PROCEEDINGS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 80, Number 3, November 1980

A NOTE ON AUTOMORPHISM GROUPS OF ALGEBRAIC NUMBER FIELDS

M. FRIED[1]

ABSTRACT. For any finite group G the paper gives an explicit and simple construction of (not necessarily Galois) algebraic extensions of $\mathbf{Q}$ having their full automorphism group equal to G.

Intrigued by both the result and the last name of one of the authors, we inspected the contents of [EFrK]. In there it is shown that, for any finite group G, there is a (not necessarily Galois) extension L of $\mathbf{Q}$ such that the full automorphism group of the extension $L/\mathbf{Q}$ is G. This is, of course, a weakened form of the celebrated Hilbert-Noether conjecture that every group can be realized as a Galois group over $\mathbf{Q}$. In this note, we make further comment on the nature of the construction of the field L; simplify the proof of the existence of L; and correct one of the lemmas of [EFrK]. We have been uncompromisingly "generic" in our approach in order to keep technique at a minimum, and also to reveal the many alternatives for the construction of L.

First assume that G is contained in S_n. Let $t_1, \ldots, t_n$ be algebraically independent indeterminates over $\mathbf{Q}$. It is well known that the splitting field $M_n^{(\mathbf{t})}$ of $x^n + t_1 \cdot x^{n-1} + \cdots + t_n$ over $\mathbf{Q}(t_1, \ldots, t_n) = \mathbf{Q}(\mathbf{t})$ is a regular Galois extension of $\mathbf{Q}(\mathbf{t})$ with group equal to S_n. This is the starting observation of [Hi]: the progenitor of so many notes in the style of this one. Let $M_G^{(\mathbf{t})}$ be the fixed field of G in $M_n^{(\mathbf{t})}$, and let $\alpha(G, \mathbf{t})$ be a primitive generator of $M_G^{(\mathbf{t})}$ over $\mathbf{Q}(\mathbf{t})$.

Let N be any integer greater than 2 and let $z_1, \ldots, z_N$ be algebraically independent indeterminates over $\mathbf{Q}(\mathbf{t})$. Finally, let $\beta(G, \mathbf{t})$ be a zero of $x^N + z_1 \cdot x^{N-1} + \cdots + z_{N-1} \cdot x + \alpha(G, \mathbf{t}) \cdot z_N$. Now consider the field

$$L^{(\mathbf{t},\mathbf{z})} = M_n^{(\mathbf{t})}(\beta(G, \mathbf{t}), \mathbf{z}) = M_G^{(\mathbf{t})}(\beta(G, \mathbf{t}), \mathbf{z}) \cdot M_n^{(\mathbf{t})}(\mathbf{z}).$$

Then $L^{(\mathbf{t},\mathbf{z})}/M_G^{(\mathbf{t})}(\beta(G, \mathbf{t}), \mathbf{z})$ is a Galois extension with group

$$\begin{aligned} G(L^{(\mathbf{t},\mathbf{z})}/M_G^{(\mathbf{t})}(\beta(G, \mathbf{t}), \mathbf{z})) &= G(M_n^{(\mathbf{t})}(\mathbf{z})/M_n^{(\mathbf{t})}(\mathbf{z}) \cap M_G^{(\mathbf{t})}(\beta(G, \mathbf{t}), \mathbf{z})) \\ &= G(M_n^{(\mathbf{t})}(\mathbf{z})/M_G^{(\mathbf{t})}(\mathbf{z})) = G, \end{aligned}$$

our original group.

Suppose that σ is any automorphism of $L^{(\mathbf{t},\mathbf{z})}/\mathbf{Q}(\mathbf{t}, \mathbf{z})$. If σ leaves $M_G^{(\mathbf{t})}(\mathbf{z})$ fixed, then $\beta(G, \mathbf{t})^\sigma$ is another zero of $x^N + z_1 x^{N-1} + \cdots + z_{N-1} x + \alpha(G, \mathbf{t}) \cdot z_N$. This

Received by the editors August 2, 1979 and, in revised form, October 19, 1979.

1980 *Mathematics Subject Classification*. Primary 12F05.

Key words and phrases. Galois theory, Hilbert's irreducibility theorem.

