CYCLOTOMIC SPLITTING FIELDS[1]

MURRAY M. SCHACHER

ABSTRACT. Suppose k is an algebraic number field and D a finite-dimensional central division algebra over k. It is well known that D has infinitely many maximal subfields which are cyclic extensions of k. From the point of view of group representations, however, the natural splitting fields are the cyclotomic ones. Accordingly it has been conjectured that D must have a cyclotomic splitting field which contains a maximal subfield. The aim of this paper is to show that the conjucture is false; we will construct a counter-example of exponent p, one for every prime p.

Throughout this paper Q will denote the field of rational numbers, and Q_p the field of p-adic numbers. If k is a number field and $\mathfrak{p}$ a valuation of k, we will write $k_\mathfrak{p}$ for the completion of k at $\mathfrak{p}$ and $D_\mathfrak{p}$ for the central simple algebra $D \otimes_k k_\mathfrak{p}$. By abuse of notation we will sometimes write $k_p(D_p)$ for $k_\mathfrak{p}(D_\mathfrak{p})$ where $\mathfrak{p}$ is a prime extending p.

Let p be a prime integer, $p \neq 2$. If ξ_p is a primitive pth root of unity over Q_p, then the field $Q_p(\xi_p)$ is cyclic and totally ramified of degree $p-1$. We construct a field k which is a cyclic extension of Q of degree p as follows:

(1) k_2 will be the cyclic unramified extension of Q_2 of dimension p.

(2) For any prime q where $q \equiv 1 \pmod p$, let $k_q =$ the unique subfield of $Q_q(\xi_q)$ of degree p. Here ξ_q denotes a primitive qth root of 1 over Q_q.

The construction of k is allowed by the Grunwald-Wang Theorem [2, Theorem 5, p. 105]. Let D be the division algebra of degree p over k defined by:

$$D_2 = D \otimes_k k_2 \quad \text{has invariant } -1/p,$$

$$D_q = D \otimes_k k_q \quad \text{has invariant } 1/p,$$

$$\operatorname{inv}(D_\mathfrak{p}) = 0 \quad \text{for } \mathfrak{p} \text{ any other prime of } k \quad (\text{see } [3, 2.1]).$$

THEOREM 1. *No maximal subfield of D can be imbedded in a cyclotomic extension of k.*

Presented to the Society, April 17, 1970 under the title *Solutions of pure equations in rational division algebras*; received by the editors November 24, 1969.

AMS Subject Classifications. Primary 1646, 1210; Secondary 1250, 1065.

Key Words and Phrases. Cyclotomic, local invariant, maximal subfield, norm, splitting field, totally ramified, valuation.

[1] The preparation of this paper was supported in part by NSF Grant #GP-13164.

PROOF. Suppose $k(\xi_m)$ is the field of mth roots of unity over k, and $L\subset k(\xi_m)$ a maximal subfield of D. Then

$$L \subset k\cdot Q(\xi_m)$$

which shows L is an abelian extension of Q of dimension p^2. There are two possibilities:

Case I. $G(L/Q) = Z_p \oplus Z_p$,
Case II. $G(L/Q) = Z_{p2}$,
where $G(L/Q)$ is the Galois group of the abelian extension L/Q.

If we are in Case I, then, since L is a splitting field of D, we must have $G(L_2/Q_2) = Z_p \oplus Z_p$. This is impossible as Q_2 has a unique cyclic extension of degree p [1, Theorem 10, p. 683]. Hence Case II applies, and L is a solution to the "extension" problem for k—a cyclic extension of dimension p^2 of Q which contains a given cyclic extension of dimension p. The solvability of such a problem depends only on k; by [2, Theorem 6, p. 106] such L exists $\Leftrightarrow$ for every primitive pth root of unity $\xi\in Q_t$ we have $\xi\in N_{k_t/Q_t}$—the local group of norms of k_t in Q_t. We will show this is false for k.

By construction k_q is a totally ramified extension of Q_q, and Q_q contains a primitive pth root of unity ξ since $q\equiv 1 \pmod p$. We claim $\xi\notin N_{k_q/Q_q}$.

If U_{Q_q}, U_{k_q} are the units of Q_q and k_q respectively, the norm map induces a homomorphism $N: U_{k_q}\to U_{Q_q}$. Those units of k (resp. Q) which are congruent to 1 modulo the maximal ideal of the integers of k_q (resp. Q_q) form a subgroup $U^1_{k_q}$ (resp. $U^1_{Q_q}$). As in [4, V, §3] we have an induced homomorphism:

$$N_0: U_{k_q}/U^1_{k_q} \to U_{Q_q}/U^1_{Q_q}. \tag{1}$$

But $U_{k_q}/U^1_{k_q}\cong \bar{k}_q^*$, the multiplicative group of the residue class field of k_q. Similarly $/U_{Q_q}U^1_{Q_q}\cong \overline{Q}_q^*$. Since k_q/Q_q is totally ramified, we have $\bar{k}_q^*\cong\overline{Q}_q^*\cong Z_q^*$. Thus (1) reduces to a homomorphism:

$$N_0: Z_q^* \to Z_q^*. \tag{2}$$

By [4, Proposition 5, p. 92] we can give an explicit formula for (2); if $x\in Z_q^*$ then $N_0(x) = x^t$, where t is the largest integer i such that the ith ramification group of $G(k_q/Q_q)$ is nonzero. The condition that k_q/Q_q is tamely ramified forces $t=0$, so finally

$$N_0: U_{k_q}/U^1_{k_q} \to U_{Q_q}/U^1_{Q_q}$$

is the trivial mapping $x\to 1$. But then N_0 does not map onto the image of ξ; it follows that ξ is not a norm. This eliminates Case II, so the theorem is established.

