Can. J. Math., Vol. XXXII, No. 2, 1980, pp. 431–440

INTERSECTIONS OF REAL CLOSED FIELDS

THOMAS C. CRAVEN

1. In this paper we wish to study fields which can be written as intersections of real closed fields. Several more restrictive classes of fields have received careful study (real closed fields by Artin and Schreier, hereditarily euclidean fields by Prestel and Ziegler [**8**], hereditarily pythagorean fields by Becker [**1**]), with this more general class of fields sometimes mentioned in passing. We shall give several characterizations of this class in the next two sections. In § 2 we will be concerned with $\mathrm{Gal}(\bar{F}/F)$, the Galois group of an algebraic closure $\bar{F}$ over F. We also relate the fields to the existence of multiplier sequences; these are infinite sequences of elements from the field which have nice properties with respect to certain sets of polynomials. For the real numbers, they are related to entire functions; generalizations can be found in [**3**]. In § 3 a characterization is given in terms of finite Galois extensions of the field. This is applied in § 4 to show that these fields suffice to obtain all isomorphism classes of reduced Witt rings (of equivalence classes of anisotropic quadratic forms over a field) with a certain finiteness condition on the rings.

In this section we shall briefly outline some of the work other authors have done with these and related classes of fields. Our interest is only in formally real fields, though to study them we shall often have to look at their algebraic extensions. For any formally real field F, we denote by F^* the intersection of all the real closed subfields of a fixed algebraic closure $\bar{F}$ which contain F. These fields have been studied in [**6**] where they are called "galois order closed" because of the following theorem.

THEOREM 1.1 (cf. [**6**]). *The field F^* is the maximum normal extension of F to which all orderings of F extend.*

A field is called *pythagorean* if every sum of squares is again a square. Thus the field F^* is pythagorean since it is an intersection of pythagorean fields. Pythagorean fields have been characterized by Diller and Dress [**4**], and this provides the inspiration for the results in § 3. One can always consider the pythagorean closure F_p of a field F, namely the intersection of all pythagorean fields containing F. See [**7**] for a construction of F_p. It is not difficult to obtain the following connection between F^* and the pythagorean closure.

Received May 29, 1978. This work was partially supported by the National Science Foundation.

PROPOSITION 1.2. (cf. [**6**]). *The pythagorean closure of F is the intersection of F^* with the quadratic closure of F.*

As examples of intersections of real closed fields, we have hereditarily euclidean fields (all formally real algebraic extensions are euclidean; i.e. pythagorean with one ordering), which are characterized as intersections of real closed fields, any two of which are isomorphic over their intersection [**8**]. More generally, we have hereditarily pythagorean fields (all formally real algebraic extensions are pythagorean), which are characterized by the property that every formally real extension L is equal to L^* [**1**]. Both of these classes of fields have been characterized in several different ways and have interesting applications in the study of Witt rings.

Example. The field $\mathbf{Q}^*$, where $\mathbf{Q}$ denotes the field of rational numbers, is an intersection of real closed fields which is not hereditarily pythagorean. First note that since $\mathbf{Q}^*$ is a normal extension of $\mathbf{Q}$, the field $\mathbf{Q}^*$ consists of precisely those elements of $\bar{\mathbf{Q}}$ whose minimal polynomial over $\mathbf{Q}$ has only real roots. Thus $\sqrt[3]{2}$ is not in $\mathbf{Q}^*$. One then checks that $1 + (\sqrt[3]{2})^2$ is not a square in $\mathbf{Q}^*(\sqrt[3]{2})$, so that this extension of $\mathbf{Q}^*$ is not pythagorean and hence $\mathbf{Q}^*$ is not hereditarily pythagorean.

2. In this section we characterize fields which are intersections of real closed fields in terms of the Galois groups of their algebraic closures and in terms of the behaviour of polynomials. We feel that the characterization in terms of modifying the coefficients of polynomials is particularly interesting since no comparable results seem to exist for other classes of fields. The proof ultimately makes use of results in entire function theory due to Polya and Schur ([**3**]). We know of no strictly algebraic proof of [**3**, Theorem 3.7], and this result is certainly crucial to our present work.

