Internat. J. Math. & Math. Sci.
VOL. 11 NO. 1 (1988) 1-4

QUADRATIC SUBFIELDS OF QUARTIC EXTENSIONS OF LOCAL FIELDS

JOE REPKA

Mathematics Department
University of Toronto
Toronto, Ontario
CANADA M5S 1A1

(Received March 18, 1987)

ABSTRACT. We show that any quartic extension of a local field of odd residue characteristic must contain an intermediate field. A consequence of this is that local fields of odd residue characteristic do not have extensions with Galois group A_4 or S_4. Counterexamples are given for even residue characteristic.

KEY WORDS AND PHRASES. Local field, quartic extension, endoscopic group.
1980 AMS SUBJECT CLASSIFICATION CODES. 12B25 12B27.

Research supported by the Natural Sciences and Engineering Research Council of Canada.

1. INTRODUCTION.

In Section 2, a simple application of local class field theory proves the existence of intermediate fields for quartic extensions of local fields with odd residue characteristic. This immediately implies the non-existence of Galois extensions of type A_4 or S_4 over such fields.

In Section 3, examples are given of A_4 and S_4 extensions of fields with even residue characteristic, and of a quartic extension with no intermediate field.

In Section 4, the results of Section 2 are used to show that the splitting field of an irreducible quartic polynomial over a local field must have degree 4 or 8, provided the residue characteristic is odd. The implications of the results of Section 2 and Section 3 for the theory of endoscopic groups are also discussed.

I wish to thank Noriko Yui for helpful conversations about this work.

2. EXISTENCE OF INTERMEDIATE EXTENSIONS.

Let F be a non-archimedean local field. Let $o = o_F$ and $p = p_F$, respectively, be the ring of integers of F and its prime ideal.

THEOREM 2.1. Suppose the residue characteristic of F is odd, and E/F is a quartic extension (i.e. $[E:F] = 4$). Then there must be an intermediate field K, i.e. $E \supset K \supset F$, $[E:K] = [K:F] = 2$.

PROOF: If E/F is unramified, the result is obvious. If the ramification index of E/F is $e = 2$, then we must have $f = 2$ and, by Corollary 4 to Theorem 7 of chapter I, Section 4 of Weil [1], there is an unramified quadratic intermediate field.

Now suppose $e = 4$, so $f = 1$. Any unit in E is of the form $u + p$, with $u \in o_F^\times$ and $p \in \mathfrak{p}_E$. The norm of such an element is $u^4 + p'$, with $p' \in \mathfrak{p}_E \cap F = \mathfrak{p}_F$. So by Hensel's Lemma the only units contained in the image of $N_{E/F}$ are fourth powers. In particular, $N_{E/F}$ is not surjective, so Corollary 1 to Theorem 4 of chapter XII, Section 3 of Weil [1] proves the theorem.

Translating this into the corresponding result on Galois groups, we obtain the following equivalent formulation ...

THEOREM 2.2. If F has odd residue characteristic, there cannot be a Galois extension E/F whose Galois group is isomorphic to A_4 or S_4.

PROOF: A_4 contains subgroups of index 4 (the cyclic group generated by any 3-cycle), none of which is properly contained in any proper subgroup (such a proper subgroup, if it existed, would be of order 6 and index 2, hence normal, hence would contain all 3-cycles, of which there are 8).

An S_4-extension of F would be an A_4-extension of a quadratic extension of F.

3. COUNTEREXAMPLE FOR RESIDUE CHARACTERISTIC 2.

Let $F = \mathbb{Q}_2$ and consider the Eisenstein polynomial $\Phi(X) = X^4 - 2X - 2 \in F[X]$. Let E be the splitting field of $\Phi(X)$; we shall show that $\mathrm{Gal}(E/F) = S_4$ and $\mathrm{Gal}(E/K) = A_4$, where $K = \mathbb{Q}_2(\sqrt{3})$. In the process we shall find a quartic extension L/F with no intermediate field.

Let α be a root of $\Phi(X)$, and let $L = F(\alpha)$.

LEMMA 3.1. The norm $N_{L/F}$ is surjective.

PROOF: Notice that $N(\alpha+1) = \Phi(-1) = 1$, $N(\alpha-1) = \Phi(1) = -3$. Also the characteristic polynomial of α^3 is $\Phi_3(X) = X^4 - 6X^3 + 12X^2 - 8X - 8$, so $N(\alpha^3+1) = \Phi_3(-1) = 19$. If $N = N_{L/F}$ were not surjective, its image would be contained in the image of the norm map from some ramified quadratic extension of F. Such an image contains exactly two of the four cosets of $o^\times$ modulo $(o^\times)^2$. We have just shown $N_{L/F}$ contains the three cosets containing 1, -3, and 19.

In particular (by Corollary 1 to Theorem 4 of chapter XII, Section 3 of Weil [1]), L/F is a quartic extension with no intermediate field.

Factoring the polynomial $\Phi(X)$ over L, we see that $\Phi(X) = (X-\alpha)\Psi(X)$, where $\Psi(X) = X^3 + \alpha X^2 + \alpha^2 X + (\alpha^3-2)$.

