TRANSACTIONS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 242, August 1978

A PROBABLE HASSE PRINCIPLE FOR PENCILS OF QUADRICS[1]

BY

WILLIAM C. WATERHOUSE

ABSTRACT. Let k be a global field, $\mathrm{char}(k) \neq 2$. Although pencils of quadrics over k may fail to satisfy a local-to-global equivalence principle, the failures are exceptional in the precise sense of having limiting probability zero. The proof uses the classification of pairs of quadratic forms. It also requires knowing that a square class in a finite extension usually comes from k when it does so locally; the Galois-theoretic criterion for this is determined.

I. **Square class descent.** Let k be a global field, $\mathrm{char}(k) \neq 2$. It is well known that an element in k is a square if it is so in all completions k_v, and indeed it is enough to assume the local condition for all but finitely many k_v. We consider now a relative version. Let c be a nonzero element in a finite extension F of k; we say that c satisfies the *global condition* of square class descent if it is an element of k times a square, or in other words the rank-one quadratic form $\langle c \rangle$ over F comes from a form over k. The question is whether this is implied by the *local conditions* that for all but finitely many k_v there are $b_v \neq 0$ in k_v with $c \otimes b_v$ a square in $F \otimes_k k_v$. The answer to this is needed for the following section on pencils of quadrics, but also has some interest of its own. Curiously, it turns on questions of finite group structure.

Notice first that we may as well assume F/k is separable. Indeed, let E be the maximal separable subextension. Then F/E is purely inseparable, and its degree q is odd since $\mathrm{char}(k) \neq 2$. If $c = u^2 b$ satisfies the global condition, then $c^q = (u^q)^2 b^q$ satisfies it in E/k. Conversely, if in E/k we have $c^q = v^2 b$, then $c = (vc^{-(q-1)/2})^2 b$ satisfies the condition in F/k. The same argument applies locally.

THEOREM 1. *Let F/k be a finite separable extension of global fields, c an element of F. Let M be a finite Galois extension of k containing $F(c^{1/2})$, with $G = \mathrm{Gal}(M/k)$. Then:*

(1) *The global condition of square class descent holds iff the subgroup fixing F has a normal complement over the subgroup fixing $F(c^{1/2})$.*

Received by the editors May 4, 1977.

AMS (MOS) subject classifications (1970). Primary 14G25; Secondary 12A65, 10C05.

[1]This work was partially supported by the National Science Foundation.

(2) *The local conditions hold iff elements fixing F but not $F(c^{1/2})$*
(i) *are not squares in G, and*
(ii) *have no conjugates fixing $F(c^{1/2})$.*

PROOF. (1) Let H and N be the subgroups fixing F and $F(c^{1/2})$. If c is a square in F, then $N = H$ and the condition is trivial, so we may assume $|H : N| = 2$. If $C = u^2b$ with b in k, then $F(c^{1/2}) = F(b^{1/2})$. Let N' be the normal subgroup of G fixing $k(b^{1/2})$; clearly $HN' = G$ and $H \cap N' = N$. Conversely, suppose we have an N' satisfying these conditions (i.e., a normal complement). Then $|G : N'| = |HN' : N'| = |H : H \cap N'| = 2$, so the fixed field of N' is a quadratic extension $k(b^{1/2})$. The composite $F \cdot k(b^{1/2})$ has fixing group $H \cap N' = N$, so $F(b^{1/2}) = F(c^{1/2})$. By Kummer theory then c and b are in the same square class in F.

(2) Consider now a completion k_v. Ignoring finitely many places, we may assume v is unramified in M. For w lying over v then the local extensions M_w/k_v are cyclic, say $\mathrm{Gal}(M_w/k_v) = \langle g_w \rangle$ Let F_w be the completion of F inside M_w. The subgroup fixing F_w is $\langle g_w \rangle \cap H$, and that fixing $F(c^{1/2})_w$ is $\langle g_w \rangle \cap N$. If these are equal, c is a square in F_w. If they are unequal, then as before we see that c is in $k_v F_w^2$ iff there is a normal complement. But since the whole group $\langle g_w \rangle$ is cyclic, this occurs iff $|\langle g_w \rangle : \langle g_w \rangle \cap H| = |F_w : k_v|$ is odd. Notice that when it occurs, the element b_w in k_v is unique up to squares in k_v, as $k_v(b_w^{1/2})$ will be the unique quadratic extension inside M_w.

