PROCEEDINGS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 122, Number 1, September 1994

AUTOMORPHISMS OF THE ORDERED MULTIPLICATIVE GROUP OF POSITIVE RATIONAL NUMBERS

A. M. W. GLASS AND PAULO RIBENBOIM

(Communicated by Andreas R. Blass)

To Trevor Evans—In Memoriam

ABSTRACT. We prove

Theorem. *The only automorphism of the ordered multiplicative group of positive rational numbers is the trivial automorphism.*

We also give other examples of multiplicative groups of real positive algebraic numbers whose only order-preserving automorphisms are trivial.

1

The following problem was proposed by Hofberger [1, Problem 13]: *Determine the group of order-automorphisms of the multiplicative group of positive rational numbers.*

We prove that this group consists only of the identity automorphism.

The proof is an embarrassingly trivial application of two known theorems, one easy and one a very deep theorem about transcendental numbers.

Hion's Theorem. *If A and B are nontrivial subgroups of the additive group of real numbers, endowed with the natural ordering, and ϕ is a homomorphism of A into B that preserves order, then for some nonnegative real number r, $\phi(a) = ra$ for all $a \in A$.*

Hion's Theorem is easy to prove; a reference is [3, p. 46].

A far deeper theorem due to Siegel (unpublished), Lang [5], and Ramachandra [6] is

The Six Exponentials Theorem. *If $\{x_1, x_2, x_3, y_1, y_2\}$ is a set of complex numbers with $\{x_1, x_2, x_3\}$ and $\{y_1, y_2\}$ both linearly independent sets over $\mathbb{Q}$, the field of rational numbers, then at least one of $\exp(x_i y_j)$ $(i = 1, 2, 3;\ j = 1, 2)$ is transcendental.*

Received by the editors September 30, 1992 and, in revised form, November 19, 1992; the contents of this paper formed part of an invited talk by the first author at MSRI at a Conference on Transcendental Number Theory in May 1993.

1991 *Mathematics Subject Classification.* Primary 06F20, 20B27, 11J81.

This work was made possible by grants from NSF and NSERC, respectively. We are most grateful for this support. We also wish to thank Michel Waldschmidt for his helpful comments.

0002-9939/94 $1.00 + $.25 per page

The proof is easily accessible in [2, p. 119]. The *Matscience Notes* of Waldschmidt also provide a good reference to this latter topic [8].

2

Let $\mathbb{R}_{>0}$ denote the multiplicative group of positive real numbers. We use Hion's Theorem to obtain

Lemma. *Let G and H be subgroups of the ordered multiplicative group $\mathbb{R}_{>0}$. If $\theta: G \to H$ is an order-preserving homomorphism of G into H, then there is a nonnegative real number r such that $\theta(g) = g^r$ for every $g \in G$.*

Proof. Let λ be the logarithm mapping; it is a surjective order-isomorphism from the multiplicative group $\mathbb{R}_{>0}$ onto the additive group $\mathbb{R}$ of all real numbers (with the usual order). Then $\lambda \circ \theta \circ \lambda^{-1}: \lambda(G) \to \lambda(H)$ is an order-preserving homomorphism of the additive group $\lambda(G)$ into the additive group $\lambda(H)$. By Hion's Theorem, there exists a nonnegative real number r such that $\lambda \circ \theta \circ \lambda^{-1}(\lambda(g)) = r\lambda(g) = \lambda(g^r)$; thus, $\theta(g) = g^r$ for all $g \in G$. □

Let $\mathbb{A}$ be the field of all real algebraic numbers and $\mathbb{A}_{>0} = A \cap \mathbb{R}_{>0}$.

Proposition 1. *Let G, H, θ, and r be as in the lemma. If $G, H \subseteq \mathbb{A}_{>0}$ and G contains three multiplicatively independent elements g_1, g_2, and g_3, then r is a nonnegative rational number.*

Proof. If r were irrational, then $\{1, r\}$ would be multiplicatively independent. By the Six Exponentials Theorem, one of the numbers $g_1^r, g_2^r, g_3^r \in \mathbb{A}_{>0}$ would be transcendental, which is a contradiction. □

Proposition 2. *If θ is an order-preserving group homomorphism of the multiplicative group $\mathbb{Q}_{>0}$ into itself, then, for some positive integer r, $\theta(g) = g^r$ for all $g \in G$.*

Proof. We use Proposition 1 with $G = H = \mathbb{Q}_{>0}$. Let $r = \frac{n}{d}$ with $\gcd(n, d) = 1$. There exists a rational number $\frac{a}{b}$ with $\gcd(a, b) = 1$ such that $2^{n/d} = \frac{a}{b}$. By considering the 2-adic values of both sides, it follows at once that $d = 1$. Thus r is a positive integer. □

The Theorem now easily follows:

Proof. If θ is an automorphism, the above applies equally to θ^{-1}. Hence $\frac{1}{r}$ is also an integer; therefore, $r = 1$. □

We did not need the entire ordered multiplicative group of positive rational numbers, just a subgroup containing a subset of three multiplicatively independent elements. The Theorem and Proposition 2 hold equally under these weaker assumptions. They also hold for any ordered multiplicative group G of positive real algebraic numbers satisfying the hypotheses of Proposition 1 and the condition that for every positive rational number r that is not an integer, there is a $g \in G$ such that $g^r \notin G$.

