PACIFIC JOURNAL OF MATHEMATICS
Vol. 45, No. 2, 1973

MAXIMAL SUBFIELDS OF TENSOR PRODUCTS

BURTON FEIN AND MURRAY SCHACHER

Let D_1 and D_2 be finite-dimensional division rings with center K such that $D_1 \otimes_K D_2$ is a division ring. If L_1 and L_2 are maximal subfields of D_1 and D_2, respectively, then clearly $L_1 \otimes_K L_2$ is a maximal subfield of $D_1 \otimes_K D_2$. In this note the converse question is considered: does there exist a maximal subfield L of $D_1 \otimes_K D_2$ which is not isomorphic to $L_1 \otimes_K L_2$ for maximal subfields L_1 and L_2 of D_1 and D_2? Examples are given to show that such noncomposite L may fail to exist even when K is a local field. For K an algebraic number field, however, it is shown that infinitely many noncomposite L always exist.

We say that a division algebra with center a field K is a *K-division ring* if it is finite-dimensional over K. Throughout this note D_1 and D_2 will denote K-division rings such that $D_1 \otimes_K D_2$ is a K-division ring. We say that a maximal subfield L of $D_1 \otimes_K D_2$ is a *composite* if $L \cong L_1 \otimes_K L_2$ where L_1 and L_2 are maximal subfields of D_1 and D_2, respectively.

A sufficient condition for $D_1 \otimes_K D_2$ to be a division ring is for $([D_1: K], [D_2: K]) = 1$ [2, Theorem 10, p. 52]. This condition is necessary if K is either an algebraic number field or a local field since for these K the exponent of a K-division ring equals its index [2, Theorem 25, p. 144, and Theorem 32, p. 149]. This condition is not, however, necessary for K arbitrary, as is shown in [1]. We begin by determining, for the case when $([D_1: K], [D_2: K]) = 1$ necessary and sufficient conditions for a maximal subfield of $D_1 \otimes_K D_2$ to be a composite.

THEOREM 1. *Let D_1 and D_2 be K-division rings such that $([D_1: K], [D_2: K]) = 1$, and let L be a maximal subfield of $D_1 \otimes_K D_2$. Then L is a composite if and only if L has subfields L_1 and L_2 with $[L_1: K]^2 = [D_1: K]$ and $[L_2: K]^2 = [D_2: K]$.*

Proof. Let $n_i = [D_i: K]^{1/2}$, $i = 1, 2$. If L_i is a maximal subfield of D_i then $[L_i: K] = n_i$, $i = 1, 2$. It follows that if $L = L_1 \otimes_K L_2$ is a composite with L_i a maximal subfield of D_i, then $[L_i: K] = n_i$, $i = 1, 2$. This establishes one direction of the Theorem.

Suppose now that L has subfields L_1 and L_2 with $[L_i: K] = n_i$, $i = 1, 2$. Since L is a maximal subfield of $D_1 \otimes_K D_2$ we have $[L: K] = n_1 n_2$. As $(n_1, n_2) = 1$, it follows that $L \cong L_1 \otimes_K L_2$. Thus to conclude L is a composite we need only show that L_i splits D_i,

$i = 1, 2$ [2, Theorem 27, p. 61]. We have $(D_1 \otimes_K D_2) \otimes_K L \cong [(D_1 \otimes_K L_1) \otimes_{L_1} L] \otimes_L [(D_2 \otimes_K L_1) \otimes_{L_1} L]$. Since L splits $D_1 \otimes_K D_2$, $(D_1 \otimes_K L_1) \otimes_{L_1} L = A_1$ is in the class of the opposite algebra of $A_2 = (D_2 \otimes_K L_1) \otimes_{L_1} L$ in the Brauer group of L. In particular, these algebras have the same exponent. Since $(n_1, n_2) = 1$ and the exponent of A_i divides n_i, it follows that A_1 and A_2 are complete matrix algebras. Thus L splits $D_1 \otimes_K L_1$. Since n_1 is prime to $[L: L_1] = n_2$, L_1 splits D_1. Similarly, L_2 splits D_2, proving the proposition.

COROLLARY 2. *Let D_1 and D_2 be K-division rings such that $([D_1: K], [D_2: K]) = 1$ and let L be a maximal subfield of $D_1 \otimes_K D_2$. If L is Galois over K with solvable Galois group, then L is a composite. In particular, if K is a local field and L is Galois over K, then L is a composite.*

Proof. Take G_i to be a Hall subgroup of order $[D_i: K]^{1/2}$ of the Galois group of L over K. Let L_1 and L_2 be the fixed fields of G_2 and G_1, respectively. Then $L \cong L_1 \otimes_K L_2$, and L is composite by Theorem 1. The final assertion of the corollary follows from the result that Galois groups over local fields are solvable [6, Proposition 3.6.6, p. 101].

