ACTA MATHEMATICA VIETNAMICA
Volume 16, Number 2, 1991

ON THE CARDINALITY OF THE GROUP OF AUTOMORPHISMS OF ALGEBRAICALLY CLOSED EXTENSION FIELDS

T. SOUNDARARAJAN

Introduction

A. Charnow [C] proved that if E is an algebraically closed field, then $|\text{Aut}E| = 2^{|E|}$. Independently, W. Wieslaw [W] has obtained the same result when $|E| > c$. These results significantly generalized an earlier result of the author [S]. Naturally one may raise the following problem : Let E be an algebraically closed extension field of a field F and G the group of all automorphisms of E over F. Determine $|G|$. In this paper we will solve this problem. We obtain the following results :

1) If E is algebraic over F, then $|G| = 2^m$, where $m = 0, 1$ or infinite. Conversely, given any $m = 0, 1$ or infinite, we can find a pair E, F with $|G| = 2^m$.

2) If E is transcendental over F, let d be the transcendence degree of E over F. There are two cases:

(a) F is finite : Then $|G| = c$ if d is finite and $|G| = 2^d$ if d is infinite.

(b) F is infinite : Then $|G| = 2^d$ if $d \geq |F|$ and $|G| = 2^{|F|}$ if $d < |F|$.

The author is extremely thankful to the referee for suggesting the proof in the case of characteristic 2 in (b) and thus enabling to present complete results.

Received November 3, 1990; in revised form October 15, 1991

1. E algebraic over F

PROPOSITION 1. *Let E be algebraic over F. Then $|G| = 2^m$ with $m =$ 0, 1 or infinite cardinal. Conversely, given $m = 0, 1$ or infinite cardinal, there exists a pair E, F with E algebraic over F such that $|G| = 2^m$.*

PROOF: If G is finite and $\neq e$, then by Artin-Schreier theorem F is real closed and hence $|G| = 2$. Suppose that G is infinite. Then E is an infinite algebraic extension of F. By the infinite Galois theory [B, p.188] G is a compact totally disconnected group. Hence $|G| = 2^m$, m being the weight of G. See [HR, 9.15]. Conversely, if $m = 0$, we can take $E = F = \mathbb{C}$, and if $m = 1$, $E = \mathbb{C}$, $F = \mathbb{R}$. Let m now be infinite. We choose a pure transcendental extension $F = \mathbb{Q}(B)$ with $|B| = m$ and let E be the algebraic closure of F. Then $|E| = |F| = m$ (see [J, p.143]) and hence $|G| \leq 2^m$. We claim that $|G| \geq 2^m$. Consider the extension $F_1 = F(\{\sqrt{x} : x \in B\})$. Then F_1 is an algebraic separable normal extension of F and $G(F_1/F) \simeq \Pi\mathbb{Z}/2\mathbb{Z}$. Hence $|G(F_1/F)| = 2^m$. Since $G(F_1/F)$ is the quotient group $G/G(E/F_1)$, we get $|G| \geq 2^m$. Now the proposition follows.

2. E transcendental over F

Throughout this section, E is a transcendental extension of F with transcendence degree d. Moreover, we will denote by B a transcendence base of E over F.

PROPOSITION 2. *Let F be a finite field. Then*

1) $|G| = c$ if d is finite.
2) $|G| = 2^d$ if d is infinite.

PROOF: (1) If d is finite, $|F(B)| = \mathcal{H}_0 = |E|$, hence $|G| \leq c$. On the other hand, $G \supset G(E/F(B))$ and E is a countably generated algebraic extension of $F(B)$. If E were a finite extension of $F(B)$, then by Artin-Schreier theorem $F(B)$ would be a real closed field and hence the characteristic of $F(B)$ would be zero. But the characteristic of $F(B) =$ the characteristic of $F = p \neq 0$, a contradiction. So E must be an infinite algebraic extension of $F(B)$. Hence by Proposition 1, $|G(E/F(B))| = 2^{\aleph_0} = c$ and $|G| \geq c$. From this (1) follows.

(2) If d is infinite, $|F(B)| = d = |E|$. Hence $|G| \leq 2^d$. On the other hand, every permutation of B extends to an element of G and so $|G| \geq 2^d$. Thus, $|G| = 2^d$ follows.

