A NOTE ON AUTOMORPHISM GROUPS
OF ALGEBRAIC NUMBER FIELDS

M. FRIED

Abstract. For any finite group G the paper gives an explicit and simple construction of (not necessarily Galois) algebraic extensions of 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 Q such that the full automorphism group of the extension L/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 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 Sn. Let t1, . . . , tn be algebraically independent indeterminates over Q. It is well known that the splitting field Mn(t) of x^n + t1 · x^{n-1} + · · · + tn over Q(t1, . . . , tn) = Q(t) is a regular Galois extension of Q(t) with group equal to Sn. This is the starting observation of [Hi]: the progenitor of so many notes in the style of this one. Let M^G be the fixed field of G in M_n(t), and let a(G, t) be a primitive generator of M^G over Q(t).

Let N be any integer greater than 2 and let z1, . . . , z_N be algebraically independent indeterminates over Q(t). Finally, let ß(G, t) be a zero of x_N + z_1 · x_{N-1} + · · · + z_{N-1} · x + a(G, t) · z_N. Now consider the field

L^{(z)} = M^G(ß(G, t), z) = M^G(ß(G, t), z) · M_n(z).

Then L^{(z)} / M^G(ß(G, t), z) is a Galois extension with group

G(L^{(z)} / M^G(ß(G, t), z)) = G(M_n(z) / M_n(z) ∩ M^G(ß(G, t), z))

= G(M_n(z) / M_n(z)) = G,

our original group.

Suppose that σ is any automorphism of L^{(z)} / Q(t, z). If σ leaves M^G(z) fixed, then ß(G, t)^s is another zero of x_N + z_1 · x_{N-1} + · · · + z_{N-1} · x + a(G, t) · z_N. This
implies that $\beta(G, t)^\sigma = \beta(G, t)$ since the splitting field of this polynomial over $M^n(\beta, z)$ is $S_N$. Now suppose that $\sigma$ does not fix $M^n(\beta, z)$. Then $\beta(G, t)$ goes to a root $\beta(G, t)^\sigma$ of $x^N + z_1 \cdot x^{N-1} + \cdots + z_{N-1} \cdot x + a(G, t)^\sigma \cdot z_N$. Our next lemma shows that

$$\beta(G, t)^\sigma \notin L^{(t, z)}$$

for each such $\sigma$.

With (1) established, $L^{(t, z)}$ is a regular extension of $Q(t, z)$ (its Galois closure over $Q(t, z)$ is regular over $Q(t, z)$ also) for which the automorphisms of $L^{(t, z)}/Q(t, z)$ 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 $\beta_i$ be a zero of

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

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

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

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

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 $\omega_1, \omega_2, \ldots, \omega_{N-1}$ are the zeros of $N x^{N-1} + (N - 1) z_1 \cdot x^{N-2} + \cdots + z_{N-1} = 0$, then $-f(\omega_j)/a_j$, $j = 1, \ldots, N - 1$, 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 $L/Q$ such that the automorphism group of $L/Q$ is isomorphic to $G$.

**Proof.** Let $\hat{L}^{(t, z)}/Q(t, z)$ be the Galois closure of the field extension $L^{(t, z)}/Q(t, z)$. The automorphism group of $L^{(t, z)}/Q(t, z)$ can be recovered as the quotient $N/G(\hat{L}^{(t, z)}/L^{(t, z)})$ where $N$ is the normalizer of $G(\hat{L}^{(t, z)}/L^{(t, z)})$ in $G(\hat{L}^{(t, z)}/Q(t, z))$. From Hilbert's irreducibility theorem there are infinitely many specializations $(t_0, z_0) \in \mathbb{Z}^n \times \mathbb{Z}^N$ of $(t, z)$ for which we obtain distinct field extensions $\hat{L}^{(t_0, z_0)}$ and $L^{(t_0, z_0)}$ over $Q$ with

$$G(\hat{L}^{(t_0, z_0)}/Q) \simeq G(\hat{L}^{(t, z)}/Q(t, z))$$

and

$$G(\hat{L}^{(t_0, z_0)}/L^{(t_0, z_0)}) \simeq G(\hat{L}^{(t, z)}/L^{(t, z)}).$$
Thus we deduce that the automorphism group of $L(t^{\omega_0})/Q$ is isomorphic to $G$. From the explicit form of Hilbert's irreducibility theorem in [MFr], we may find arithmetic progressions $P^{(i)}$ and $P^{(z)}$ in $Z^n$ and $Z^N$, respectively, such that this holds for $(t_0, z_0) \in P^{(i)} \times P^{(z)}$. □

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 $p$th powers for some prime $p$, then there exists $t \in Z$ such that $f_i(t)$ is not a $p$th 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 $m = 1, p = 2, f_i(x) = x^3$ 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 $t \in Z$ such that $g_{i,j}(t, y)$ remains irreducible over $Q$ for $j = 1, \ldots, m(i); i = 1, \ldots, t$.

REFERENCES


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