THE CONSTRUCTION OF FIELDS WITH INFINITE CYCLIC AUTOMORPHISM GROUP

WILLEM KUYK*

1. Introduction. This paper deals with a problem raised in a paper by J. de Groot **(1)**: Do there exist fields Ω whose full automorphism group is isomorphic to the additive group of integers Z?

The answer to this question is yes. In this paper we construct, given any subfield k of the complex numbers, extension fields Ω of k such that the automorphism group $G(\Omega/k)$ of Ω with respect to k is infinite cyclic. Fields having the infinite cyclic group as a *full* group of automorphisms are obtained by choosing the base field k in such a way that it does not contain any subfield k_0 so that k possesses non-trivial automorphisms leaving k_0 pointwise fixed. This property is seen immediately. Examples of such special base fields are the field of rationals and the field of real numbers.

The fields Ω have transcendence degree 1 with respect to k, and can be obtained as follows. Let K be an algebraic closure of $k(t_0)$. For $i \leqslant 0$, define the elements $t_{i-1} \in k(t_0)$ by

$$t_i^2 = t_{i-1} + 1. \tag{1}$$

For $i > 0$ choose for each $i = 1, 2, 3, \ldots$ an element $t_i \in K$ satisfying (1). Now let Ω be the union of the subfields $k(t_i)$ of K. Ω is a field, since for every i, $k(t_{i+1})$ is an algebraic extension of $k(t_i)$ of degree 2. The fact that $G(\Omega/k)$ contains a subgroup isomorphic to Z is seen by considering the substitution $\pi : t_i \rightarrow t_{i+1}$ $(i \in Z)$. This substitution defines a mapping of Ω upon itself. It is an isomorphism because π preserves the relation $t_i^2 = t_{i-1} + 1$ and because t_i is transcendental with respect to k. π has infinite order and generates together with its inverse $\pi^{-1}: t_{i+1} \rightarrow t_i$ the infinite cyclic group $C[\pi] \cong Z$. We shall prove that, besides the automorphisms in $C[\pi]$, there are no other automorphisms of Ω leaving the elements of k fixed.

THEOREM. *The automorphism group* $G(\Omega/k)$ *of the field* $\Omega = \bigcup_{i \in Z} k(t_i)$ *is* $C[\pi]$.

2. Proof of the Theorem.

LEMMA 1. *Every element of the set* $k(t_i)\backslash k(t_{i-1})$ $(i \in Z,\ i \geqslant 1)$ *has algebraic degree* 2^i *with respect to* $k(t_0)$.

Proof (by induction). Every element of $k(t_1)\backslash k(t_0)$ has degree 2 with respect

*N.R.C. Postdoctorate Fellow 1963, University of Ottawa.
Received May 5, 1964.

to $k(t_0)$. We shall show that there are no other elements in Ω with degree 2 over $k(t_0)$. For let θ be such an element, $\theta \in k(t_n)\backslash k(t_{n-1})$ for some $n \geqslant 2$. Then $\theta = a_0 + a_1 t_n$, with $a_0, a_1 \in k(t_{n-1})$ and $a_1 \neq 0$. There exist isomorphisms of $k(t_{n-1}, \theta)$ into K which are the identity on $k(t_{n-1})$ and take Ω into itself and θ into $a_0 + a_1(-t_n)$. But also the isomorphism σ of $k(t_{n-1})$ into K which is the identity on $k(t_{n-2})$ and takes t_{n-1} into $-t_{n-1}$ can be extended in two ways to isomorphisms of $k(t_n)$ which take t_n into s_n and $-s_n$, where s_n is an element of K with $s_n^2 = -t_{n-1} + 1$. These isomorphisms take θ into $a_0^\sigma \pm a_1^\sigma s_n$. One can easily verify that

$$k(t_{n-1}, s_n) \cap k(t_n) = k(t_{n-1}),$$

so these four images of θ are distinct. Thus θ has at least four conjugates over $k(t_0)$ and cannot be quadratic over $k(t_0)$.

COROLLARY. *Ω has no non-trivial automorphisms with respect to $k(t_0)$.*

Proof. Suppose σ is such an automorphism. Then let n be the smallest integer for which t_n is not invariant under σ. σ changes t_n into $-t_n$. But this isomorphism cannot be extended to $k(t_{n+1})$, because the $k(t_0)$-conjugate s_{n+1}, which has degree 2 over $k(t_n)$, is not in $k(t_{n+1})$, and hence not in Ω. The same argument shows that if a k-automorphism σ of Ω carries an element t_m into an element t_n, then σ has to be equal to π^{n-m}.