The Chebotarev density theorem [**6**, p. I-7] shows that for every g in G there are infinitely many w with $g_w = g$. As we saw, the condition for c to be in $k_v F_w^2$ is that, if g^r is the first power of g to lie in H, then either g^r is in N or r is odd. If these fail, g^r is a square in H outside N. Conversely, if $h = f^2$ is a square in H outside N, then f is not in H, and taking $g_w = f$ gives infinitely many places where the condition fails. Thus (i) is the condition for c to be in all but finitely many $k_v F_w^2$.

This however is not the full local condition: $F \otimes k_v$ is the product of the various F_w, and we must be able to find b_v in k_v so that cb_v is a square in all F_w at once. The g_w chosen as Frobenius elements for various M_w fill out precisely a conjugacy class in G. There is of course no extra condition if $c^{1/2}$ is in all F_w, that is, $\langle g \rangle \cap H = \langle g \rangle \cap N$ for all g in the class. Similarly there is no extra condition if $c^{1/2}$ is outside all F_w, since the b_v needed is in all cases the one giving the unique quadratic subextension of M_w.

Suppose now that $\langle g \rangle \cap H \neq \langle g \rangle \cap N$ but $\langle g' \rangle \cap H = \langle g' \rangle \cap N$ for some conjugate g' of g. The b_v is needed at the completion giving g. If it works also for g', the completion of F there must include not only $c^{1/2}$ but also the quadratic extension $k_v(b_v^{1/2})$. That is, $|\langle g' \rangle : \langle g' \rangle \cap H|$ must be even. If g is in H outside N and g' is in N, clearly this condition fails. Conversely, suppose (i) holds but this further condition fails. Let g^r and $(g')^s$

be the first powers lying in H. By assumption g^r is not in N, so r is odd by (i). By assumption also s is odd and $(g')^s$ is in N. The least common multiple n of r and s then is odd, g^n is in H outside N, and its conjugate $(g')^n$ is in N. Thus (ii) is precisely what we need. □

COROLLARY 2. (a) *If $|F : k|$ is odd, the local conditions imply the global condition.*

(b) *If $F(c^{1/2})$ is an abelian extension of k, the local conditions imply the global condition.*

PROOF. The proof of (b) is elementary, looking at G modulo squares. For (a), note that (2)(ii) says the focal group of H in G is contained in N; the result then follows from a standard group-theory argument using the transfer, e.g. [4, p. 98]. □

COROLLARY 3. *Let c in F satisfy the local conditions. Let L be the Galois closure of F over k. Then $L(c^{1/2})$ is Galois over k.*

PROOF. Let A and B be the greatest normal subgroups contained in H and N respectively; we must show $A \cap N \subseteq B$. But any conjugate of $A \cap N$ is $\subseteq A \subseteq H$, so by (ii) of the theorem it is $\subseteq N$. □

When the local conditions hold, we see now that M in the theorem can be taken simply as $L(c^{1/2})$. The global condition can then be approached in two steps. *A fortiori* c satisfies the local conditions in L/k, and we ask first whether it satisfies the global condition in L/k; by the theorem this is a question of whether a certain $Z/2Z$-extension of $\mathrm{Gal}(L/k)$ splits. If it does, some b in k gives in L the same square class as c. Replacing c by c/b, we reduce the question to one where c is a square in L. This leaves only finitely many square classes, possibly no nontrivial ones, to check in F. The following examples show, however, that the implication may fail at either of these two steps.

EXAMPLE 4. (a) There is an abelian F/k with some c in F satisfying the local conditions but not the global condition.

(b) There is an F/k with some c in F having $c^{1/2}$ in L and satisfying the local conditions but not the global condition.