Definition 2.1. Let F be a formally real field, and let

$$\Gamma = \{\gamma_0, \gamma_1, \ldots, \gamma_n\}$$

be a sequence of elements of F. For any polynomial $f(x) = \sum a_i x^i$ of degree at most n in $F[x]$, write $\Gamma[f]$ for the polynomial $\sum a_i \gamma_i x^i$. We call Γ an *n-sequence for F* if, given any such polynomial f which splits in F, the polynomial $\Gamma[f]$ also splits in F. If an infinite sequence Γ is an n-squence for all $n = 1, 2, 3, \ldots$, we call Γ a *multiplier sequence for F.*

Multiplier sequences for the real numbers have been studied by Polya and Schur and related to entire functions; generalizations to other fields can be found in [**3**]. Among other things, the following theorem shows that an infinite sequence of totally positive elements (that is, positive in all orderings) is a multiplier sequence for a field $F = F^*$ if and only if $\Gamma[(x + 1)^n]$ splits in F for all positive integers n.

https://doi.org/10.4153/CJM-1980-034-2 Published online by Cambridge University Press

THEOREM 2.2. *Let F be a formally real field with algebraic closure $\bar{F}$. The following conditions are equivalent:*

(a) *If $\Gamma = \{\gamma_0, \gamma_1, \dots, \gamma_n\}$ is a sequence of totally positive elements of F and the polynomial*

$$\Gamma[(x+1)^n] = \sum_{k=0}^{n} \binom{n}{k} \gamma_k x^k$$

splits in F^*, then Γ is an n-sequence for F.

(b) *If a polynomial f over F splits in F^*, then f splits in F.*

(c) *Let I be the subgroup of $G = \mathrm{Gal}(\bar{F}/F)$ generated by all involutions. Then I is dense in G in the profinite topology; that is, $IN = G$ for any normal subgroup N of finite index in G.*

(d) *F is an intersection of real closed fields; that is, $F = F^*$.*

Proof. (a) $\Rightarrow$ (b). Let $f(x) = \sum_{i=0}^{n} a_i x^i$, $a_n = 1$ be a polynomial over F which splits in F^*. Let α be any root of F. For any ordering of F^* and corresponding absolute value, we have

$$\alpha = -a_{n-1} - a_{n-2}\alpha^{-1} - \dots - a_0\alpha^{1-n} \leqq \sum_{i=0}^{n-1} |a_i\alpha^{i+1-n}|.$$

From this it follows that

$$\alpha \leqq 1 + \sum_{i=0}^{n-1} |a_i| \leqq 1 + \sum_{i=0}^{n-1} (1 + a_i^2) = b.$$

Without loss of generality, we may replace $f(x)$ by $f(x + b)$, so that the roots of f may be assumed to be negative in all orderings. Thus the coefficients of f are totally positive. Now set Γ equal to $\{\gamma_0, \dots, \gamma_n\}$ where γ_k is a totally positive element of F defined by

$$f(x) = \sum_{k=0}^{n} \gamma_k \binom{n}{k} x^k.$$

Then, since f splits in F^*, condition (a) says that Γ is an n-sequence for F, and thus $f(x) = \Gamma[(x + 1)^n]$ splits in F.

(b) $\Rightarrow$ (c). Let H be the closure of I and let K be the fixed field of H. Since H contains every involution of G, the field K is contained in every fixed field of an involution; that is, the field K is contained in every real closed subfield of $\bar{F}$ which contains F, and hence $K \subset F^*$. Now let α be an element of K with minimal polynomial f over F. Since F^* is a normal extension of F, the polynomial f splits in F^*, and so (b) implies that $\alpha \in F$. Therefore $K = F$ and so $H = G$ by the Galois correspondence theorem.