PROPOSITION 3. *Suppose that F is infinite. Then $|G| = 2^d$ if $d \geq |F|$.*

PROOF: E is an algebraic closure of $F(B)$ and so every permutation of B extends to an element of G. Hence we get $|G| \geq 2^d$. On other hand, we easily have $|F(B)| = d$, hence $|E| = d$ (See [J, p.143]). So $|G| \leq 2^d$. From this the proposition follows.

LEMMA 4. *Suppose that F is infinite and $d < |F|$. Then $|G| \leq 2^{|F|}$.*

PROOF: Since $d < |F|$, we have $|F(B)| = |F|d = |F|$. Hence $|E| = |F|$ (See [J, p.143]). Thus $|G| \leq 2^{|E|} = 2^{|F|}$.

PROPOSITION 5. *Suppose that F is infinite and $d < |F|$. Then $|G| = 2^{|F|}$.*

PROOF: By Lemma 4, we have $|G| \leq 2^{|F|}$. To prove $|G| \geq 2^{|F|}$ let $x \in B$ and F_1 be the algebraic closure of $F(B \setminus \{x\})$ in E and $K = F_1(x)$.

Suppose that the characteristic of $F \neq 2$. Consider the extension

$$L = K(\{\sqrt{x+a} : a \in F \setminus \{0\}\}).$$

Claim : If $a_1, ..., a_n$ are distinct elements from F and $y_i = \sqrt{x + a_i}$ for $i = 1, ..., n$, then $y_1, ..., y_n$ are linearly independent over K.

It is enough to prove that $[K(y_1, ..., y_n) : K] = 2^n$. We prove this by induction on n. If $n = 1$, it is easy. Let us now assume the claim whenever less than n elements are involved.

Consider y_n. If $y_n \in K(y_1,...,y_{n-1})$, then $y_n = b_2 + c_2 y_{n-1}$, where $b_2, c_2 \in K(y_1,...,y_{n-2})$. If $c_2 = 0$, then $y_n \in K(y_1,...,y_{n-2})$ in which case we are through by applying the induction hypothesis to the $(n-1)$ elements $y_1,...,y_2$ and y_n. So we can assume that $c_2 \neq 0$. If $b_2 \neq 0$, then $b_2 c_2 \neq 0$ and hence $2b_2c_2 \neq 0$ since the characteristic of $K \neq 2$. Squaring $y_n = b_2 + c_2 y_{n-1}$ gives $x + a_n = b_2^2 + c_2^2(x + a_{n-1}) + 2b_2c_2y_{n-1}$. This yields $y_{n-1} \in K(y_1,...,y_{n-2})$ and hence

$$[K(y_1,...,y_{n-1}) : K] = [K(y_1,...,y_{n-2}) : K] = 2^{n-2},$$

contradicting the induction hypothesis. Thus we are left with the situation

$$y_n = c_2 y_{n-1},\ c_2 \in K(y_1,...,y_{n-2}),\ c_2 \neq 0.$$

Now $c_2 = b_3 + c_3 y_{n-2}$, b_3, $c_3 \in K(y_1,...,y_{n-3})$. If $c_3 = 0$, then $y_n \in K(y_1,...,y_{n-3}, y_{n-1})$, contradicting the induction hypothesis. So $c_3 \neq 0$. If $b_3 \neq 0$, then $y_n^2 = c_2^2 y_{n-1}^2$ gives $x + a_n = c_2^2(x + a_{n-1})$. From this we get $y_{n-2} \in K(y_1,...,y_{n-3})$, contradicting the induction hypothesis. So $b_3 = 0$ and we are left with the situation $y_n = y_{n-1}y_{n-2}c_3$, $c_3 \neq 0$, $c_3 \in K(y_1,...,y_{n-3})$. We continue this process. Either we get a contradiction or we come to the situation (in atmost $n-1$ stages) : $y_n = y_{n-1}y_{n-2}...y_1c_n$, $c_n \neq 0$, $c_n \in K$ and hence

$$c_n = \frac{f(x)}{g(x)},\ (f(x), g(x)) = 1,\ f(x), g(x) \in F[x].$$

Squaring we get

$$(x + a_n) = (x + a_{n-1})|(x + a_{n-2}) \cdots\cdots \frac{f(x)^2}{g(x)^2}$$

Using unique factorization, we get $x + a_n$ divides both $f(x)$ and $g(x)$, contradicting the assumption $(f(x), g(x)) = 1$. Therefore $[K/y_1,...,y_n : K] = 2^n$. Thus the claim follows.

