BULLETIN 13 (1), 1970

THE AUTOMORPHISMS OF AN ALGEBRAICALLY CLOSED FIELD

BY
A. CHARNOW

I. It is well known that the complex number field has infinitely many automorphisms. Moreover, it seems to be part of the folklore that the family of all automorphisms of the complex field has cardinality 2^{c}, where $c=2^{\aleph_0}$. In this article the following generalization of this fact is proved: If k is any algebraically closed field then the family of all automorphisms of k has cardinality $2^{\text{card } k}$.

The complex field has infinite transcendency degree over its prime subfield. For fields of this type the proof is accomplished by essentially permuting the elements in a transcendency basis and extending each permutation to an automorphism of the field. On the other hand, an algebraically closed field which has finite transcendence degree over its prime subfield must be countable and in this case the problem reduces to proving the existence of $2^{\aleph_0}$ automorphisms.

II. Lemma 1. *Let Ω be an algebraic closure of a field k. Let K be a subfield of Ω containing k. Let ϕ be an isomorphism of K into Ω. Assume that $k\subset\phi(k)$. Then ϕ can be extended to an automorphism of Ω.*

Proof. Let $K'=\phi(K)$. Let S be the set of all polynomials in $K[x]$ of positive degree. Since Ω is also an algebraic closure of K, Ω is a splitting field of S over K. Since $k\subset\phi(k)$, $k\subset K'\subset\Omega$ and hence Ω is an algebraic closure of K'. Let S' be the set of all polynomials in $K'[x]$ of positive degree. Then Ω is a splitting field of S' over K'. Hence by [2] Theorem 2, p. 145, ϕ can be extended to an isomorphism of Ω onto Ω.

Theorem 1. *If Ω is an algebraically closed field and if A is the family of all automorphisms of Ω then* card $A\geq 2^{\aleph_0}$.

Proof. Let π be the prime subfield of Ω and let B be a transcendency basis of Ω over π. We first construct inductively a sequence $\{k_n\}$ of subfields of Ω satisfying the following conditions:

(1) $\pi(B)\subset k_1$, $k_n\subset k_{n+1}$, $[k_n:\pi(B)]<\infty$ for all n.

(2) For each n there exist 2^n distinct $\pi(B)$ isomorphisms of k_n into Ω. These isomorphisms will be denoted $\phi(i_1, i_2, \ldots, i_n)$ where each i_j is either 0 or 1.

(3) Each $\phi(i_1, i_2, \ldots, i_n, i_{n+1})$ extends $\phi(i_1, i_2, \ldots, i_n)$.

Since π is a prime field there exist irreducible polynomials in $\pi[x]$ of arbitrarily

Received by the editors September 24, 1969.

https://doi.org/10.4153/CMB-1970-019-3 Published online by Cambridge University Press

high degree. (This follows from the Eisenstein Criteria if π is the rationals and from [1] Corollary 3, p. 128, if π is the integers modulo a prime.) Let f be an irreducible polynomial in $\pi[x]$ of degree ≥ 2. Since π is perfect, f is separable. Clearly f remains irreducible in the polynomial ring $\pi(B)[x]$. Let a and b be distinct roots of f in Ω. Let $k_1=\pi(B)(a)$. Let $\phi(0)$ be the $\pi(B)$ isomorphism of k_1 onto $\pi(B)(b)$ which sends a into b. Let $\phi(1)$ be the identity isomorphism of k_1. Now suppose we have constructed fields $k_1, k_2, \ldots, k_N$ satisfying conditions 1, 2 and 3. Let $t=[k_N\colon \pi(B)]$. Choose an irreducible separable polynomial g in $\pi[x]$ with degree $g>t$. Then g remains irreducible in $\pi(B)[x]$. Let c be a root of g in Ω. Since c is separable over $\pi(B)$, it follows that c is also separable over k_N. If $c\in k_N$ then $t<\deg g=[\pi(B)(c)\colon \pi(B)]\leq[k_N\colon \pi(B)]=t$, a contradiction. Thus $c\notin k_N$ and $[k_N(c)\colon k_N]\geq 2$. Let h be the minimal polynomial of c over k_N. Then h is irreducible in $k_N[x]$ and separable, and $\deg h\geq 2$. Let $k_{N+1}=k_N(c)$. Let $\phi=\phi(i_1,\ldots,i_N)$ be any one of the already determined isomorphisms of k_N into Ω. Let $\bar{k}_N=\phi(k_N)$ and let $\bar{h}$ be the polynomial obtained by applying ϕ to the coefficients of h. Then clearly $\bar{h}$ is irreducible in $\bar{k}_N[x]$ and separable, and degree $\bar{h}=$ degree $h\geq 2$. Let r_0 and r_1 be distinct roots of $\bar{h}$ in Ω. Then ϕ can be extended to an isomorphism $\phi(i_1, i_2, \ldots, i_N, 0)$ of k_{N+1} onto $\bar{k}_N(r_0)$ which sends c into r_0. But ϕ can also be extended to an isomorphism $\phi(i_1, i_2, \ldots i_N, 1)$ of k_{N+1} onto $\bar{k}_N(r_1)$, sending c into r_1. Thus each $\phi(i_1,\ldots,i_N)$ has 2 distinct extensions to isomorphisms of k_{N+1} into Ω. Hence we have found 2^{N+1} distinct isomorphisms of k_{N+1} into Ω. This completes the proof of the existence of the sequence $\{k_n\}$.