(c) $\Rightarrow$ (d). Each involution in G fixes some real closed field containing F, so F^* is fixed by I. But then F^* is fixed by the closure of I, which is all of G, whence $F = F^*$ is an intersection of real closed fields.

(d) $\Rightarrow$ (a). Assume $\Gamma[(x+1)^n]$ splits in F^* and $f \in F[x]$ splits in F. We must show that $\Gamma[f]$ splits in F. But [**3**, Theorem 3.7] shows that $\Gamma[f]$ splits in every real closed field containing F^*, and thus it splits in $F = F^*$ which is the intersection of those real closed fields.

COROLLARY 2.3. *Let F be a field with a unique ordering and let R be a real closure of F. The following conditions are equivalent:*

(a) *If Γ is a sequence of positive elements of F and $\Gamma[(x+1)^n]$ splits in R, then Γ is an n-sequence for F.*

(b) *If $f \in F[x]$ splits in R, then it splits in F.*

(c) *The field R contains no proper normal extension of F.*

(d) $\mathrm{Gal}(\bar{F}/F)$ *has no proper normal closed subgroup containing an involution.*

(e) *The field F is an intersection of real closed fields.*

Proof. Since F has a unique ordering, any two real closures of F are isomorphic over F. Thus a polynomial over F which splits in one will split in all of them. Also, any two involutions in $\mathrm{Gal}(\bar{F}/F)$ are conjugate since their fixed fields are isomorphic over F. In view of these facts, the result follows immediately from the previous theorem.

Example 2.4. Let F be a field satisfying the conditions of Theorem 2.2. Let a, b be totally positive elements of F (i.e., squares in F). Then $\Gamma = \{\gamma_0, \gamma_1, \gamma_2, \ldots\}$, where $\gamma_k = a + kb$, is a multiplier sequence for F. We need only check that $\Gamma[(x+1)^n]$ splits in F. But we have

$$\Gamma[(x+1)^n] = \sum_{k=0}^{n} (a+kb)\binom{n}{k}x^k = a(x+1)^n + b\sum_{k=1}^{n} k\binom{n}{k}x^k$$

$$= a(x+1)^n + bnx\sum_{k=0}^{n-1}\binom{n-1}{k}x^k = (x+1)^{n-1}((a+bn)x+a).$$

3. In this section we shall give a characterization of fields which are intersections of real closed fields in terms of their finite Galois extensions. This characterization will be used to obtain our results in § 4. The ideas behind the theorem are due to Griffin, though the results he claims in [**6**] are incorrect. The following proposition shows that [**6**, Proposition 8] is incorrect. We shall obtain corrected versions of Proposition 11 and Corollary 12 of [**6**] as our characterization of intersections of real closed fields. The proofs of the following two propositions are contained in the proof of [**4**, Satz 1]. These also appear as an exercise in [**7**].

PROPOSITION 3.1. *Let K be a field, b an element of K which is not a square, and $L = K(\sqrt{b})$. There exists a quadratic extension M of L such that M/K is cyclic of degree 4 if and only if b can be written as a sum of two squares. If M exists, it may be chosen inside K_p.*

Proof. Assume first that b is a sum of two squares.

https://doi.org/10.4153/CJM-1980-034-2 Published online by Cambridge University Press

First note that, without loss of generality, we may assume $b = a^2 + 1$. Set $M = K(e)$ where $e = (b + \sqrt{b})^{1/2}$ and $f = (b - \sqrt{b})^{1/2}$. Over K, the element e has four different conjugates $\pm e$, $\pm f = \pm e^{-1}a\sqrt{b}$, all of which lie in M. Thus M is Galois over K. Let $\sigma \in \mathrm{Gal}(M/K)$ with $\sigma(\sqrt{b}) = -\sqrt{b}$ and $\sigma(e) = f$. Since $f = e^{-1}a\sqrt{b}$, we have $\sigma^2(e) = \sigma(e^{-1}a\sqrt{b}) = -e$, so that σ does not have order 2. Therefore $\mathrm{Gal}(M/K)$ must be cyclic of order 4. Finally, we have $M \subset K_p$ since $b + \sqrt{b} = \frac{1}{2}a^2 + \frac{1}{2}(1 + \sqrt{b})^2$ is a square in K_p.