LEMMA 2. *Any automorphism σ of Ω which is the identity on k and takes $k(t_0)$ into itself is the identity.*

Proof. By a well-known theorem (**2**, Section 63), σ takes t_0 into

$$s_0 = \frac{at_0 + b}{ct_0 + d}, \qquad a, b, c, d \in k; \begin{vmatrix} ab \\ cd \end{vmatrix} \neq 0.$$

Let $s_1 = \sigma(t_1)$. By isomorphism, $s_1^2 = s_0 + 1$, and $k(s_1)$ is the unique quadratic extension of $k(s_0) = k(t_0)$ in Ω. Thus $k(s_1) = k(t_1)$ and

$$s_0 + 1 = \frac{p^2}{q^2}(t_0 + 1),$$

with $p, q \in k[t_0]$. Suppose p/q is in lowest terms. Then

$$\frac{(a + c)t_0 + b + d}{ct_0 + d} = \frac{p^2(t_0 + 1)}{q^2}. \tag{2}$$

Case 1, $(t_0 + 1) \nmid q$. Then the right side of (2) is still in lowest terms, so q^2 is a constant and $c = 0$. We may assume that $d = q = 1$. Then (2) becomes $at_0 + b + 1 = p^2 t_0 + p^2$; by comparing coefficients we see that p is a constant and that $s_0 = p^2 t_0 + p^2 - 1$. This yields $s_1^2 = p^2(t_0 + 1)$, $s_1 = pt_1$ (for p suitably chosen in k), and

$$(\sigma t_2)^2 = s_2^2 = s_1 + 1 = pt_1 + 1.$$

By the same argument, $(pt_1 + 1)/(t_1 + 1)$ must be the square of an element of $k(t_1)$, which cannot be true unless $p = 1$.

Case 2, $q = q_1(t_0 + 1)^i$. Then

$$\frac{(a + c)t_0 + b + d}{ct_0 + d} = \frac{p^2}{q_1^2(t_0 + 1)^{2i-1}},$$

with both sides in lowest terms; so p = constant, q_1 = constant, and $i = 1$. We can take $q_1 = 1$ and obtain

$$s_0 = \frac{-t_0 + p^2 - 1}{t_0 + 1} = \frac{p^2}{t_0 + 1} - 1.$$

This yields $s_1 = pt_1^{-1}$. As before,

$$\frac{s_1 + 1}{t_1 + 1} = \frac{p + t_1}{t_1(t_1 + 1)}$$

must be a square in $k(t_1)$, but there can be no such square. Therefore Lemma 2 follows.

Proof of the theorem. Let σ be any automorphism of Ω which is the identity on k. Then $\sigma t_0 = s_0 \in k(t_n)$ for some smallest integer n. Replacing σ by $\pi^{-n}\sigma$ if necessary, we may assume that

$$\sigma t_0 = s_0 \in k(t_0)\backslash k(t_{-1}).$$

Let $s_\nu = \sigma t_\nu$ for each ν. Then there is a smallest m with $t_0 \in k(s_m)$, since σ is a k-automorphism. Then $m \geqslant 0$, since otherwise $s_0 \in k(t_0)$, $s_0 \notin k(s_{-1})$ gives a contradiction. $k(s_m)$ contains $k(s_0)$ and is of degree 2^m over it. Applying Lemma 1, we see that $k(s_0, t_0) = k(t_0)$ is of degree 2^m over $k(s_0)$, and hence $k(t_0) = k(s_m)$. Now $s_m = \sigma\pi^m t_0$; hence $\sigma\pi^m$ takes $k(t_0)$ onto itself and is by Lemma 2 equal to the identity.

Remark 1. If we take the defining equation for t_i to be $t_i^2 = t_{i-1} + c$ with $0 \neq c \in k$, then the proof of the theorem remains valid. We obtain in this way a set of different field extensions of k having infinite cyclic automorphism group. If, however, the relation is chosen to be $t_i^2 = t_{i-1}$, then the theorem remains true only if k does not contain the imaginary unit i. It is easily seen that in that case the lemma remains valid because $i \notin k$ implies that

$$k((-t_{n-1})^{\frac{1}{2}}) \cap k(t_n) = k(t_{n-1}).$$

Remark 2. We may try to take the defining relations between the t_i to be of higher degree. If, for example, $t_i^3 = t_{i-1} + c$, $0 \neq c \in K$, then the theorem still holds true, but the computational work as carried out in the lemmas is considerably more complicated. If $t_i^3 = t_{i-1}$, where K does not contain a primitive third root of unity, then $G(\Omega/k)$ is isomorphic to the direct product of Z and a group of order 2. The automorphism of the latter group stems from the fact that

$$k((-t_{n-1})^{1/3}) \cap k(t_n) = k(t_n).$$

Remark 3. The proof of the theorem can be seen to remain valid if we take for k a field of characteristic $p > 0$, $p \neq 2$.

REFERENCES

1. J. de Groot, *Groups represented by homeomorphism groups* I, Math. Ann., *138* (1959), 80–102.
2. B. L. Van der Waerden, *Algebra*, Vol. I (Berlin, 1955).

Mathematical Centre, Amsterdam, and
McGill University, Montreal

https://doi.org/10.4153/CJM-1965-066-4 Published online by Cambridge University Press