ISRAEL JOURNAL OF MATHEMATICS, Vol. 73, No. 2, 1991

ALGEBRAIC NUMBER FIELDS ELEMENTARILY DETERMINED BY THEIR ABSOLUTE GALOIS GROUP

BY

ALEXANDER PRESTEL

Fakultät für Mathematik, Universität Konstanz, 7750 Konstanz, FRG

ABSTRACT

Let K be an (infinite) number field. If K is elementarily determined by its absolute Galois group $G(K)$ (see (1.1) below), then K is isomorphic to $\tilde{\mathbf{Q}}$, $\mathbf{R} \cap \tilde{\mathbf{Q}}$ or some henselian subfield of $\tilde{\mathbf{Q}}$.

1. Introduction and result

In this note we prove that an algebraic number field K (i.e., a subfield of the algebraic closure $\tilde{\mathbf{Q}}$ of the field $\mathbf{Q}$ of rational numbers) whose "algebraic properties" are completely "determined" by its absolute Galois group $G(K) = \mathrm{Aut}(\tilde{K}/K)$ is isomorphic to either $\mathbf{C} \cap \tilde{\mathbf{Q}}$, $\mathbf{R} \cap \tilde{\mathbf{Q}}$, or an algebraic extension of $\mathbf{Q}_p \cap \tilde{\mathbf{Q}}$ where $\mathbf{Q}_p$ is the field of p-adic numbers for some rational prime p. This answers a question posed by M. Jarden.

To be more precise, we will consider fields $K \subset \tilde{\mathbf{Q}}$ such that, for all fields L of characteristic zero,

$$(1.1) \qquad \textit{if } G(L) \cong G(K) \quad \textit{and} \quad \tilde{L} = L\tilde{\mathbf{Q}}, \quad \textit{then } L \equiv K.$$

The isomorphism is meant as isomorphism of profinite groups, and $L \equiv K$ denotes that L and K are elementarily equivalent. This last notion comes from model theory (see, e.g., [C–K] or [P]) and means, in the case of the fields K and L, that every property of K which can be expressed by some formula φ, using only field operations and quantification over arbitrary elements of K, also holds in L.

Received May 16, 1990

(Note that by passing to negated formulas $\neg\varphi$ one sees that the relation $K \equiv L$ is actually symmetric.) In this paper we will understand by an "algebraic property" of K a property which can be expressed by such a formula. Thus, K and L have the same algebraic properties if they are elementarily equivalent. It is known from model theory that a field K (of characteristic zero) has elementarily equivalent fields L in any infinite cardinality. Thus, elementary equivalence of K and L by no means implies isomorphism. However, it is also well known in model theory that K and L are elementarily equivalent, if and only if they have isomorphic ultrapowers (see [C–K]).

If an algebraic number field K satisfies (1.1), we say that K is *elementarily determined by* $G(K)$. Fields K, for which (1.1) holds, are the local fields $\mathbf{C}$, $\mathbf{R}$, and all $\mathbf{Q}_p$. In fact, for fields L of characteristic zero we have:

$$\text{(1.2)} \qquad \textit{if } G(L) \cong G(\mathbf{C}), \qquad \textit{then } L \equiv \mathbf{C},$$

$$\text{(1.3)} \qquad \textit{if } G(L) \cong G(\mathbf{R}), \qquad \textit{then } L \equiv \mathbf{R},$$

$$\text{(1.4)} \qquad \textit{if } G(L) \cong G(\mathbf{Q}_p) \quad \textit{and} \quad L\tilde{\mathbf{Q}} = \tilde{L}, \qquad \textit{then } L \equiv \mathbf{Q}_p.$$

In (1.2), $G(L) = 0$ implies that L is algebraically closed. Since char $L = 0$, it is well known† that $L \equiv \mathbf{C}$. In (1.3) we have $G(L) = \mathbf{Z}/2\mathbf{Z}$ which, by a theorem of Artin–Schreier ([A–S], Satz 4), implies that L is real closed. Now the well-known Tarski Principle gives that $L \equiv \mathbf{R}$. The result of (1.4) is due to F. Pop ([Po], Theorem E.11). Whether the additional condition $L\tilde{\mathbf{Q}} = \tilde{L}$ can be dropped or not is still unknown. For that reason we have also added this condition to (1.1). But it should be pointed out that adding this condition actually strengthens our result.