Let $K=\bigcup_1^\infty k_n$. Then K is a field and $\pi(B)\subset K\subset\Omega$. Let x be any real number with $0<x<1$. Let $x=.i_1\, i_2\ldots$ be the binary expansion of x. Let ϕ_x be the map defined on K by: $\phi_x(t)=\phi(i_1, i_2,\ldots, i_n)(t)$ if $t\in k_n$. Clearly ϕ_x is a $\pi(B)$ isomorphism of K into Ω. Since Ω is an algebraic closure of $\pi(B)$ we can apply Lemma 1 and extend ϕ_x to an automorphism of Ω. Then the map $x\rightarrow\phi_x$ is an injection of the interval (0, 1) into A. Thus card $A\geq 2^{\aleph_0}$.

LEMMA 2. *Let S be a set with card $S\geq 2$. Then there exists a permutation f of S such that $f(x)\neq x$ for all $x\in S$.*

Proof. Let $F=\{f \mid f$ is a permutation of some subset of S, $f(x)\neq x$ for all $x\in$ domain $f\}$. Since card $S\geq 2$, F is not empty. If f and g are in F we place $f<g$ provided domain f is a subset of domain g and g extends f. Thus $<$ partially orders F. By Zorn's Lemma F has a maximal member g. Let $A=$ domain g. If $A=S$ we set $f=g$ and the proof is complete. Assume $A\neq S$. Since g is maximal it follows that card $(S-A)=1$. Thus $S=A\cup\{x\}$, $x\notin A$. Fix an element $a\in A$. Let f be the mapping defined on S as follows: $f(a)=x$; $f(x)=g(a)$; $f(t)=g(t)$ if $t\neq a$, $t\in A$. It is easily seen that f is a permutation of S and $f(t)\neq t$ for all $t\in S$.

THEOREM 2. *Let B be an infinite set. Let A be the family of all permutations of B. Then* card $A=2^{\text{card}\, B}$.

https://doi.org/10.4153/CMB-1970-019-3 Published online by Cambridge University Press

Proof. Let T be the family of all those subsets of B having cardinality ≥ 2. If $S \in T$ then by Lemma 2 there exists a permutation f_S of S such that $f_S(x) \neq x$ for all $x \in S$. Let g_S be a map on B defined by:

$$g_S(x) = \left\{\begin{matrix} f_S(x) & \text{if } x \in S \\ x & \text{if } x \in B-S \end{matrix}\right\}.$$

Then $g_S \in A$. Let h be the map of T into A defined by $h(S) = g_S$ for $S \in T$. It follows that h is 1-1 and hence card $T \leq$ card A. Let C be the family of all subsets of B. Then:

$$2^{\text{card}\, B} = \text{card}\, C = 1 + \text{card}\, B + \text{card}\, T = \text{card}\, T \leq \text{card}\, A.$$

Now let D be the family of all subsets of $B \times B$. Since $A \subset D$ we have: card $A \leq$ card $D = 2^{\text{card}(B \times B)} = 2^{\text{card}\, B}$. Thus card $A = 2^{\text{card}\, B}$.

Theorem 3. *Let Ω be an algebraically closed field and let F be the family of all automorphisms of Ω. Then* card $F = 2^{\text{card}\, \Omega}$.

Proof. Let A be the family of all subsets of $\Omega \times \Omega$. Since $F \subset A$ and Ω is infinite we have: card $F \leq$ card $A = 2^{\text{card}(\Omega \times \Omega)} = 2^{\text{card}\, \Omega}$.

Now let B be a transcendence basis of Ω over its prime subfield π.

Case 1. B is finite. Then clearly $\pi(B)$ is countable and card $\Omega = \aleph_0$. By Theorem 1 we have that card $F \geq 2^{\aleph_0} = 2^{\text{card}\, \Omega}$.

Case 2. B is infinite. Then clearly card $\pi(B) =$ card B. Also, card $\Omega =$ card $\pi(B)$ ([2] lemma p. 143). By Theorem 2 there exist $2^{\text{card}\, B}$ permutations of B. Each of these yields a distinct π automorphism of $\pi(B)$. If ϕ is such an automorphism, then by Lemma 1, ϕ can be extended to an automorphism of Ω. Hence $2^{\text{card}\, \Omega} = 2^{\text{card}\, B} \leq$ card F.

References

1. I. Adamson, *Introduction to field theory*, Oliver and Boyd, London, 1964.
2. N. Jacobson, *Lectures in abstract algebra*, vol. 3, Van Nostrand, Princeton, N.J., 1964.

California State College,
Hayward, California

https://doi.org/10.4153/CMB-1970-019-3 Published online by Cambridge University Press