[1]This paper was written while the author was a speaker at the 1979 AMS Summer Conference in Group Theory held at Santa Cruz. Supported by NSF Grant MCA-76-07159 and Conference funds.

implies that $\beta(G, \mathbf{t})^\sigma = \beta(G, \mathbf{t})$ since the splitting field of this polynomial over $M_n^{(\mathbf{t})}(\mathbf{z})$ is S_N. Now suppose that σ does *not* fix $M_G^{(\mathbf{t})}(\mathbf{z})$. Then $\beta(G, \mathbf{t})$ goes to a root $\beta(G, \mathbf{t})^\sigma$ of $x^N + z_1 \cdot x^{N-1} + \cdots + \alpha(G, \mathbf{t})^\sigma \cdot z_N$. Our next lemma shows that

$$\beta(G, \mathbf{t})^\sigma \notin L^{(\mathbf{t},\mathbf{z})} \quad \text{for each such } \sigma. \tag{1}$$

With (1) established, $L^{(\mathbf{t},\mathbf{z})}$ is a regular extension of $\mathbf{Q}(\mathbf{t}, \mathbf{z})$ (its Galois closure over $\mathbf{Q}(\mathbf{t}, \mathbf{z})$ is regular over $\mathbf{Q}(\mathbf{t}, \mathbf{z})$ also) for which the automorphisms of $L^{(\mathbf{t},\mathbf{z})}/\mathbf{Q}(\mathbf{t}, \mathbf{z})$ give the group G.

LEMMA. *Let $z_1, \ldots, z_N$ (with $N > 1$) be algebraically independent indeterminates over a field M of characteristic zero. Let $a_1, a_2 \in M$ be distinct nonzero elements, and let β_i be a zero of*

$$x^N + z_1 \cdot x^{N-1} + \cdots + z_{N-1} \cdot x + a_i \cdot z_N, \qquad i = 1, 2. \tag{2}$$

Then the fields $M(\mathbf{z}, \beta_1)$ and $M(\mathbf{z}, \beta_2)$ are distinct.

PROOF. Suppose that $M(\mathbf{z}, \beta_1) = M(\mathbf{z}, \beta_2)$. Consider the field $L = M(z_1, \ldots, z_{N-1})$, so that $M(\mathbf{z}, \beta_i) = L(z_N, \beta_i)$, $i = 1, 2$. Let $\bar{L}$ be an algebraic closure of L, so that $\bar{L}(z_N, \beta_1) = \bar{L}(z_N, \beta_2)$ by assumption. The *finite branch points* of the field extension $\bar{L}(z_N, \beta_i)/\bar{L}(z_N)$ with respect to the variable z_N consist of the values (in $\bar{L}$) of z_N for which

$$Nx^{N-1} + (N-1) \cdot z_1 \cdot x^{N-2} + \cdots + z_{N-1} = 0 \tag{3}$$

and equation (2) for "i" have a common solution in x. Since $z_1, \ldots, z_{N-1}$ are algebraically independent over M, these branch points are algebraically independent over M. However, these branch points are determined by the field extension, so the two sets of branch points corresponding to $i = 1$ and 2 are the same. If $\omega_1, \ldots, \omega_{N-1}$ are the zeros of $Nx^{N-1} + (N-1)z_1 \cdot x^{N-2} + \cdots + z_{N-1} = 0$, then $-f(\omega_j)/a_i$, $j = 1, \ldots, N-1$, runs over the branch points corresponding to i, where $f(x) = x^N + z_1 \cdot x^{N-1} + \cdots + z_{N-1} \cdot x$. Thus multiplication by a_1/a_2 maps the branch points corresponding to $i = 1$ to the branch points corresponding to $i = 2$. This contradicts the algebraic independence of these branch points over M. □

Finally we prove the main theorem of the paper.