PROOF. (a) We know there are extensions M/k of number fields with arbitrary Galois groups, so we need only a group-theoretic example. Take $Z/2Z \times Z/4Z$, and let $\langle g \rangle$ of order 2 act on it by ${}^g(1, 0) = (1, 0)$ and ${}^g(0, 1) = (1, 1)$. Let G be the semidirect product, H the subgroup of order 2 generated by (1, 0), and N trivial. The quotient G/H is abelian of order 8. It is easy to compute that (1, 0) is the commutator $g(0, 1)g(0, -1)$, so H has no normal complement; but (1, 0) is not a square, and obviously is not conjugate to an element of N.

(b) For this example let G be the simple group $\mathrm{PSL}_2(F_{17})$. By [4, p. 115] its Sylow 2-group is dihedral of order 16, containing a cyclic subgroup H of order 8. Let N be the subgroup of H having order 4. The field F corresponding to H has by simplicity of G the Galois closure L equal to M, which of course contains the quadratic extension corresponding to N. The elements of H outside N all have order 8, so they have no conjugates in N; and they are not squares in G, since G contains no elements of order 16. As G is simple, H has no normal complement over N. □

Other group-theoretic arguments will give other situations where the local conditions do or do not imply the global condition. One further example is contained in the following result, which is what will be needed in the next section.

THEOREM 5. *Let F/k be an extension of degree n whose normal closure L has Galois group the symmetric group S_n. Then the local conditions in Theorem* 1 *imply the global condition.*

PROOF. Suppose first $n = 2$, so $L = F$. By Corollary 3 we know $F(c^{1/2})$ is Galois. Being of degree at most 4, it is abelian, and the result follows from Corollary 2. Thus we may assume $n > 2$, and of course we may also assume $c^{1/2}$ is not in F.

In any case $L(c^{1/2})$ is Galois. If $c^{1/2}$ is in L, we note that $\mathrm{Gal}(L/F) = S_{n-1}$ has only one subgroup of index 2, namely A_{n-1}; since $A_{n-1} = S_{n-1} \cap A_n$, there is a normal complement. Thus we may assume $L(c^{1/2}) \neq L$. We have then a group extension

$$0 \to Z/2Z \to G \to S_n \to 1.$$

Since $L(c^{1/2}) = L \otimes_F F(c^{1/2})$, the extension is split over the copy of S_{n-1} naturally embedded in S_n. We will show this implies the original extension is split. Since

$$H^1(S_n, Z/2Z) = \mathrm{Hom}(S_n, Z/2Z) \cong \mathrm{Hom}(S_{n-1}, Z/2Z),$$

we can adjust a splitting to make it agree with the given one on S_{n-1}, and we will be done.

If $Z/2Z$ is not in the commutator subgroup G', we get an extension

$$0 \to Z/2Z \to G/G' \to S_n/A_n \to 1.$$

This must be split since the corresponding extension of S_{n-1}/A_{n-1} is split. Hence there is a nonzero map $G/G' \to Z/2Z$ vanishing on S_n/A_n, and that splits the original extension. Thus we may assume the central $Z/2Z$ is in the commutator subgroup.

Such extensions of S_n were classified by Schur [5, p. 166]. For S_3 there are none. For $n \geqslant 4$ there are two of them, T_n and T_n', given as follows. Let $s_1 = (12), \ldots, s_{n-1} = (n-1, n)$ be the usual generators of S_n. Then T_n and

T_n' each have generators $u, t_1, \ldots, t_{n-1}$ with respective relations

$$\begin{aligned} u^2 &= e \\ t_i^2 &= u \\ (t_i t_{i+1})^3 &= u \\ t_i t_j &= u t_j t_i, \quad j \geqslant i+2 \end{aligned}$$

and

$$\begin{aligned} u^2 &= e \\ t_i^2 &= e \\ (t_i t_{i+1})^3 &= e \\ t_i t_j &= u t_j t_i, \quad j \geqslant i+2 \\ u t_i &= t_i u. \end{aligned}$$

Suppose first $n \geqslant 5$. Inside T_n the inverse image of the natural copy of S_{n-1} has order $2(n-1)!$. It contains u and $t_1, \ldots, t_{n-2}$; and these generate it, since $s_1, \ldots, s_{n-2}$ generate S_{n-1}. These elements satisfy the T_{n-1} relations, so by counting orders we see the inverse image is precisely T_{n-1}. Since T_{n-1} is not split over S_{n-1}, our hypotheses rule out this case. Similarly the restriction of T_n' to S_{n-1} is the nonsplit extension T_{n-1}'.