Now $\{\sqrt{x+a} : a \in F \setminus \{0\}\}$ is a linearly independent set over K. Then L is an algebraic separable normal extension of K and $G(L/K) \simeq \Pi\mathbf{Z}/2\mathbf{Z}$. Hence $|G(L/K)| = 2^{|F|}$. Since E is an algebraic closure of L, each element of

$G(L/K)$ extends to an element of $G(E/K) \subset G$. Hence $|G| \geq 2^{|F|}$ when the characteristic of $F \neq 2$.

Suppose that the characteristic of $F = 2$. Consider the extension

$$M = K(\{\sqrt[3]{x+a} : a \in F \setminus \{0\}\}.$$

Claim. If $a_1, ..., a_n$ are distinct elements of $F \setminus \{0\}$ and $z_i = \sqrt[3]{x + a_i}$ for $i = 1, ..., n$, then $1, z_n, z_n^2$ are linearly independent over $K(z_1, ..., z_{n-1})$. It is enough to prove that $[K(z_1, ..., z_n) : K] = 3^n$. We prove this by induction on n.

Suppose that $n = 1$. Then z_1 is a root of the polynomial $z^3 - (x + a_1)$ over K. If this polynomial is reducible in $K[Z]$, it has a root in K. But F_1 being algebraically closed contains all the cube roots of unity. Hence all the roots of this polynomial will be in K. Hence $z_1 \in K$. But $x + a_1 \to x$ yields an automorphism of K. Hence we get $\sqrt[3]{x} \in K$. This is a contradiction. Thus $Z^3 - (x + a_1)$ is irreducible in $K[Z]$ and hence $[K(z_1] : K] = 3$.

Let us now assume the claim whenever less than n elements are involved. Suppose that the polynomial $Z^3 - (x + a_n)$ is reducible in $K(z_1, ..., z_{n-1})[Z]$. Then it has a root in $K(z_1, ..., z_{n-1})$ and since F_1 contains all the roots of unity, we get $z_n \in K(z_1, ..., z_{n-1})$. Therefore $z_n = b_2 + c_2 z_{n-1} + d_2 z_{n-1}^2$, where $b_2, c_2, d_2 \in K(z_1, ..., z_{n-2})$. Since $1, z_{n-1}, z_{n-1}^2$ are linearly independent over $K(z_1, ..., z_{n-2})$, the equation $z_n^3 = (b_2 + c_2 z_{n-1} + d_2 z_{n-1}^2)^3$ gives the relations

$$b_2^3 + c_2^3(x + a_{n-1}) + d_2^3(x + a_{n-1})^2 = x + a_n,$$

$$(*) \qquad b_2^2 c_2 + d_2(b_2 d_2 + c_2^2)(x + a_{n-1}) = 0,$$

$$(**) \qquad b_2(b_2 d_2 + c_2^2) + c_2 d_2^2(x + a_{n-1}) = 0.$$

Case (1) : $b_2 \neq 0$.

If $c_2 = 0$, then $(**)$ gives $b_2^2 d_2 = 0$, hence $d_2 = 0$. If $d_2 = 0$, then $(*)$ gives $b_2^2 c_2 = 0$, hence $c_2 = 0$. In this case, $z_n \in K(z_1, ..., z_{n-2})$ and we get a contradiction by applying the induction hypothesis to the $(n-1)$ elements $z_1, ..., z_{n-2}$ and z_n. So we have $c_2 \neq 0$ and $d_2 \neq 0$.

Eliminating $(x+a_{n-1})$ from $(*)$ and $(**)$ we get

$$\begin{aligned}
&d_2(b_2d_2+c_2^2)b_2(b_2d_2+c_2^2)=c_2d_2^2b_2^2c_2,\\
&(b_2d_2+c_2^2)^2=c_2^2b_2d_2,\\
&c_2^4+b_2^2d_2^2=c_2^2b_2d_2,\\
&c_2^4=b_2d_2(b_2d_2+c_2^2).
\end{aligned}$$

Hence

$$x+a_{n-1}=\frac{b_2(b_2d_2+c_2^2)}{c_2d_2^2}=\frac{c_2^4}{c_2d_2^3}=(\frac{c_2}{d_2})^3.$$

Thus $z_{n-1}^3=(\frac{c_2}{d_2})^3$. Hence $z_{n-1}=\frac{c_2}{d_2}$ or $w\frac{c_2}{d_2}$ or $w^2\frac{c_2}{d_2}$ where $w^3=1$. Now $w\in F_1$ and $\frac{c_2}{d_2}\in K(z_1,...,z_{n-2})$. Thus $z_{n-1}\in K(z_1,...,z_{n-2})$. This contradicts the induction hypothesis for the $n-1$ elements $z_1,...,z_{n-2}$ and z_{n-1}.