THEOREM. *Given any finite group G, we can explicitly find an infinite number of field extensions $L/\mathbf{Q}$ such that the automorphism group of $L/\mathbf{Q}$ is isomorphic to G.*

PROOF. Let $\hat{L}^{(\mathbf{t},\mathbf{z})}/\mathbf{Q}(\mathbf{t}, \mathbf{z})$ be the Galois closure of the field extension $L^{(\mathbf{t},\mathbf{z})}/\mathbf{Q}(\mathbf{t}, \mathbf{z})$. The automorphism group of $L^{(\mathbf{t},\mathbf{z})}/\mathbf{Q}(\mathbf{t}, \mathbf{z})$ can be recovered as the quotient $N/G(\hat{L}^{(\mathbf{t},\mathbf{z})}/L^{(\mathbf{t},\mathbf{z})})$ where N is the normalizer of $G(\hat{L}^{(\mathbf{t},\mathbf{z})}/L^{(\mathbf{t},\mathbf{z})})$ in $G(\hat{L}^{(\mathbf{t},\mathbf{z})}/\mathbf{Q}(\mathbf{t}, \mathbf{z}))$. From Hilbert's irreducibility theorem there are infinitely many specializations $(\mathbf{t}_0, \mathbf{z}_0) \in \mathbf{Z}^n \times \mathbf{Z}^N$ of $(\mathbf{t}, \mathbf{z})$ for which we obtain distinct field extensions $\hat{L}^{(\mathbf{t}_0,\mathbf{z}_0)}$ and $L^{(\mathbf{t}_0,\mathbf{z}_0)}$ over $\mathbf{Q}$ with

$$G(\hat{L}^{(\mathbf{t}_0,\mathbf{z}_0)}/\mathbf{Q}) \simeq G(\hat{L}^{(\mathbf{t},\mathbf{z})}/\mathbf{Q}(\mathbf{t}, \mathbf{z}))$$

and

$$G(\hat{L}^{(\mathbf{t}_0,\mathbf{z}_0)}/L^{(\mathbf{t}_0,\mathbf{z}_0)}) \simeq G(\hat{L}^{(\mathbf{t},\mathbf{z})}/L^{(\mathbf{t},\mathbf{z})}).$$

Thus we deduce that the automorphism group of $L^{(\mathbf{t}_0,\mathbf{z}_0)}/\mathbf{Q}$ is isomorphic to G. From the explicit form of Hilbert's irreducibility theorem in **[MFr]**, we may find arithmetic progressions $P^{(t)}$ and $P^{(z)}$ in $\mathbf{Z}^n$ and $\mathbf{Z}^N$, respectively, such that this holds for $(\mathbf{t}_0, \mathbf{z}_0) \in P^{(t)} \times P^{(z)}$. $\square$

The authors of **[EFrK]** base their proof on the result that there exists a finite undirected graph having neither loops nor isolated points whose automorphism group is G **[Fru]**. There is a correctable, but significant, error in the proof of their Lemma 2. *Let L be a number field, R the ring of integers. If $f_1, \ldots, f_m \in R[x]$ are monic polynomials that are not pth powers for some prime p, then there exists $t \in \mathbf{Z}$ such that $f_i(t)$ is not a pth power in L, $i = 1, \ldots, t$.* The authors conclude that $y^p - f_i(x) = 0$ is not a genus zero curve, and they apply Siegel's theorem to conclude that there are only finitely many integral points. First of all, such a use of Siegel's theorem would make their field construction completely ineffective (which it should not be), and secondly (for a trivial counterexample) take $m = 1$, $p = 2$, $f_1(x) = x^3$ to get a genus zero curve. However, this can be corrected by using Hilbert's irreducibility theorem as in the proof of the theorem above. Let $g_i^{(j)}(x, y)$, $j = 1, \ldots, m(i)$, run over the irreducible factors of $y^p - f_i(x)$. By hypothesis, $g_i^{(j)}(x, y)$ is of degree greater than 1 in y. By Hilbert's theorem there exists $t \in \mathbf{Z}$ such that $g_i^{(j)}(t, y)$ remains irreducible over $\mathbf{Q}$ for $j = 1, \ldots, m(i)$; $i = 1, \ldots, t$.

References

[EFrK] E. Fried and J. Kollár, *Automorphism groups of algebraic number fields*, Math. Z. **163** (1978), 121–123.

[MFr] M. Fried, *On Hilbert's irreducibility theorem*, J. Number Theory **6** (1974), 211–232.

[Fru] R. Frucht, *Herstellung von Graphen mit Vorgegebener abstrakter Gruppe*, Compositio Math. **6** (1938), 239–250.

[Hi] D. Hilbert, *Über die Irreduzibilität ganzer rationaler Functionen, mit ganzzahligen Koeffizienten*, Crelles J. Math. **110** (1892), 104–129.

Department of Mathematics, University of California, Irvine, California 92717