It should be noted that we do not need the full force of the Six Exponentials Theorem to prove just the Theorem and Proposition 2. A far simpler proof due to Halberstam [4] shows that if r is irrational, then at least one of 2^r, 3^r, and 5^r is not an integer. A minor modification of his proof shows that not all of these numbers can be rational; this is all that is required to prove the Theorem and Proposition 2 but not Proposition 1.

Can we remove the extra hypothesis on G in Proposition 1?

The answer is yes. The key ingredient is again provided by Lang [5], Ramachandra [6], and Siegel, and is a corollary to the Six Exponentials Theorem:

If r is any irrational complex number and a $(\neq 0, \pm 1)$ is algebraic, then at least one of a^r, a^{r^2}, and a^{r^3} is transcendental.

By the lemma, if θ is any endomorphism of an ordered multiplicative group G of positive real numbers all of which are algebraic, then, for some real number $r \geq 0$, $\theta(a) = a^r$ for all $a \in G$. By the result just stated, either $G = \{1\}$ or r is rational (since $\theta \circ \theta$, etc., are also endomorphisms). Thus

Theorem. *If $G \neq \{1\}$ is an ordered multiplicative group of positive real numbers all of which are algebraic, then $\mathrm{Aut}(G, \cdot, \leq)$ is isomorphic to a subgroup of $(\mathbb{Q}^+, \cdot)$.*

3

The same ideas allow us to construct many multiplicative groups of real positive algebraic numbers whose only order-preserving group automorphism is the identity.

We begin by establishing some easy facts.

Let G be a subgroup of the multiplicative group $\mathbb{R}_{>0}$, $r \in \mathbb{R}_{>0}$, and $G^r = \{g^r \mid g \in G\}$.

(3.1). *If $r = \frac{n}{d}$ with $\gcd(n, d) = 1$ and $G = G^r$, then $G = G^d$.*

Proof. Since $G = G^r$, it follows that $G^d = G^n$. Write $1 = an + bd$ with a and b integers. Let $g \in G$, so $g = (g^a)^n (g^b)^d$. Since $G^n = G^d$, there is $h \in G$ such that $g^n = h^d$. Hence $g = (h^a g^b)^d \in G^d$. □

(3.2). *Assume $G \neq G^d$ for all positive integers d greater than 1. If $r \in \mathbb{Q}_{>0}$ and $G = G^r$, then $r = 1$.*

Proof. Let $r = \frac{n}{d}$ with $\gcd(n, d) = 1$. If $d > 1$, then $G = G^d$ by (3.1). This is absurd, so $d = 1$ and $r = n$. Then $G = G^r = G^n$, and $n = 1$ by assumption. □

(3.3). *If $G \neq G^p$ for every prime p, then $G \neq G^d$ for every integer $d > 1$.*

Proof. If $d > 1$, let p be a prime divisor d. Then $G^d \subseteq G^p \subsetneq G$. □

Let G be a multiplicative subgroup of $\mathbb{A}_{>0}$. If v is any valuation of any subfield K of $\mathbb{A}$ containing G, then $v(G) = \{v(g) \mid g \in G\}$ is a subgroup of the additive group $\mathbb{Q}$, as is well known (see, e.g., [7]).

Extending Proposition 2, we show

Proposition 3. *Let K be any subfield of $\mathbb{A}$ having one valuation v with value group $v(K) = \frac{1}{e}\mathbb{Z}$, $e \geq 1$ (for example, if $[K : \mathbb{Q}] < \infty$). If G is any multiplicative subgroup of $K_{>0} = K \cap \mathbb{A}_{>0}$, then the identity is the only order-automorphism of G.*