Case (2) : $b_2=0$.

Then $c_2d_2^2(x+a_{n-1})=0$. But $x+a_{n-1}\neq 0$. Hence $c_2=0$ or $d_2=0$.

Thus we are left with the situation $z_n=c_2z_{n-1}$ or $z_n=d_2z_{n-1}^2$, where $c_2\neq 0$, $d_2\neq 0$ and $c_2,d_2\in K(z_1,...,z_{n-2})$. We have $z_n=z_{n-1}^{\epsilon_1}e_2$, where $\epsilon_1=1$ or 2, $e_2\neq 0$, $e_2\in K(z_1,...,z_{n-2})$. Now $e_2=b_3+c_3z_{n-2}+d_3z_{n-2}^2$, where $b_3,c_3,d_3\in K(z_1,...,z_{n-3})$.

As above we may assume that $b_3=0$ and either $c_3=0$ or $d_3=0$. Thus we may assume that $z_n=z_{n-1}^{\epsilon_1}z_{n-2}^{\epsilon_2}e_3$ where $\epsilon_2=1$ or 2 and $e_3\in K(z_1,...,z_{n-3})$, $e_3\neq 0$. Continuing this process (in atmost $n-1$ stages), we come to the situation $z_n=z_{n-1}^{\epsilon_1}z_{n-2}^{\epsilon_2},...,z_1^{\epsilon_{n-1}}$, $e_n\neq 0$, $e_n\in K$ and hence $e_n=\frac{f(x)}{g(x)}$, $(f(x),g(x))=1$, $f(x),g(x)\in F_1[x]$ and $\epsilon_1=1$ or 2 for all i with $1\leq i\leq n-1$. Taking cubes on both sides we get

$$(x+a_n)=(x+a_{n-1})^{\epsilon_1}(x+a_{n-2})^{\epsilon_2}...(x+a_1)^{\epsilon_{n-1}}\frac{f(x)^3}{g(x)^3}$$

Using unique factorization, we get $x+a_n$ divides both $f(x)$ and $g(x)$, contradicting $(f(x),g(x))=1$.

We have proved that $Z^3-(x+a_n)$ is irreducible in $K(z_1,...,z_{n-1})[Z]$ and hence $[K(z_1,...,z_n):K(z_1,...,z_{n-1})]=3$. So we get $[K(z_1,...,z_n):K]=$

3^n. Thus $1, z_n, z_n^2$ are linearly independent over $K(z_1, ..., z_{n-1})$. Now M is an algebraic separable normal extension of K and from the above considerations we easily have $G(M/K) \simeq \Pi\mathbf{Z}/3\mathbf{Z}$. Hence $|G(M/K)| = 3^{|F|}$. Since E is an algebraic closure of M, each element of $G(M/K)$ extends to an element of $G(E/K) \subset G$. Hence $|G| \geq 3^{|F|} = 2^{|F|}$ when the characteristic of $F = 2$.

Therefore $|G| = 2^{|F|}$ and the proof of Proposition 5 is complete.

REMARK: Our paper [S1] determined the center of G.

REFERENCES

[B]. N. Bourbaki, *Algebra II*, Hermann, Paris, 1959.

[C]. A. Charnow, *The automorphisms of an algebraically closed field*, Canad. Math. Bull **18** (1970), 95–97.

[HR]. E. Hewitt and K.A. Ross, *Abstract harmonic analysis I*, Grundlehren series, Springer-Verlag, Heidelberg, 1963.

[J]. N. Jacobson, *Lectures in abstract algebra*, vol. 3, Van Nostrand, 1964.

[S]. T. Soundararajan, *On the automorphisms of the complex numbered field*, Math. Mag. **40** (1967), 213.

[S1]. T. Soundararajan, *Groups of automorphisms of algebraically closed extension field*, Maths. Today **I** (1983), 17–24.

[V]. B.L. Vander Waerden, *Algebra I*, Frederick Ungar Publishing Co., New York, 1970.

[W]. W. Wiesław, *On some characterisations of the complex number field*, Colloq. Math. **XXIV** (1972), 139–145.

DEPARTMENT OF MATHEMATICS
MADURAI KAMARAJ UNIVERSITY
MADURAI 625 021
INDIA