THE DETERMINATION OF CERTAIN FIELDS OF INVARIANTS

JULIO R. BASTIDA
Florida Atlantic University, Boca Raton, FL 33431

It is often difficult to determine Galois groups and their fields of invariants by elementary methods. The objective of this note is to illustrate how some basic considerations on fields and polynomials can be used to determine the fields of invariants of certain groups of field automorphisms.

We shall be concerned with a field K and the field $K(X)$ of rational functions in one variable. The Galois group of $K(X)$ over K will be denoted by

$$\mathrm{Gal}(K(X)/K);$$

for every subgroup Γ of $\mathrm{Gal}(K(X)/K)$, the field of invariants of Γ will be denoted by

$$\mathrm{Inv}(\Gamma).$$

For each $u \in K - \{0\}$, let ρ_u denote the K-automorphism of $K(X)$ such that $X \to uX$; and for each $u \in K$, let τ_u denote the K-automorphism of $K(X)$ such that $X \to u + X$.

Now we are in a position to state and prove the following assertions.

$\mathcal{A}$. If M is an infinite subgroup of the multiplicative group of nonzero elements of K, then the mapping $u \to \rho_u$ from M to $\mathrm{Gal}(K(X)/K)$ is an injective group homomorphism, and K is the field of invariants of its image.

$\mathcal{B}$. If A is an infinite subgroup of the additive group of K, then the mapping $u \to \tau_u$ from A to $\mathrm{Gal}(K(X)/K)$ is an injective group homomorphism, and K is the field of invariants of its image.

A quick proof of these assertions can be obtained from the following two results: (1) $K(X)$ is a finite algebraic extension of each of its subfields properly containing K; and (2) Artin's theorem on the field of invariants of a finite group of field automorphisms. These results are discussed in [1, p. 158] and [2, p. 69], respectively. We shall now prove $\mathcal{A}$ and $\mathcal{B}$ by using only very elementary properties of polynomials.

In the discussion that follows, we shall consider an element Y of $K(X)$ not belonging to K, and write it in the form $Y = f(X)/g(X)$, where $f(X)$ and $g(X)$ are relatively prime polynomials in $K[X]$. Put $m = \deg(f(X))$ and $n = \deg(g(X))$; then write

$$f(X) = \sum_{i=0}^{m} a_i X^i \quad \text{and} \quad g(X) = \sum_{j=0}^{n} b_j X^j,$$

where $a_0, a_1, \ldots, a_m, b_0, b_1, \ldots, b_n \in K$ and $a_m \neq 0 \neq b_n$.

Proof of $\mathcal{A}$: If $u, v \in M$, then $(uv)X = u(vX)$, whence $\rho_{uv} = \rho_u\rho_v$. It follows that the mapping $u \to \rho_u$ from M to $\mathrm{Gal}(K(X)/K)$ is a group homomorphism. Its injectivity is evident: indeed, if $u \in A$ and ρ_u is the identity mapping on $K(X)$, then $X = \rho_u(X) = uX$, which implies that $u = 1$.

Let Γ denote the image of this homomorphism. We shall now prove that the condition $Y \in \mathrm{Inv}(\Gamma)$ leads to a contradiction.

Now assume that $Y \in \mathrm{Inv}(\Gamma)$. Then, for every $u \in M$, we have $Y = \rho_u(Y)$, which means that

$$f(X)/g(X) = \rho_u(f(X))/\rho_u(g(X)) = f(uX)/g(uX),$$

and, hence, $f(X)g(uX) = f(uX)g(X)$; since $f(X)$ and $g(X)$ are relatively prime in $K[X]$, and since

$$\deg(f(X)) = m = \deg(f(uX))$$

and
$$\deg(g(X)) = n = \deg(g(uX)),$$
it now follows that
$$f(uX) = u^m f(X) \quad \text{and} \quad g(uX) = u^n g(X),$$
which means that $u^{m-i}a_i = a_i$ for $0 \leq i \leq m$ and $u^{n-j}b_j = b_j$ for $0 \leq j \leq n$.

If $0 \leq i < m$ and $a \neq 0$, then $u^{m-i} = 1$ for every $u \in M$; hence, every element of M is an $(m - i)$th root of unity in K. As M is infinite, this is impossible. Similarly, the conditions $0 \leq j < n$ and $b_j \neq 0$ imply an absurd conclusion. We conclude that $a_i = 0 = b_j$ for $0 \leq i < m$ and $0 \leq j < n$.

Consequently, we have $f(X) = a_m X^m$ and $g(X) = b_n X^n$. If we put $c = a_m/b_n$ and $r = m - n$, then $c \in K - \{0\}$ and $Y = cX^r$; since $Y \notin K$, we see that $r \neq 0$. For every $u \in M$, we now have
$$cX^r = Y = \rho_u(Y) = c(uX)^r = cu^r X^r,$$
which implies that $u^r = 1$. Thus, every element of M is an $|r|$th root of unity in K. This contradicts the infiniteness of M, and completes the proof of A.

Proof of B: If u, $v \in A$, then
$$(u + v) + X = u + (v + X),$$
which implies that $\tau_{u+v} = \tau_u \tau_v$. Thus the mapping $u \to \tau_u$ from A to $\mathrm{Gal}(K(X)/K)$ is a group homomorphism. To verify that it is injective, note that if $u \in A$ and τ_u is the identity mapping on $K(X)$, then $X = \tau_u(X) = u + X$, whence $u = 0$.

Let Δ denote the image of this homomorphism. Assume, by way of contradiction, that $Y \in \mathrm{Inv}(\Delta)$. For each $u \in A$, we have $Y = \tau_u(Y)$, which implies that
$$f(X)/g(X) = \tau_u(f(X))/\tau_u(g(X)) = f(u + X)/g(u + X),$$
and hence
$$f(X)g(u + X) = f(u + X)g(X);$$
taking into account that $f(X)$ and $g(X)$ are relatively prime in $K[X]$, and that
$$\deg(f(X)) = m = \deg(f(u + X))$$
and
$$\deg(g(X)) = n = \deg(g(u + X)),$$
we conclude that
$$f(u + X) = f(X) \quad \text{and} \quad g(u + X) = g(X).$$

It now follows that $f(u) = f(0) = a_0$ and $g(u) = g(0) = b_0$ for every $u \in A$. This means that every element of A is a root of the polynomials $f(X) - a_0$ and $g(X) - b_0$, which is incompatible with the assumption that M is infinite. This completes the proof of B.

REFERENCES

1. N. Jacobson. *Lectures in Abstract Algebra*. Vol. III. Princeton: D. van Nostrand, 1964.
2. M. Nagata. *Field Theory*. New York & Basel: Marcel Dekker, Inc., 1977.

*****