases: (0) $g$ is the symmetric group permuting $X_1, X_2, \ldots, X_n$, (1) $g$ is abelian and $k$ is the complex number field, (2) $g$ is a cyclic group of order $n$, $\rho$ is its regular representation and $k$ contains the primitive $n$-th roots of unity, provided that the characteristic of $k$ does not divide $n$ (cf. [5]) and (3) $k$ is of characteristic $p>0$, $g$ is a $p$-group and $\rho$ is its regular representation (cf. [2], [3] and [4]). In this note we shall give a principle, written in language of algebraic groups, which covers the three cases (1), (2) and (3), and which may be applied to other cases where $g$ is soluble.

A connected algebraic group $G$ is called $k$-soluble if there exists a normal chain $G_0=GDG_1\supseteq GDG_2\supseteq \cdots \supseteq GDG_r=\{e\}$ such that $G_i$ is defined over $k$ and $G_i/G_{i+1}$ is isomorphic to $G_a$ or $G_m$ over $k$, where $G_a$ and $G_m$ are the additive group of the universal domain $\Omega$ and the multiplicative group of non-zero elements of $\Omega$. The following property of $k$-soluble algebraic groups is used here (cf. [6]): let $G$ be a $k$-soluble algebraic group; let $V$ be a homogeneous space with respect to $G$ over $k$, then the function field $k(V)$ over $k$ is purely transcendental over $k$.

From this we have

(P) Let $G$ be a $k$-soluble algebraic group such that $k(G)=K$; let $g$ be a finite subgroup of $G$ which is rational over $k$ such that the invariant subfield of $K$ by the left translations of $g$ is $L$, then $L$ is purely transcendental over $k$.

In fact, there exists the quotient variety $G/g$, defined over $k$, which is a homogeneous space with respect to $G$ over $k$.

Let us consider the case where $g$ is abelian.

Lemma. Let $g$ be a finite abelian subgroup of $GL(n, k)$ of exponent $m$. Then, if $k$ contains the primitive $m$-th roots of unity, there exists $x \in GL(n, k)$ such that $x \cdot g \cdot x^{-1}$ is contained in the set of matrices of the form

Received May 1, 1967.

* This paper was prepared when the author was at University of California, Berkeley, partially supported by NSF GP-1610.
where $N_i$ is upper triangular matrix with only one eigenvalue, and further if the characteristic of $k$ does not divide $m$, $g$ is a group of semisimple matrices and $x \cdot g \cdot x^{-1}$ is diagonal.

The first part follows, for example, from the proof of the Lemma 6.4 of [1]. To prove the second part, take any element $g \in \mathfrak{g}$ and let $g = g_u g_s$ be the multiplicative Jordan decomposition of $g$; then the orders of $g_u$ and $g_s$ divide that of $g$. If the characteristic of $k$ is 0, any non-identity unipotent matrix has the infinite order (cf. Prop. 8.1 of [1]); hence $g$ is semisimple; in the characteristic $p > 0$ case, a matrix is unipotent if and only if its order is a power of $p$ (cf. Prop. 8.1 of [1]); hence $g$ is semisimple.

Now we have a proposition which generalizes (1) and (2).

**Proposition 1.** Let $\mathfrak{g}$ be a finite abelian group of exponent $m$. If the characteristic of $k$ does not divide $m$ and if $k$ contains the primitive $m$-th roots of unity, $L$ is purely transcendental over $k$.

In fact, we may suppose that $\rho$ is faithful and that $g$ is a subgroup of $GL(M)$. By the Lemma we have a base $Y_1, Y_2, \ldots, Y_n$ of the vector space $M$ such that $Y_1 = z_1(\sigma)Y_1$ for $\sigma \in Q$. Take $G$ the group of diagonal matrices with coordinate functions $Y_1, Y_2, \ldots, Y_n$, then $k(G) = K$. We can consider that $g$ is the subgroup of $G$ consisting of diagonal matrices $(z_1(\sigma), z_2(\sigma), \ldots, z_n(\sigma))$ for $\sigma \in \mathfrak{g}$. Since $Y_1(g) = z_1(\sigma)Y_1(g) = Y_1(\sigma g)$ for $g \in G$, the proposition follows from (P).