If we replace the fields $\mathbf{C}$, $\mathbf{R}$, and $\mathbf{Q}_p$ by their algebraic parts $\mathbf{C} \cap \tilde{\mathbf{Q}}$, $\mathbf{R} \cap \tilde{\mathbf{Q}}$, and $\mathbf{Q}_p \cap \tilde{\mathbf{Q}}$, nothing changes in (1.2)–(1.4). In fact, the absolute Galois group of the algebraic part is the same as that of the corresponding local field. Now our result is

THEOREM. *Let K be an algebraic number field. If K is elementarily determined by $G(K)$, then K is isomorphic either to $\mathbf{C} \cap \tilde{\mathbf{Q}}$, $\mathbf{R} \cap \tilde{\mathbf{Q}}$ or to some algebraic extension of $\mathbf{Q}_p \cap \tilde{\mathbf{Q}}$ where p is a rational prime.*

An algebraic extension K of $\mathbf{Q}_p \cap \tilde{\mathbf{Q}}$ clearly is henselian valued by the unique extension of the p-adic valuation to K. The classification of those extensions which actually are elementarily determined by their absolute Galois groups is still missing.

†Often called the Lefschetz Principle.

2. Proof of the theorem

In the lemma below we will show that an algebraic number field K which satisfies (1.1) carries a V-topology τ such that K is relatively algebraically closed in the completion $(\widehat{K,\tau})$. Before stating and explaining this result, let us introduce the relevant notions. We will use here the notations of [P-Z].

By a field topology τ of K we mean a topology τ (given by the set of zero neighbourhoods) such that all field operations are continuous when defined. τ is called a *V-topology* if

(2.1)
$$\textit{for all } U \in \tau \textit{ there exists } V \in \tau \textit{ such that for all } x, y \in K: \quad \textit{if } xy \in V \textit{ then } x \in U \textit{ or } y \in U.$$

It is known from [F] and [K-D] that V-topologies are exactly those topologies τ which are either induced by some archimedean absolute value or some valuation (of arbitrary rank) on K.

The completion $(\widehat{K,\tau})$ of a topological field (K,τ), as a uniform space, is in general no longer a topological field (see [B], Ch. III, §6.8). In the case of a V-topological field, however, the completion is either **R** or **C** together with the usual topology (if τ is induced by some archimedean absolute value) or it is a complete valued field (see, e.g., [A], Appendix, §3). Thus, $(\widehat{K,\tau})$ is again a V-topological field. In both cases the V-topology of K can be extended to a V-topology $\tilde{\tau}$ of $\tilde{K}$ such that τ is induced from $\tilde{\tau}$ to K. Clearly, $(\widehat{K,\tau})$ is a closed subspace in the completion $(\widehat{\tilde{K},\tilde{\tau}})$ of $(\tilde{K},\tilde{\tau})$. It is now easy to prove that K is relatively algebraically closed in (K,τ) if and only if

(2.2)
$$\textit{every polynomial } f \in K[X] \textit{ whose value set } f(K) \textit{ approaches } 0, \quad \textit{actually has a zero in } K.$$

In fact, if $\alpha \in \hat{K}\backslash K$ is algebraic over K, then $f = \operatorname{Irr}(\alpha, K)$ has no zero in K, but clearly approaches 0 with values from K. Thus (2.2) does not hold. Conversely, let K be relatively algebraically closed in $(\widehat{K,\tau})$ and assume $f \in K[X]$ has no zero in K. Then, in $\tilde{K}$ we have $f(X) = a\prod_{i=1}^{n}(x - \alpha_i)$ with $\alpha_i \in \tilde{K}\backslash\hat{K}$. Hence, there is some neighbourhood U in the completion $(\widehat{\tilde{K},\tilde{\tau}})$ such that $\alpha_i + U \cap \hat{K} = \varnothing$ for all $1 \leq i \leq n$. From (2.1) it now follows that there exists a neighbourhood V in $(\widehat{\tilde{K},\tilde{\tau}})$ such that $f(\hat{K}) \cap V = \varnothing$. This clearly implies $f(K) \cap (V \cap K) = \varnothing$. Thus, $f(K)$ cannot approach 0.

The main step for the proof of our theorem is the following

LEMMA. *Let K be an algebraic number field satisfying* (1.1). *Then there exists a V-topology on K such that K is relatively algebraically closed in the completion* $(\widehat{K,\tau})$.