PROPOSITION 3.2. $\Psi(X)$ is irreducible over L.

PROOF: If all roots of $\Psi(X)$ were in L, then $L = E$ would be Galois, in contradiction of Lemma 3.1. The only other way for $\Psi(X)$ to be reducible would be for exactly one root, α' say, to be in L. In this case,

$F(\alpha')$ would be a quartic extension of F contained in L, hence $F(\alpha') = F(\alpha) = L$.

Let $\sigma \in \mathrm{Gal}(E/F)$ be such that $\sigma(\alpha) = \alpha'$. Then $\sigma(F(\alpha)) = F(\alpha')$, and $\alpha' \in F(\alpha)$ implies that $\sigma(\alpha') \in F(\alpha') = F(\alpha) = L$. Since $\sigma(\alpha') \neq \alpha'$, $\sigma(\alpha')$ must equal the only other conjugate of α' in L, i.e. $\sigma(\alpha') = \alpha$. Hence the fixed field L^σ contains $\alpha + \alpha'$ and $\alpha\alpha'$, so $(X-\alpha)(X-\alpha') = X^2 - (\alpha+\alpha')X + \alpha\alpha' \in L^\sigma[X]$, which shows that α is quadratic over L^σ. So $[L:L^\sigma] = [L^\sigma:F] = 2$. This also contradicts Lemma 3.1.

So E is the splitting field of $\Psi(X)$ over L, and $\mathrm{Gal}(E/L)$ is either A_3 or S_3.

Now $\Psi(X) = X^3 + \alpha X^2 + \alpha^2 X + \alpha^3 - 2 = X'^3 + (2/3)\alpha^2 X' + (20/27)\alpha^3 - 2$, where $X' = X + 2/3$. Hence the discriminant of $\Psi(X)$ is $27((20/27)\alpha^3-2)^2 - 4((2/3)\alpha^2)^3 = 4.27 + (368/27)\alpha^6 - 80\alpha^3 \equiv 4.9.3 \bmod{}^*(1+4p_L)$.

Since $4.9(1+4p_L) \subset (L^\times)^2$, the discriminant of $\Psi(X)$ is a square in L if and only if 3 is.

LEMMA 3.3. The element 3 is not a square in L.

PROOF: If 3 were a square, truncation of its square root would give an element of the form $x = 1 + a\alpha + b\alpha^2 + c\alpha^3$, with a, b, and c each equal to 0 or 1 and so that $3 - x^2 \in 4p_L$. A trivial computation shows that this is impossible.

Accordingly $\mathrm{Gal}(E/L) = S_3$, $\mathrm{Gal}(E/F) = S_4$, and $\mathrm{Gal}(E/K) = A_4$, where $K = F(\sqrt{3})$.

4. APPLICATIONS.

1. The splitting field of a quartic polynomial over a local field is severely constrained by the results of Section 2.

THEOREM 4.1. Let F be a local field with odd residue characteristic. Let $f(X) \in F[X]$ be an irreducible polynomial with $\deg f(X) = 4$. Let E be the splitting field of $f(X)$ over F. Then $[E:F] = 4$ or 8.

PROOF: $\mathrm{Gal}(E/F)$ is a subgroup of S_4. But by Theorem 2.2 it cannot be S_4 or A_4. Since $4 \mid [E:F]$, the only possibilities are 4 or 8.

The polynomial $\Phi(X)$ of Section 3 gives a counterexample to this result when the residue characteristic is 2. Theorem 4.1 is clearly equivalent to Theorem 2.2 (and hence to Theorem 2.1).

2. If F is a local field, let $G = SL(4,F)$, and let T be an elliptic torus in G. To T is associated a quartic extension E/F so that the centralizer of T in $GL(4,F)$ is isomorphic to $E^\times$, and T itself is isomorphic to $E_1^\times = \{x \in E^\times ; N_{E/F}(x) = 1\}$.

The theory of endoscopic groups (cf. Langlands [2], Shelstad [3]) associates to G and T some other groups, among which the most interesting are constructed as follows: let $E \supsetneq K \supsetneq F$ and let $G' = \{g \in GL(2,K) : N_{K/F}(\det g) = 1\}$. In G' it is possible to find an elliptic torus T' associated to the quadratic extension E/K, and there is an isomorphism between T and T'. The hope is to simplify calculations with orbital integrals over the G-conjugacy class of $t \in T$ by comparing them with orbital integrals over the G'-conjugacy class of the corresponding $t' \in T'$.

The example of Section 3 shows that this approach will not apply for certain tori when the residue characteristic is 2; happily, for these tori the ordinary orbital integrals are invariant under stable conjugacy, so the problem does not arise. The results of Sections 2 encourage optimism in the case of odd residue characteristic.

REFERENCES

1. WEIL, A. Basic Number Theory, 3rd Edition, Springer-Verlag (New York, Heidelberg, Berlin) 1974.

2. LANGLANDS, R.P. Les Débuts d'une Formule des Traces Stable, Publ. Math. de l'Université Paris VII (1983) 188p.

3. SHELSTAD, D. Orbital integrals and a family of groups attached to a real reductive group, Ann. Scient. Ec. Norm. Sup. 12 (1979), 1-31.