Conversely, assume b cannot be written as a sum of two squares and assume $M = K(\sqrt{b}, (\alpha + \beta\sqrt{b})^{1/2})$ is a cyclic extension of K of degree 4 with $\alpha, \beta \in K$. Set $e = (\alpha + \beta\sqrt{b})^{1/2}$ and $f = (\alpha - \beta\sqrt{b})^{1/2}$. Since M is a normal extension of K, the element f must lie in M, and hence $ef = (\alpha^2 - \beta^2 b)^{1/2} \in M$.

We first note that $ef \notin K$; for if $ef \in K$, one can easily check that $\mathrm{Gal}(M/K)$ has exponent 2, a contradiction. Also we can write

$$\alpha^2 - \beta^2 b = (r + s\sqrt{b} + t(\alpha + \beta\sqrt{b})^{1/2} + u(\alpha b + \beta b\sqrt{b})^{1/2})^2,$$

where $r, s, t, u \in K$. This implies

$$\begin{aligned}
&(1)\ \alpha^2 - \beta^2 b = r^2 + bs^2 + \alpha t^2 + \alpha b u^2 + 2\beta btu\\
&(2)\qquad\quad\ \ 0 = \beta t^2 + \beta bu^2 + 2rs + 2\alpha tu\\
&(3)\qquad\quad\ \ 0 = 2rt + 2bsu\\
&(4)\qquad\quad\ \ 0 = 2ru + 2st.
\end{aligned}$$

Equations (3) and (4) imply either $ru = st = 0$ or $b = (tu^{-1})^2$, contradicting our choice of b.

Case 1. $u = 0$. Equations (3) and (4) imply either $t = 0$ or $r = s = 0$. The latter clearly contradicts (1) and (2). For the former, equation (2) implies either $s = 0$ (and $ef = \pm r \in K$) or $r = 0$ (and $b = (\alpha s(s^2 + \beta^2)^{-1})^2 + (\alpha\beta(s^2 + \beta^2)^{-1})^2$ by (1)), neither of which can occur.

Case 2. $r = 0$. Equations (3) and (4) imply either $s = 0$ or $u = t = 0$. The latter was eliminated in Case 1. For the former, equation (2) becomes

$$0 = \beta bu^2 + 2\alpha tu + \beta t^2,$$

which when solved for u, implies that $ef \in K$. Thus all possibilities lead to contradictions and the proposition is proved.

PROPOSITION 3.2. *Let M be a field with proper subfields $K \subset L$ such that M/K is cyclic of degree 4. Then $L \subset K_p$.*

Proof. Assume that $L = K(\sqrt{a})$ and $M = L((b + c\sqrt{a})^{1/2})$, $a, b, c \in K$. Let σ be a generator of $\mathrm{Gal}(M/K)$ and set $e = (b + c\sqrt{a})^{1/2}$. Then σ^2 fixes L, so $\sigma^2(e) = -e$. Since σ does not fix L, we must have $\sigma(\sqrt{a}) = -\sqrt{a}$, and hence $\sigma(e^2) = b - c\sqrt{a}$. These lead to

$$(e\sigma(e))^2 = e^2\sigma(e^2) = b^2 - ac^2 \quad \text{and} \quad \sigma^2(e\sigma(e)) - e\sigma(e),$$

https://doi.org/10.4153/CJM-1980-034-2 Published online by Cambridge University Press

so that $e\sigma(e) \in L$. Thus

$$(e\sigma(e))^2 = b^2 - ac^2 \in K \cap L^2 = K^2 \cup aK^2.$$

If $(e\sigma(e))^2 \in K^2$, then $e\sigma(e)$ is fixed by σ, leading to a contradiction of $\sigma^2(e) = -e$. Therefore $b^2 - ac^2 \in aK^2$; say $b^2 - ac^2 = ax^2$. Then

$$a = b^2(c^2 + x^2)^{-1} = (bx(c^2 + x^2)^{-1})^2 + (bc(c^2 + x^2)^{-1})^2$$

is a sum of squares, hence is a square in K_p; and thus $L \subset K_p$.