Finally say $n = 4$. The restriction of T_4 to S_3 has generators u, t_1, t_2 satisfying $u^2 = e$ and $t_1^2 = u = t_2^2 = (t_1 t_2)^3$; these define a group of order 12 and hence are defining relations. There is then a homomorphism onto $Z/4Z$ (sending t_1 and t_2 to the generator), and so the restriction is not split.

The restriction of T_4' to S_3 is split, and we must look directly at the local conditions. Here H is the inverse image of S_3, and N the subgroup $\simeq S_3$ generated either by t_1, t_2 or by ut_1, ut_2 (the two splittings). In T_4' we have $ut_1 t_3 = t_3 t_1$, or $t_3^{-1}(ut_1)t_3 = t_1$; thus an element of H not in N is conjugate to one in N, and the local conditions fail. □

Finally, it might be natural to ask whether we could deduce the global condition if we strengthened our hypotheses and assumed the local conditions at all primes without exception. This can be true in special cases, but we now show it does not always hold.

EXAMPLE 6. There is a finite abelian extension F/k of number fields with an element c in F not satisfying the global condition such that yet for every completion k_v there are $0 \neq b_v$ in k_v with $c \otimes b_v$ a square in $F \otimes_k k_v$.

PROOF. The local conditions in Theorem 1 hold at unramified primes, so the result will follow from Example 4(a) if we can choose the extension M/k to be everywhere unramified as well as having a specified group G. But a theorem of number theory shows this is possible–see the Appendix. □

II. **Pencils of quadrics.** A *pencil of quadrics* is a geometrically natural object of study which in algebraic terms is simply a two-dimensional space of quadratic forms. It is known that a local-to-global principle holds for pairs of quadratic forms over global fields [**8**, Theorem 5.3], so it is reasonable to ask whether it also holds for pencils of quadrics. The answer to this is *no* [**8**, Theorem 5.5]. But it takes some effort to find counterexamples, which suggests that in some sense the answer ought to be *yes*. We here establish this by proving that, as announced in [**10**], counterexamples occur only with asymptotic probability zero.

To have at least one way of making this precise, consider any property which may hold for m-tuples of elements in k. Suppose first that k is a number field. For each basis b of k over the rationals, consider the m-tuples whose entries in that basis all have integer coefficients no greater than N in absolute value. Let $P_b(N)$ be the portion of them having the property. If $P_b(N)$ always approaches 1 as N goes to infinity (i.e., the failures eventually occur with negligible frequency), we will say the property *holds with probability one*. For function fields we can use a similar definition, replacing Q by a rational function field and integers $\leqslant N$ by polynomials of degree $< N$. As an example, notice that any particular nontrivial polynomial in the m-tuples will be nonzero with probability one.

THEOREM 7. *Let k be a global field,* $\mathrm{char}(k) \neq 2$. *Let A and B be symmetric matrices corresponding to quadratic forms on k^n. With probability one B is nondegenerate and the matrix $T = B^{-1}A$ has an irreducible characteristic polynomial with Galois group S_n.*

PROOF. Let a_{ij} and b_{ij} for $i \leqslant j$ be indeterminate, and form the symmetric matrices $A = (a_{ij})$ and $B = (b_{ij})$. Here B is nondegenerate, and we can form the characteristic polynomial $f(x; a, b)$ of $B^{-1}A$. It has coefficients in the pure transcendental extension field $k(a_{ij}, b_{ij})$. If we specialize a_{ij} and b_{ij} to values in k, then with probability one B will still be nondegenerate, since we rule out only the zeros of the nontrivial polynomial $\det(b_{ij})$; and f will specialize to the characteristic polynomial of $B^{-1}A$.