To find a counterexample when $p=2$ we will construct k explicitly. $L=Q(\sqrt{-1})$ and $M=Q(\sqrt{7})$. We define $k=$composite of L and M over Q. Clearly k/Q is abelian and $G(k/Q)=Z_2\oplus Z_2$. Furthermore, one easily checks that $G(k_2/Q_2)=G(k_7/Q_7)=Z_2\oplus Z_2$.

We define a quaternion D over k as follows:

$$\operatorname{inv}(D_2 = D\otimes_k k_2) = \tfrac{1}{2}, \qquad \operatorname{inv}(D_7) = \tfrac{1}{2},$$
$$\operatorname{inv}(D_{\mathfrak{p}}) = 0 \text{ for any other prime } \mathfrak{p} \text{ of } k.$$

Then

THEOREM 1′. *No maximal subfield of D can be imbedded in a cyclotomic extension of k.*

PROOF. Suppose $L\subset k(\xi_m)$ is a maximal subfield of D. Again since $L\subset Q(\xi_m)\cdot k$ we conclude L is an abelian extension of Q. Clearly $G(L/Q)$ is an abelian group of order 8. Since $G(L/Q)$ is manifestly not cyclic, there are two possibilities:

Case I. $G(L/Q) = Z_2\oplus Z_2\oplus Z_2$,
Case II. $G(L/Q) = Z_4\oplus Z_2$.

If Case I held, then the requirement that L splits D forces $G(L_7/Q_7)=Z_2\oplus Z_2\oplus Z_2$. This is impossible as Q_7 has only 3 quadratic extensions [**5**, 6-5-4]. The remaining possibility is that $G(L/Q)=Z_4\oplus Z_2$. It is easily verified that this group has precisely 3 subgroups of order 4; these must correspond to the three quadratic subfields $Q(\sqrt{-1})$, $Q(\sqrt{7})$, and $Q(\sqrt{-7})$. One of these fields must then be imbedded in a cyclic extension of Q of dimension 4. By [**2**, Theorem 6, p. 106] we conclude that -1 is a norm from one of these three fields. This is clearly impossible for the two imaginary fields, and by [**5**, 6-3-2] the fundamental unit in $Q(\sqrt{7})$ has norm one. Therefore no such extension L exists.

Algebras like the ones constructed above were studied by Albert in [**1**]. He used them to construct the following: a division algebra D of dimension n^2 over its center k so that there is no cyclic extension L of Q of degree n with Lk a splitting field of D. The algebras in Theorems 1 and 1′ have this property. It was pointed out to me by Burton Fein, who suggested the orginal problem, that the conjecture is true in case the dimension of k/Q is prime to the exponent of D. The following argument, which is his, was noted essentially by Albert in [**1**].

THEOREM 2. *Suppose k is an algebraic number field with* $[k:Q]=n$ *and D a central division algebra over k of exponent m. Assume* $(m, n)=1$. *Then D has infinitely many cyclic maximal subfields which are contained in cyclotomic extensions of k.*

PROOF. By the Grunwald-Wang Theorem we construct L an m-dimensional cyclic extension of Q satisfying

L_p/Q_p is cyclic of degree m whenever $D_{\mathfrak{p}} = D \otimes_k k_{\mathfrak{p}}$ is not a split algebra and $\mathfrak{p} \mid P$.

Since $(m, n) = 1$ we have $L \cdot k$ an m-dimensional cyclic extension of k, and by construction $L \cdot k$ is a splitting field of k. It follows that $L \cdot k$ is a maximal subfield of D. By [2, Theorem 6, p. 74] $L \subset Q(\xi_r)$ for some primitive rth root of unity ξ_r. Then $L \cdot k \subset k(\xi_r)$, and $L \cdot k$ is the desired maximal subfield of D. As there are infinitely many choices for L we can construct infinitely many nonisomorphic $L \cdot k$.

REFERENCES

1. A. A. Albert, *On p-adic fields and rational division algebras*, Ann. of Math. (2) **41** (1940), 674–693. MR **2**, 123.
2. E. Artin and J. Tate, *Class field theory*, Benjamin, New York, 1968. MR **36** #6383.
3. M. Schacher, *Subfields of division rings*. I, J. Algebra **9** (1968), 451–477. MR **37** #2809.
4. J. P. Serre, *Corps locaux*, Actualités Sci. Indust., no. 1296, Hermann, Paris, 1962. MR **27** #133.
5. E. Weiss, *Algebraic number theory*, McGraw-Hill, New York, 1963. MR **28** #3021.

UNIVERSITY OF CALIFORNIA, LOS ANGELES, CALIFORNIA 90024