Definition 3.3. Let L be a finite extension of a field K. Following [**6**], a chain of subfields $K = L_0 \subset L_1 \subset \ldots \subset L_n = L$, $n \geqq 0$, is called *pythagorean* if for each i, the degree $[L_{i+1} : L_i] = 2$ and L_{i+1} is contained in some cyclic extension of L_i of degree 4. The extension L/K is called *multiquadratic* if L is generated over K by the square roots of elements of K.

LEMMA 3.4. *Let L be a finite Galois extension of the formally real field K with $G = \mathrm{Gal}(L/K)$. The following conditions are equivalent:*

(a) $L \subset K^*$.

(b) *There exists a pythagorean chain from the fixed field of each Sylow 2-subgroup of G to a multiquadratic extension F of L contained in L_p. The field F can be chosen so that it is a finite Galois extension of K contained in K^*.*

(c) *There exists a pythagorean chain from the fixed field of some Sylow 2-subgroup of G to a multiquadratic extension F of L contained in L_p.*

Proof. (a) $\Rightarrow$ (b). Let M be the fixed field of a Sylow 2-subgroup of G and let $M = L_1 \subset L_2 \subset \ldots \subset L_n = L$ be a maximal chain of subfields from M to L. Since $\mathrm{Gal}(L/M)$ is a 2-group and any proper subgroup of a 2-group is contained in a normal subgroup of index 2, we have $[L_{i+1} : L_i] = 2$ for each i. Since $K \subset M \subset K^*$, any real closure of M contains K and any real closure of K contains $K^* \supset M$, so that $M^* = K^*$. Thus L is contained in the intersection of M^* with the quadratic closure of M, which by Proposition 1.2 is M_p. It follows that for each i, $L_{i+1} \subset (L_i)_p$, so we can write

$$L_{i+1} = L_i(\sqrt{b_i}) \quad \text{where}$$

$$b_i = \sum_{j=1}^{m_i} a_{ij}{}^2, \quad m_i \geqq 2, a_{ij} \in L_i.$$

We now construct a new chain of fields above M. Let

$$F_{11} = L_1;\ F_{1k} = F_{1,k-1}((a_{11}{}^2 + \ldots + a_{1k}{}^2)^{1/2}),\ k = 2, \ldots, m_1 - 1;$$
$$F_{21} = F_{1,m_1-1}(\sqrt{b_1});$$

and so forth to F_n, a multiquadratic extension of L contained in M_p. The chain just constructed is pythagorean by Proposition 3.1 since each

https://doi.org/10.4153/CJM-1980-034-2 Published online by Cambridge University Press

field is extended by the square root of a sum of two squares. Now let F be the normal closure of F_n over K. For any $\sigma \in \mathrm{Gal}(\bar{K}/K)$, we have $\sigma(\sum a_i^2) = \sum (\sigma(a_i))^2$ so that

$$\sigma((\sum a_i^2)^{1/2}) = \pm(\sum(\sigma(a_i))^2)^{1/2};$$

therefore, since L is normal over K, F is also a multiquadratic extension of L contained in $M_p \subset M^* = K^*$. It is easy to see that the chain of fields from M to F_n can be extended to F so that it remains pythagorean.

(b) $\Rightarrow$ (c). This is clear.