If the original f is irreducible with Galois group S_n, the Hilbert irreducibility theorem [**2**, Chapter 8] and a supplementary argument of Hilbert's [**1**, Volume II, p. 181] show that the same is true of the specializations with probability one. Furthermore, the specializations (residue field extensions) always have group no larger than the original. Thus we need only show that there is at least one pair over k for which we get the symmetric group.

For this, let F be an extension of k of degree n whose normal closure has Galois group S_n. Let α be a generator of F/k. Define symmetric bilinear forms on the k-space $F \simeq k^n$ by $B(x, y) = \mathrm{Tr}_{F/k}(xy)$ and $A(x, y) =$

$\mathrm{Tr}_{F/k}(\alpha xy)$. Then T is the linear map multiplication by α, and its characteristic polynomial has the required property. □

THEOREM 8. *Let k be a global field,* $\mathrm{char}(k) \neq 2$. *Let A and B be two quadratic forms in $n \geq 5$ variables spanning a pencil of quadrics over k. With probability one the pencil has the property that any other pencil equivalent to it everywhere locally is equivalent over k.*

PROOF. We may assume A and B satisfy the conclusion of Theorem 7. Recall from [8] that a nonsingular pair (A, B) is classified by giving, for various exponents and various places of $k(X)$, quadratic forms over the residue fields. When B is nondegenerate, the places and exponents are those in the structure of T. In our case, then, (A, B) has simply an exponent 1, rank 1 invariant $\langle c \rangle$ over the field $F = k[X]/(f)$. A pencil spanned by A', B' will be equivalent iff it has some other basis $(sA' + tB', uA' + vB')$ with the same invariant as (A, B).

The map $T' = (B')^{-1}A'$ will in the new basis be replaced by $(sT' + t)(uT' + v)^{-1}$. Consider now the projective linear automorphisms of the projective line. If over any field a nontrivial one takes the set of $n \geq 5$ eigenvalues of T to itself, a nontrivial polynomial condition (equality of certain cross-ratios) must be satisfied. Hence with probability one this does not happen. Suppose now that A', B' span a pencil which is everywhere locally equivalent. Over each completion k_v there is then a projective linear map taking the eigenvalues of T' to those of T. This map is defined over the algebraic extension given by the eigenvalues, is unique by our previous argument, and lies in each k_v; hence it is defined over k.

Changing the basis (A', B') over k, then, we may assume the pair has single invariant $\langle c' \rangle$ at the same place $k[X]/(f)$. The uniqueness shows further that (bA', bB') are the only other pairs in that pencil which have invariant at that same place. Our pencils are equivalent over k then iff $\langle bc' \rangle$ is equivalent to $\langle c \rangle$, iff cbc' is a square, iff cc' in F is a square times an element of k.

The invariants over k_v occur at places corresponding to the factorization of f, with residue fields the various composites Fk_v: up to fixed scalar factors, they agree with c at each place [8, Theorem 4.3]. Again the only pairs in the other pencil with invariants at the same places are (b_vA', b_vB'). Thus local equivalence holds iff there are $0 \neq b_v$ in k_v such that $\langle c \rangle$ is equivalent to $\langle b_v c' \rangle$ in each composite, iff $cc' \otimes b_v$ is a square in $F \otimes k_v$. We thus have precisely the situation discussed in §I. Since the Galois group is S_n, Theorem 5 shows the local conditions imply the global condition. □

This probability one result is particularly striking in view of a further consequence which we can deduce from §I. The example in [8] of local-to-global failure for pencils is geometrically special: the eigenvalues of T are not distinct. It would be natural to think that the failure was caused by this

degeneracy and the associated change in the automorphism group. But we can now show that failure may occur for purely arithmetic reasons in a geometrically generic situation.