Corollary 2 is false without the restriction that L have a solvable Galois group. By [5, Theorem 9.1, p. 472] there is a field K, a K-division ring D, and a maximal subfield L of D such that L is a Galois extension of K with group A_5. By [2, Theorem 18, p. 77], $D \cong D_1 \otimes_K D_2$ where D_1 and D_2 are K-division rings with D_1 of index 20 and D_2 of index 3. However, L clearly has no subfield L_2 with $[L_2: K] = 3$, since A_5 has no subgroup of order 20.

Theorem 1 is false without the assumption that $([D_1: K], [D_2: K]) = 1$. In [1] an example is presented of two quaternion algebras D_1 and D_2 central over a field K such that $D_1 \otimes_K D_2$ is a cyclic division algebra. If L is a maximal subfield of $D_1 \otimes_K D_2$ with $L \mid K$ cyclic, then L contains a subfield of degree two over K but is not a composite as composites would have Galois group $Z_2 \times Z_2$.

While one might expect that there should always exist maximal subfields of $D_1 \otimes_K D_2$ which are not composites, this is not the case even when K is a local field. Our next result treats the case when K is local and $[D_1 \otimes_K D_2: K]^{1/2}$ is a product of two primes. The general case may be expected to be much more complicated.

THEOREM 3. *Let p and r be distinct primes, $p < r$, and let K be a local field with residue class field $GF(q)$ where $p \nmid q$, $r \nmid q$. Let D_1 and D_2 be K-division rings of indices p and r respectively. If either $p \nmid r - 1$ or $q \equiv 1 \pmod{pr}$, then every maximal subfield of*

$D_1 \otimes_K D_2$ is a composite. If $p \mid r-1$ there are infinitely many primes q and Q_q-division rings D_1 and D_2 (where Q_q is the q-adic field) of indices p and r, respectively, having maximal subfields which are not composites.

Proof. Suppose $p \nmid r-1$ or $q \equiv 1 \pmod{pr}$. Let L be a maximal subfield of $D_1 \otimes_K D_2$. Then $[L: K] = pr$. Since $p \nmid q$, $r \nmid q$, L is tamely ramified over K. L will have subfields of degrees p and r over K if L is either unramified or totally ramified over K. From Corollary 2 we also see that L will be a composite if L is Galois over K. Let e and f be, respectively, the ramification and residue class degrees of L over K. Thus $ef = pr$ and we may assume that $e > 1$ and $f > 1$. If $q \equiv 1 \pmod{e}$ then L is normal over K [3, Theorem 6, p. 680]. Thus L is a composite if $q \equiv 1 \pmod{pr}$, so we assume that $p \nmid r-1$ and $e \nmid q-1$. By [3, Theorem 2, p. 678], we may assume that $L = K(\zeta, \alpha)$, where ζ is a primitive (q^f-1)th root of unity, $\alpha^e = \zeta^i \pi$, i is an integer, and π is a prime element of K. Let $q^f - 1 = (q-1)t$. If e divided t, then $q^f \equiv 1 \pmod{e}$. But $(f, e-1) = 1$ since $p \nmid r-1$ and $p < r$. Thus $q \equiv 1 \pmod{e}$, against our assumption. Thus $(e, t) = 1$ so there is an integer j with $jt \equiv i \pmod{e}$. Let β be any root of $x^e - \zeta^{jt}\pi$ in an algebraic closure of K. Then $K(\zeta, \beta)$ is isomorphic to L by [3, Theorem 3, p. 679]. But $\zeta^t \in K$ since K contains all $(q-1)$th roots of unity, so $[K(\beta): K] = e$. Thus L has a subfield isomorphic to $K(\beta)$ which is of degree e over K. Since L also contains an unramified extension of degree f over K, Theorem 1 shows L is a composite.

Now suppose $p \mid r-1$. Let b be an integer, $b \not\equiv 1 \pmod{r}$, $b^p \equiv 1 \pmod{r}$. Take q a prime, $q \equiv b \pmod{r}$. There are infinitely many such q by Dirichlet's theorem. If $q^p - 1 = (q-1)t$, then r divides t. Let D_1 and D_2 be Q_q-division rings of indices p and r respectively. Let ζ be a primitive (q^p-1)th root of unity and let $\alpha^r = \zeta q$. Since $[Q_q(\zeta, \alpha): Q_q] = pr$, $Q_q(\zeta, \alpha)$ is a maximal subfield of $D_1 \otimes_K D_2$ [2, Theorem 23, p. 144]. If $Q_q(\zeta, \alpha)$ were a composite, it would have a subfield E with $[E: Q_q] = r$. E would be totally and tamely ramified over Q_q, and so $E \cong Q_q(\beta)$ where $\beta^r = \zeta^{ti} q$ for some integer j. Thus $Q_q(\zeta, \alpha) \cong Q_q(\zeta, \beta)$ so $1 \equiv jt \pmod{d}$ where $d = (r, q^p - 1)$ by [3, Theorem 3, p. 678]. Since $d = r$, we have $jt \equiv 1 \pmod{r}$. But $r \mid t$, a contradiction.