(c) $\Rightarrow$ (a). Let M be the fixed field of the Sylow 2-subgroup of G. Note that since F is a multiquadratic extension of L, the Galois group $\mathrm{Gal}(F/L)$ is a 2-group, so that M is also the fixed field of a Sylow 2-subgroup of $\mathrm{Gal}(F/K)$. Since $[M : K]$ is odd, all orderings of K extend to M. By Proposition 3.2 each field in the pythagorean chain is contained in the pythagorean closure of the preceding field. Thus $F \subset M_p \subset M^*$ and all of the orderings of M extend to F. Therefore all orderings of K extend to F. Since F is Galois over K, we obtain $F \subset K^*$ by Theorem 1.1 and therefore the subfield L is contained in K^*.

THEOREM 3.5. *Let K be a formally real field. The field K can be written as an intersection of real closed fields if and only if for every nontrivial finite Galois extension L of K, there is no pythagorean chain from the fixed field of any Sylow 2-subgroup of* $\mathrm{Gal}(L/K)$ *to L.*

Proof. Assume first that $K = K^*$, and that there is a pythagorean chain from the fixed field M of a Sylow 2-subgroup of $\mathrm{Gal}(L/K)$. Then $[M : K]$ is odd and $L \subset M_p$ so that every ordering of K extends to L. Since L is Galois over K, we obtain $L \subset K^*$ by Theorem 1.1. But $K = K^*$, so $L = K$, a contradiction. Conversely, assume $K \neq K^*$. Then there exists a nontrivial finite Galois extension L/K with $L \subset K^*$. Let M be the fixed field of a Sylow 2-subgroup of $\mathrm{Gal}(L/K)$. By the previous lemma, there exists a Galois extension F/K with $L \subset F \subset K^*$ and there exists a pythagorean chain from M to F. Also $F \subset L_p$, so that $\mathrm{Gal}(F/L)$ is a 2-group and M is also the fixed field of a Sylow 2-subgroup of $\mathrm{Gal}(F/K)$. Thus F is the desired extension to complete the proof of the theorem.

4. In this section we relate intersections of real closed fields to the study of quadratic forms over formally real fields. One approach to the study of quadratic forms over a field F is to consider the Witt ring of equivalence classes of anisotropic quadratic forms $W(F)$. When F is formally real, it is also useful to consider the reduced Witt ring $W_{\mathrm{red}}(F)$ (i.e., $W(F)$ modulo its nilradical). It is a well known fact that $W(F) = W_{\mathrm{red}}(F)$ for a formally real field F if and only if F is pythagorean. For further information on Witt rings, see [**7**]. The objective of this section is to prove the following theorem.

THEOREM 4.1. *Given any formally real field F with finitely many places into the real numbers, there exists a field K which is an intersection of real closed fields with $W(K)$ isomorphic to $W_{\text{red}}(F)$.*

In [**2**] we proved that a pythagorean field K satisfying the theorem always exists. Furthermore, the finiteness condition is independent of the chosen field F. The present theorem further restricts the class of fields needed to obtain all isomorphism classes of reduced Witt rings with the given finiteness condition. We conjecture that the theorem is true without the restriction to finitely many real places. We hope that by restricting the class of fields which one needs to consider, a deeper understanding of the structure of reduced Witt rings can be obtained. The proof of the above theorem will be based on valuation theory. The reader is referred to [**5**] or [**9**] for basic facts and definitions.

LEMMA 4.2. *If (F, v) is a henselian valued field with residue class field F_v where $F_v = F_v^*$ and the value group Γ_v is divisible, then $F = F^*$.*