Proof. Let p be any prime and v any valuation of K with value group $v(K) = \frac{1}{e}\mathbb{Z}$. If $G = G^p$ then $v(G) = pv(G)$ and iterating, for each $n \geq 1$, $v(G) = p^n v(G)$. Thus, given $g \in G$, for each $n \geq 1$ there exists $h_n \in G$ such that $v(g) = p^n v(h_n)$. If $v(g) = \frac{m}{e}$ and $v(h_n) = \frac{d_n}{e}$ with $m, d_n \in \mathbb{Z}$, then $m = p^n d_n$ for every $n \geq 1$, which is impossible. Thus, for each prime p, $G \neq G^p$. By (3.3), $G \neq G^d$ for each $d > 1$. By Proposition 1, if θ is an ordered-group

automorphism of G, then there exists $r \in \mathbb{Q}_{>0}$ such that $\theta(g) = g^r$ for every $g \in G$. By (3.2), $r = 1$, so θ is the identity mapping. □

To conclude, we observe that it is possible (and well known) to construct subfields K of $\mathbb{A}$ with the property required in Proposition 3 but of infinite degree over $\mathbb{Q}$. This construction uses a particular case of the following existence theorem of Hasse-Krull [7, p. 270].

Hasse-Krull Theorem. *Let K be a number field of finite degree over $\mathbb{Q}$. Suppose d is a positive integer greater than 1, and let $v_1, \dots, v_k$ be valuations of K. Assume that integers $e_{ij} \geq 1$ and $f_{ij} \geq 1$ $(j = 1, \dots, r_i;\ i = 1, \dots, k)$ are given such that $\sum_{j=1}^{r_i} e_{ij} f_{ij} = d$ for each $i = 1, \dots, k$. Then there exists a field $\hat{K}$ of degree d over K such that each valuation v_i has r_i extensions $\hat{v}_{i1}, \dots, \hat{v}_{ir_i}$ to $\hat{K}$, the valuation $\hat{v}_{ij}$ having ramification index e_{ij} and inertial degree f_{ij}.*

We will only use this result for $k = 1$.

Let p be any prime, d_1 an integer greater than 1, $e_p = 1$, and $f_1 = d_1$. Then there exists a field $\hat{K}_1$ of degree d_1 over $\mathbb{Q}$ such that the p-adic valuation of $\mathbb{Q}$ has only one extension $\hat{v}_1$ to $\hat{K}_1$ and $\hat{v}_1(\hat{K}_1) = \mathbb{Z}$. Let $K_1 = \hat{K}_1 \cap \mathbb{A}$, and let v_1 be the restriction of $\hat{v}_1$ to K_1; so $v_1(K_1) = \mathbb{Z}$.

Assume that $\mathbb{Q} = K_0 \subset K_1 \subset K_2 \subset \cdots \subset K_n$ are subfields of $\mathbb{A}$ such that K_n has exactly one valuation v_n extending the p-adic valuation and $v_n(K_n) = \mathbb{Z}$.

Given $d_{n+1} > 0$, $e_{n+1} = 1$, and $f_{n+1} = d_{n+1}$, the above argument shows that there exists a subfield K_{n+1} of $\mathbb{A}$ of degree d_{n+1} over K_n such that v_n has exactly one extension to K_{n+1}; moreover, $v_{n+1}(K_{n+1}) = \mathbb{Z}$.

Let $K = \bigcup_{n \geq 0} K_n$ and let v be the unique valuation of K extending the p-adic valuation. Then $v(K) = \mathbb{Z}$.

Proposition 3 is applicable to any subgroup G of $K_{>0}$. In particular, choose $g_n \in K_{n,>0} \backslash K_{n-1}$ for each $n \geq 1$. Then the multiplicative group G generated by $\{g_n \mid n \geq 1\}$, like $\mathbb{Q}_{>0}$, is not finitely generated, and the identity is the only ordered-group automorphism of G.

References

1. M. Giraudet (ed.), *First meeting on ordered groups and infinite permutation groups, problem sessions & abstracts*, CIRM Luminy, France, July 1990.
2. A. Baker, *Transcendental number theory*, Cambridge Univ. Press, Cambridge, 1975.
3. L. Fuchs, *Partially ordered algebraic systems*, Pergamon Press, Oxford, 1963.
4. H. Halberstam, *Transcendental numbers*, Math. Gaz. **58** (1974), 276–284.
5. S. Lang, *Algebraic values of meromorphic functions*, Topology **5** (1966), 363–370.
6. K. Ramachandra, *Contributions to the theory of transcendental numbers.* II, Acta Arith. **14** (1967), 73–88.
7. P. Ribenboim, *Théorie des valuations*, Presses Univ. Montréal, Montréal, 1964.
8. M. Waldschmidt, *Linear independence of logarithms of algebraic numbers*, Mathematical Notes, Matscience Institute, Madras.

Department of Mathematics and Statistics, Bowling Green State University, Bowling Green, Ohio 43403-0221

Department of Mathematics and Statistics, Queen's University, Kingston, Ontario, Canada K7L 3N6