The theorem now follows from the lemma. In fact, let K be an algebraic number field. If the V-topology τ given by the lemma is induced by some archimedean absolute value of K, the completion $(\widehat{K,\tau})$ must be either $\mathbf{C}$ or $\mathbf{R}$ with the canonical topology. Since K is relatively algebraically closed in $(\widehat{K,\tau})$, K is either $\mathbf{C} \cap \tilde{\mathbf{Q}}$ or $\mathbf{R} \cap \tilde{\mathbf{Q}}$. If, however, the V-topology τ is induced by some valuation v of K, the restriction of v to $\mathbf{Q}$ must coincide with some p-adic valuation v_p of $\mathbf{Q}$. Since K is an algebraic extension of $\mathbf{Q}$, the value group $v(K)$ has rank 1 (it actually is contained in $\mathbf{Q}$). Thus the completion $(\widehat{K,\tau})$ contains the completion of $(\mathbf{Q}, v_p)$, i.e., it contains the p-adic number field $\mathbf{Q}_p$. Since K is relatively algebraically closed in $(\widehat{K,\tau})$, it contains the algebraic part $\mathbf{Q}_p \cap \tilde{\mathbf{Q}}$ of $\mathbf{Q}_p$. Thus, in particular, K is henselian w.r.t. the valuation v.

PROOF OF THE LEMMA. Let K be an algebraic number field. We consider the field‡

$$L = K((t^{\mathbf{Q}})) \tag{2.3}$$

of formal series in t with rational, well-ordered exponents and coefficients from K. By v we denote the canonical valuation of L which assigns to each series the lowest exponent of t occurring in this series. The valued field (L, v) is henselian and the value group $v(L) = \mathbf{Q}$ is divisible. From these facts one easily deduces that

$$G(L) \cong G(K) \quad \textit{and} \quad \tilde{L} = L\tilde{\mathbf{Q}}. \tag{2.4}$$

For the second part of (2.4) one uses that a henselian field of residue characteristic zero cannot have an immediate algebraic extension. Thus, after making the residue field K algebraically closed by adding zeros from $\tilde{\mathbf{Q}}$, the field itself becomes algebraically closed.

Now by (1.1) we obtain $L \equiv K$ from (2.4). For L we have a V-topology τ, namely that induced by v, such that L is relatively algebraically closed in the completion $(\widehat{L,\tau})$, since (L,τ) is actually complete. The main point of the proof is now to transfer the existence of such a V-topology from L to K. This will be done by expressing the existence of such a V-topology purely 'algebraically'.

In case $K = \tilde{\mathbf{Q}} = \mathbf{C} \cap \tilde{\mathbf{Q}}$ there is nothing left to prove. Thus, we may assume that there exists a polynomial $g \in \mathbf{Z}[X] \setminus \mathbf{Z}$ which has no zero in K. Since $K \equiv L$ and

‡We are grateful to M. Jarden for drawing our attention to this field.

the coefficients of g are integers, g has no zero in L too. Since L is relatively algebraically closed in the completion $(\widehat{L,\tau})$, we get from (2.2) that $g(L)$ is bounded away from 0, i.e. there is some $U \in \tau$ such that $U \cap g(L) = \varnothing$. If we choose $a \in K$ such that $g'(a) \neq 0$, Hensel's Lemma implies that $b = g(a)$ is an inner point of $g(L)$. Thus, the set

$$S = \left\{ g(x)^{-1} - b^{-1} \,\middle|\, x \in L \right\} \tag{2.5}$$

is a bounded neighbourhood of zero, and hence the multiples

$$c \cdot S \text{ with } c \in L^{\times} \tag{2.6}$$

form a base for the topology τ (cf. [P–Z], Lemma 2.1, and the definition of V-topologies). Using this fact, we can now formulate (2.2) as follows:

$$\begin{gathered} \textit{for all } f \in L[X]\textit{: if to any } c \in L^{\times} \textit{ there exists some } a \in L \\ \textit{such that } f(a) \in cS\textit{, then } f \textit{ has a zero in } L. \end{gathered} \tag{2.7}$$