Proof. Since F_v is formally real, the field F is also. Assume $F \neq F^*$. Then Theorem 3.5 implies that there exists a Galois extension L of F and a chain of subfields $F \subset L_0 \subset L_1 \subset \ldots \subset L_n = L$ such that L_0 is the fixed field of a Sylow 2-subgroup of $\mathrm{Gal}(L/F)$; for each i, the degree $[L_{i+1} : L_i] = 2$; and L_{i+1} is contained in some extension M_i with $\mathrm{Gal}(M_i/L_i)$ cyclic of order 4. We shall show that a corresponding chain exists for F_v, contradicting the hypothesis that $F_v = F_v^*$. Since (F, v) is henselian, the valuation v extends uniquely to each extension field L_i. For each i, let k_i be the residue class field and Γ_i the value group. Each $\Gamma_i = \Gamma_v$ since Γ_v is divisible. Thus the relation

$$[L_{i+1} : L_i] = [\Gamma_{i+1} : \Gamma_i][k_{i+1} : k_i]$$

shows that $[k_{i+1} : k_i] = 2$, $i = 0, \ldots, n - 1$. Similarly, $[L_0 : F] = [k_0 : F_v]$, and $[L : F] = [k_n : F_v]$, and the degree of the residue class field of M_i over k_i is 4. By [**10**, Chapter 6, Theorem 21], whenever our extensions are Galois, the residue class field extensions are also Galois with isomorphic Galois groups. In particular, the residue class field of M_i is a cyclic extension of degree 4 over k_i and k_0 is the fixed field of a Sylow 2-subgroup of $\mathrm{Gal}(k_n/F_v)$. We have thus shown that $k_0 \subset k_1 \subset \ldots \subset k_n$ is a pythagorean chain, contradicting our assumption that $F_v = F_v^*$.

Proof of Theorem 4.1. The reduced Witt rings of fields with finitely many places into the real numbers have been characterized in [**2**, Theorem 2.1]. They are precisely the rings constructed via the following recursion:

(a) The ring of integers, $\mathbf{Z}$, is one such ring.

(b) If R_1 and R_2 are such rings and M_i is the unique maximal ideal of R_i containing 2, then $R = \mathbf{Z} + M_1 \times M_2$ is again such a ring, where $\mathbf{Z}$ has the diagonal embedding in $R_1 \times R_2$.

(c) If R_0 is such a ring, then so is the group ring $R_0[\Lambda]$ where Λ is any group of exponent 2.

For (a), we can take the real numbers as our field. For construction (b), assume we have fields K_1, K_2 satisfying the theorem such that $R_i = W(K_i)$. We shall construct a field F which is an intersection of real closed fields with Witt ring isomorphic to $R = \mathbf{Z} + IK_1 \times IK_2$; here IK_i denotes the ideal of $W(K_i)$ formed by equivalence classes of all even dimensional forms, or equivalently, the unique maximal ideal containing 2. We first show that we can raise the transcendence degree of K_i over $\mathbf{Q}$ without changing the Witt ring. Let v be the x-adic valuation on $K_1(x)$, and let $M = K_1(x^{1/2}, x^{1/3}, x^{1/4}, x^{1/5}, \ldots)$ with w the extension of v to M. Then the residue class fields M_w and $K_1(x)_v$ are isomorphic to K_1, and the value group of w is divisible. Let $\tilde{K}_1$ be the henselization of M with respect to w. The field $\tilde{K}_1 = \tilde{K}_1{}^*$ by the previous lemma with $W(\tilde{K}_1) \cong W(K_1)$ [**2**] and transcendence degree over $\mathbf{Q}$ one greater that the transcendence degree of K_1 over $\mathbf{Q}$.

Iterating the above construction (infinitely often, if necessary), we may assume that $L \subset K_1, K_2$, where L is a purely transcendental extension of $\mathbf{Q}$ and the fields K_1, K_2 are algebraic over L. We consider two valuations on $L(x)$: the x-adic valuation will be denoted by v and the degree valuation will be denoted by w. Note that v and w are independent, and for both of them the residue class field is isomorphic to L. Theorem 27.6 of [**5**] implies that there exists a field L' algebraic over $L(x)$ and extensions v', w' of v, w, respectively, such that the value groups of v' and w' are divisible and the residue class fields satisfy $L'_{v'} \cong K_1$ and $L'_{w'} \cong K_2$. Let M_1, $\tilde{v}$ be the henselization of L' at v' and let M_2, $\tilde{w}$ be the henselization of L' at w'. Let $F = M_1 \cap M_2$. We have $M_1 = M_1{}^*$ and $M_2 = M_2{}^*$ by the lemma so $F = F^*$ also. To show that $W(F) \cong \mathbf{Z} + IK_1 \times IK_2 = \mathbf{Z} + IM_1 \times IM_2$, it will suffice to show that the canonical map