For this, let F/k be separable of degree $\geqslant 5$. As k is infinite, we can choose λ in F not lying in the finitely many intermediate fields and not satisfying any nontrivial cross-ratio identities among its conjugates. Let f be its minimal polynomial. Consider two pencils, one spanned by a pair with invariant $\langle 1\rangle$ at $k[X]/(f)$, the other spanned by a pair with invariant $\langle c\rangle$ there. The absence of cross-ratio identities shows that over $\bar{k}$ the automorphism groups of these pencils are of the generic type. As in the preceding proof, the pencils are equivalent over k iff c satisfies the global condition, and locally equivalent iff c satisfies the local conditions at every k_v. We know by Example 6 that the one need not imply the other.

Low dimensions are not covered by the proof of Theorem 8, since the eigenvalues of T then have nontrivial projective linear automorphisms. We conclude by settling a couple of these cases.

THEOREM 9. *The conclusion of Theorem* 8 *holds also for* $n = 2$ *and* $n = 3$.

PROOF. Again we may assume the conclusion of Theorem 7. Take first the case $n = 2$. Let $F = k(d^{1/2})$. By [9, p. 238] we can write $B(x, y) = \mathrm{Tr}_{F/k}(pxy)$ and $A(x, y) = \mathrm{Tr}_{F/k}(\alpha pxy)$ for some $0 \neq p$, α with $F = k(\alpha)$. As p and αp are k-independent, there is a k-linear map taking p to 1 and αp to $d^{1/2}$. Making the corresponding base change in the pencil, we get it spanned by $\mathrm{Tr}(xy)$ and $\mathrm{Tr}(d^{1/2}xy)$. That is, there is just one pencil with $k[X]/(f) \simeq F$. No two quadratic extensions of k split at the same completions, so the invariant for (A', B') must also be at a place with residue field F, and hence they actually span the *same* pencil.

Now suppose $n = 3$, so that we have pencils of conics. It is easiest to approach this geometrically, since (apart from degenerate cases which have probability zero) such a pencil is determined precisely by the four points in the projective plane which lie on all the conics. We first show that with probability one the Galois action on these points induces the full permutation group S_4. As before, this follows from Hilbert irreducibility provided there is some one case where the group is this large.

To construct the example, take M/k Galois with group S_4. Let E be the cubic subextension fixed by a Sylow 2-subgroup, $E(c^{1/2})$ fixed by a cyclic subgroup of order 4, and L fixed by the Klein four-group. The conjugates of c then are in different square classes in L. Let f be the minimal polynomial for a generator of E, and take a pair with invariant $\langle c\rangle$ at $k[x]/(f)$. If the four intersection points are rational over some extension K, then T is diagonalizable over K, so $K \supseteq L$. Over L it is easy to write down the pair explicitly

and compute the lines joining the points in pairs (degenerate conics in the pencil). One finds that these are individually rational only if the ratios of conjugates of c are squares. Thus $K \supseteq M_3$ and the Galois group has no subgroup of index less than 24 acting trivially on the points.

Suppose now we have a pencil where the Galois action on the intersection points $P_1, \ldots, P_4$ is S_4. Suppose the pencil with intersections $Q_1, \ldots, Q_4$ is everywhere locally equivalent. An automorphism σ acting nontrivially on the P_i will (by Chebotarev density) lie in some local Galois group and hence act nontrivially on the Q_i, and vice versa. Since S_4 has only inner automorphisms, we can match up these Galois actions. That is, after renumbering the Q_i if necessary, we will have for each σ a permutation τ with $\sigma(P_i) = P_{\tau(i)}$ and $\sigma(Q_i) = Q_{\tau(i)}$. Let ψ now be the unique projective linear map taking each P_i to Q_i. We have

$$(\sigma\psi)(\sigma P_i) = \sigma(\psi P_i) = \sigma(Q_i) = Q_{\tau(i)} = \psi P_{\tau(i)} = \psi\sigma(P_i).$$

Thus all $\sigma\psi = \psi$, so ψ is defined over k, and the pencils are equivalent over k. □

The case $n = 4$ seems related to nontrivial arithmetic problems on elliptic curves.