Let us consider the case where $\rho$ is the regular representation of $g$. Let $Q[\mathfrak{g}]$ be the group ring of $g$ over $Q$. Then the unit group of $Q[\mathfrak{g}]$ has a structure of a connected algebraic group $G$ defined over the prime field $Z_p$ of $k$ such that $k(G) = K$ and $g$ can be imbedded in $G$ by $\sigma \mapsto 1 \cdot \sigma$. Then, the notation being as above, by (P) we have

**Proposition 2.** If the algebraic group $G$ is $k$-soluble, $L$ is transcendental over $k$.

When $g$ is a $p$-group, the following Lemma gives the structure of the algebraic group $G$.

**Lemma.** If $k$ is of characteristic $p > 0$ and $g$ is a $p$-group, $G$ is a connected nilpotent algebraic group defined over $Z_p$ and has the direct decomposition $G = G_s \times G_u$ over $Z_p$, where $G_s$ is central and isomorphic to $G_u$ over $Z_p$ and $G_u$ is the unipotent part of $G$.
Let $N$ be the radical of the algebra $O[\mathfrak{g}]$; let $s$ be a positive integer such that $N^s = \{0\}$. Let $U_i = \{ a \in O[\mathfrak{g}] \mid a \equiv e \pmod{N^i} \}$. Then we have

(i) $$(G, G) \subseteq U_i,$$

(ii) $$(G, U_i) \subseteq U_{i+1}.$$

In fact, for any $a = \sum_{\sigma \in \mathcal{P}} a\sigma$, let $\text{tr}(a) = \sum_{\sigma \in \mathcal{P}} a\sigma$, then $\text{tr}$ is a rational homomorphism of $G$ onto $G_m$ defined over $\mathbb{Z}_p$; we have $a = \text{tr}(a)e + \sum_{\sigma \in \mathcal{P}} a\sigma (e - e) = \text{tr}(a)e + r(a) = \text{tr}(a)e$, mod $N$ and $a^{-1} = \text{tr}(a)^{-1}(e + \text{tr}(a)^{-1}r(a))^{-1} = \text{tr}(a)^{-1}e$, mod $N$, where $r(a) \in N$; hence, for $a, b \in G$, $aba^{-1}b^{-1} \equiv \text{tr}(a)\text{tr}(b)\text{tr}(a)^{-1}\text{tr}(b)^{-1}e = e$, mod $N$; thus we have (i). To show (ii), take $a \in G$ and $b \in U_i$; then $a = \text{tr}(a)e + r(a)$ and $b = e + r(b)$, where $r(a) \in N$ and $r(b) \in N$; then $aba^{-1}b^{-1} = e + (ab - ba)a^{-1}b^{-1} = e + (r(a)r(b) - r(b)r(a))a^{-1}b^{-1} = e$, mod $N^{i+1}$; thus we have (ii). Since $U_i = \{ e \}$, we have that $G$ is nilpotent. Each element $a \in G$ has a unique expression $a = \text{tr}(a)e + (e + \text{tr}(a)^{-1}r(a))$. It is easily seen that the semisimple part $G_s$ and the unipotent part $G_u$ of $G$ are defined over $\mathbb{Z}_p$ and that we have the Lemma.

Since any connected algebraic group of unipotent matrices defined over a perfect field $k$ is $k$-soluble, we have the following Corollary of the Proposition 2 which is nothing but (3).

**Corollary.** If $k$ is of characteristic $p > 0$ and if $\rho$ is the regular representation of a $p$-group $\mathfrak{g}$, $L$ is purely transcendental over $k$.

**Bibliography**


Department of Mathematics,
Tokyo Institute of Technology.