$$\varphi : F^{\cdot}/F^{\cdot 2} \rightarrow M_1{}^{\cdot}/M_1{}^{\cdot 2} \times M_2{}^{\cdot}/M_2{}^{\cdot 2}$$

is an isomorphism, since the Harrison subbasis determines the (reduced) Witt ring. (We use $F^{\cdot}$ to denote the multiplicative group of nonzero elements of F.) It is injective because $F = M_1 \cap M_2$. Let $v_0 = \tilde{v}|F$ and $w_0 = \tilde{w}|F$. Then M_1 is the henselization of F at v_0 and M_2 is the henselization of F at w_0. The valuations v_0 and w_0 are independent since they are extensions of v and w on $L(x)$. Given elements $m_i \in M_i{}^{\cdot}$, $i = 1, 2$, we can first find elements $a_i \in F^{\cdot}$ such that $m_i/a_i \equiv 1$ modulo the maximal ideal of the valuation ring of $\tilde{v}$ (for $i = 1$) or $\tilde{w}$ (for $i = 2$). Then apply the approximation theorem for independent valuations [**5**, Theorem 3.13] to obtain an element $a \in F$ such that

$$v(a - a_i) < \min(v(a_i), 1) \ (i = 1, 2).$$

Then $a/a_i - 1$ lies in the maximal ideal of the valuation ring of v_0 (for $i = 1$) or w_0 (for $i = 2$). Thus $am_i \in M_i^{\cdot 2}$, so the map φ is surjective.

Finally we consider construction (c). Given a group ring $W(K)[\Lambda]$ where $K = K^*$ and Λ is a group of exponent 2, we take F to be an iterated power series field over K, the number of variables being equal to the cardinality of an $\mathbf{F}_2$-vector space basis for Λ, where $\mathbf{F}_2$ denotes the field with two elements. Then F satisfies $W(F) \cong W(K)[\Lambda]$ [**2**]. To see that $F = F^*$, we need only note that when $K = \cap R_i$ with each R_i real closed, then $K((t)) = \cap R_i((t))$ where each field $R_i((t))$ is hereditarily pythagorean [**1**, Chapter 3, § 2]. This concludes the proof of the theorem.

References

1. E. Becker, *Hereditarily pythagorean fields and orderings of higher level*, Lecture Notes, Instituto de Matemática Pura e Aplicada, Rio de Janeiro (1978).

2. T. Craven, *Characterizing reduced Witt rings of fields*, J. Algebra *53* (1978), 68–77.

3. T. Craven and G. Csordas, *Multiplier sequences for fields*, Illinois J. Math. *21* (1977), 801–817.

4. J. Diller and A. Dress, *Zur Galoistheorie pythagoreischer Körper*, Arch. Math. *16* (1965), 148–152.

5. O. Endler, *Valuation theory* (Springer Verlag, New York, 1972).

6. M. Griffin, *Galois theory and ordered fields*, Queen's University Preprint (1972).

7. T. Y. Lam, *The algebraic theory of quadratic forms* (Benjamin, Reading, Mass., 1973).

8. A. Prestel and M. Ziegler, *Erblich euklidische Körper*, J. Reine Angew. Math. *274/275* (1975), 196–205.

9. P. Ribenboim, *Théorie des valuations* (Les Presses de l'Université de Montréal, 1964).

10. O. Zariski and P. Samuel, *Commutative algebra*, Vol. II (Van Nostrand, Princeton, NJ, 1960).

University of Hawaii,
Honolulu, Hawaii