We remark that there are other examples where every maximal subfield of $D_1 \otimes_K D_2$ is a composite. In [4] an example is constructed of a field K and two quaternions D_1 and D_2 over K such that every maximal subfield of $D_1 \otimes_K D_2$ (which is a division ring) is a composite.

Our final result shows that over number fields it is never the

case that every maximal subfield of a tensor product is a composite. We use freely the classification of rational division algebras by means of Hasse invariants [2, Chapter 9].

THEOREM 4. *Let K be an algebraic number field, D_1 and D_2 K-division rings such that $D_1 \otimes_K D_2$ is a division ring. Then there are infinitely many maximal subfields of $D_1 \otimes_K D_2$ which are not composites.*

Proof. Suppose that $[D_1: K] = n^2$, $[D_2: K] = m^2$ and $m < n$. Let $[\mathfrak{P}_1, \cdots, \mathfrak{P}_m\}$ be the set of finite primes of K for which the Hasse invariants of $D_1 \otimes_K D_2$ are nonzero. Let $\mathfrak{P}$ be a finite prime of K, $\mathfrak{P} \notin \{\mathfrak{P}_1, \cdots, \mathfrak{P}_m\}$. Let K_i be the completion of K at $\mathfrak{P}_i$, $K_{\mathfrak{P}}$ the completion of K at $\mathfrak{P}$. Let $K_i(\alpha_i)$ have degree mn over K_i and $K_{\mathfrak{P}}(\alpha)$ have degree n over $K_{\mathfrak{P}}$. We write $f_i(x)$ for the monic minimal polynomial of α_i over K_i and $f(x)$ for the monic minimal polynomial of α over $K_{\mathfrak{P}}$. Let $g(x)$ be monic in $K[x]$ of degree nm "sufficiently close" to $f_i(x)$ in the $\mathfrak{P}_i$-topology, $i = 1, \cdots, m$, and "sufficiently close" to $(x-1)^{nm-n}f(x)$ in the $\mathfrak{P}$-topology. If nm is even, take $g(x)$ also "sufficiently close" to $(x^2+1)^{mn/2}$ at all infinite primes of K. Here "sufficiently close" means close enough to guarantee

(1) $g(x)$ is irreducible over K

(2) For any root β of $g(x)$, the field $L = K(\beta)$ has local degree nm at $\mathfrak{P}_i$, $i = 1, \cdots, m$, and $\mathfrak{P}$ splits into $n(m-1)$ primes of degree one and one prime of degree n in L.

(3) If nm is even, L is totally imaginary.

This is possible by [6, Ex. 3.2, p. 116].

It follows from the theory of Hasse invariants that L splits $D_1 \otimes_K D_2$. Since $[L: K] = nm$, L is a maximal subfield of $D_1 \otimes_K D_2$. Suppose there were a field E, $L \supset E \supset K$, $[E: K] = n$. If π is a prime of E dividing $\mathfrak{P}$ of degree greater than one, then π must remain irreducible in L since otherwise L would have two primes of degree >1 dividing $\mathfrak{P}$. But then if γ is the prime of L extending π, the local degree of γ over $\mathfrak{P}$ is divisible by $[L: E] = m$. Thus m would divide n which is not the case since $D_1 \otimes_K D_2$ is a division ring. This shows that $\mathfrak{P}$ splits completely in E. But then the local degree of any prime of L dividing $\mathfrak{P}$ is at most $[L: E] = m < n$. This proves that E can not exist and so L is not a composite. Since there are infinitely many choices for $\mathfrak{P}$, there are infinitely many such L.

REFERENCES

1. A. A. Albert, *A note on cyclic algebras of order* 16, Bull. Amer. Math. Soc., **37** (1931), 727-30.
2. ———, *Structure of algebras*, Amer. Math. Soc. Colloq. Publ., **24**, Amer. Math. Soc., Providence, R.I., 1939.
3. ———, *On p-adic fields and rational division algebras*, Ann. Math., **41** (1940), 674-693.
4. S. Amitsur, *On central division algebras*, to appear Israel J. Math., **12** (1972), 408-421.
5. M. Schacher, *Subfields of division rings*, I, J. of Algebra, **9** (1968), 451-477.
6. E. Weiss, *Algebraic number theory*, McGraw-Hill, New York, 1963.

Received November 11, 1971. This research was supported in part by National Science Foundation grants GP-29068 and GP-28696.

OREGON STATE UNIVERSITY
AND
UNIVERSITY OF CALIFORNIA, LOS ANGELES