Clearly, this can be expressed in the (algebraic) language of fields: let $\varphi(c,y)$ denote the formula

$$\exists x\; y = c(g(x)^{-1} - b^{-1}), \tag{2.8}$$

then (2.7) may be expressed as a scheme of formulas depending on the degree of f. If we let

$$f = a_0 + \cdots + a_d X^d \tag{2.9}$$

then (2.7) for the degree d is expressed by the formula ψ_d

$$\forall a_0, \ldots, a_d [\forall c \neq 0\; \exists z\, \varphi(c, f(z)) \rightarrow \exists z\, f(z) = 0]. \tag{2.10}$$

Since $K \equiv L$, every ψ_d also holds in K. Thus the collection of sets

$$c \cdot S_K \textit{ with } c \in K^{\times} \textit{ and } S_K = \left\{ g(x)^{-1} - b^{-1} \,\middle|\, x \in K \right\} \textit{ satisfies (2.7) in } K. \tag{2.11}$$

It remains to be seen that the collection (2.11) is a base of some V-topology on K. This, however, also can be easily expressed by some formula σ using, again, the base defined by φ as in (2.10). Since σ holds in L by construction, and $K \equiv L$, it also holds in K. q.e.d.

Let us mention at the end of this note that it was essential to start with an algebraic number field K. In this case a V-topology τ on K which is not induced by some archimedean absolute value must come from a rank 1 valuation v. This implies that the completion of (K, v) is a henselian field. In case K is an arbitrary field of characteristic zero which would satisfy

$$G(K) \cong G(L) \Rightarrow K \equiv L \tag{2.12}$$

for every field L of characteristic zero, the proof of our Lemma would give a valuation v of arbitrary rank, and thus $(\widehat{K, v})$ would no longer be henselian. In this case, however, one can strengthen the lemma in the following sense.

In [P–Z] the notion of a *topological henselian* field has been introduced. This is a V-topological field (K, τ) which satisfies the following topological version of Hensel's Lemma:

(2.13) *to every n there exists some $U \in \tau$ such that every polynomial*

$$X^{n+1} + X^n + a_{n-1}X^{n-1} + \cdots + a_0 \text{ with } a_i \in U \text{ has a zero } \alpha \neq 0 \text{ in } K.$$

Every algebraically closed field K with any V-topology τ is topologically henselian. Also, every real closed field K with the V-topology induced from its unique ordering as well as every henselian valued field (K, v) with the V-topology induced by v is topologically henselian. As shown in [P–Z], these examples, however, do not exhaust the class of topological henselian fields.

Using essentially the same arguments as in the proof of the lemma (see also [P–Z], Remark 7.11) one gets the following

REMARK. Every field K of characteristic zero satisfying (2.12) carries a V-topology τ such that (K, τ) is topologically henselian.

It should be mentioned that a topological henselian field (K, τ) always is relatively algebraically closed in its completion, but not conversely.

What we have just explained is only relevant if the following problem has a positive answer.

PROBLEM. Does there exist a field K of characteristic zero such that for all fields L of characteristic zero

$$G(K) \cong G(L) \Rightarrow K \equiv L \quad \text{and} \quad L \not\subset \tilde{\mathbf{Q}}? \tag{2.14}$$

REFERENCES

[A–S] E. Artin and O. Schreier, *Eine Kennzeichnung der reell abgeschlossenen Körper*, Abh. Math. Seminar Hamburg **5** (1927), 225–231.

[A] J. Ax, *A metamathematical approach to some problems in number theory*, AMS Symp. **20** (1971), 161–190.

[B] N. Bourbaki, *Elements of Mathematics, General Topology*, Part I, Hermann, Paris, 1966.

[C–K] C. C. Chang and H. J. Keisler, *Model Theory*, North-Holland, Amsterdam, 1973.

[F] I. Fleischer, *Sur les corps localement bornés*, C. R. Acad. Sci. Paris Sér. B **237** (1953), 546–548.

[K-D] H. J. Kowalsky and H. Dürbaum, *Arithmetische Kennzeichung von Körpertopologien*, J. Reine Angew. Math. **191** (1953), 135–152.

[Po] F. Pop, *Galoissche Kennzeichnung p-adisch abgeschlossener Körper*, J. Reine Angew. Math. **392** (1988), 145–175.

[P.] A. Prestel, *Einführung in die Mathematische Logik und Modelltheorie*, Braunschweig, 1986.

[P-Z] A. Prestel and M. Ziegler, *Model theoretic methods in the theory of topological fields*, J. Reine Angew. Math. **299/300** (1978), 318–341.