Appendix.

THEOREM. *Let G be a finite group. Then there is a finite Galois extension of number fields which has group G and is everywhere unramified.*

This theorem is due to Artin, and is stated as an exercise in [3, p. 80] (a reference which I owe to J. S. Hsia). Since the lemma involved is only vaguely indicated there and has other uses [7], I append here a sketch of the proof.

LEMMA. *Let k be a global field, S a finite set of places of k. For each v in S let E_v be a finite separable k_v-algebra with all $|E_v : k_v|$ equal. Then there is a field extension E/k with $E \otimes k_v \simeq E_v$ for all v in S.*

PROOF. Adding a nonarchimedean v to S if necessary, we may assume some E_v is a field. Separability implies that each E_v has only finitely many subalgebras, and the usual argument for infinite k shows it has the form $k_v[X]/(f_v)$. Choose g in $k[X]$ monic of the right degree with coefficients close in each k_v to those of f_v. If $k_v[X]/(f_v) \simeq k_v[X]/(g)$, then $E = k[X]/(g)$ is a field satisfying the conditions. For $k_v = C$ [or $k_v = R$] we need only the familiar fact that g close enough to f_v has no repeated roots [and the same number of real roots]. For nonarchimedean k_v we can scale X to assume f_v has coefficients in the valuation ring R_v. Making g close to f_v forces the generator x of $R_v[X]/(g)$ to be a root of f_v modulo a high power of the

maximal ideal of R_v. As f_v is separable and $R_v[X]/(g)$ is complete, Hensel's lemma gives an actual root y close to x. Then $X \mapsto y$ induces a map $R_v[X]/(f_v) \to R_v[X]/(g)$ which is an isomorphism by Nakayama's lemma. □

PROOF OF THEOREM. Choose L/k with group G, and let S be the places of k ramified in L. By Chebotarev density we can choose a nonarchimedean w of k split totally in L. Construct E/k with $E \otimes k_v \simeq L \otimes k_v$ for v in S and $E \otimes k_w$ an unramified field extension of k_w. In $L \cap E$ the place w splits totally (as in L) and stays prime (as in E), so $L \cap E = k$. Thus $F = EL$ is Galois over E with group G. Any place of E lying over a place v of k not in S is unramified in F, since v is unramified in L. Let u now be a place of E for which the underlying place v is in S. Choose f in $k[X]$ with splitting field L. We know $E \otimes k_v \simeq L \otimes k_v$ is a product of copies of the splitting field of f over k_v, and so f splits into linear factors in E_u. Hence u splits totally in F, and in particular u is unramified. □

REFERENCES

1. D. Hilbert, *Gesammelte Abhandlungen*, Springer, Berlin, 1933.
2. S. Lang, *Diophantine geometry*, Interscience, New York, 1962.
3. _____, *Algebraic numbers*, Addison-Wesley, Reading, Mass., 1964.
4. D. Passman, *Permutation groups*, Benjamin, New York, 1968.
5. I. Schur, *Uber die Darstellung der symmetrischen und der alternierenden Gruppe durch gebrochene lineare Substitutionen*, J. Reine Angew. Math. **139** (1911), 155–250.
6. J.-P. Serre, *Abelian l-adic representations and elliptic curves*, Benjamin, New York, 1968.
7. R. Ware, *Some remarks on the map between Witt rings of an algebraic extension*, Conference on Quadratic Forms, Queen's Papers Pure. Appl. Math. **46** (1977), 634–649.
8. W. Waterhouse, *Pairs of quadratic forms*, Invent. Math. **37** (1976), 157–164.
9. _____, *Self-adjoint operators and formally real fields*, Duke Math. J. **43** (1976), 237–243.
10. _____, *Pairs of forms and pencils of quadrics*, Conference on Quadratic Forms, Queen's Papers Pure Appl. Math. **46** (1977), 650–656.

DEPARTMENT OF MATHEMATICS, PENNSYLVANIA STATE UNIVERSITY, UNIVERSITY PARK, PENNSYLVANIA 16802