

EMBEDDING RATIONAL DIVISION ALGEBRAS¹

BURTON FEIN

ABSTRACT. Necessary and sufficient conditions are given for two K -division rings, K an algebraic number field, to have precisely the same set of subfields. Using this, an example is presented of two K -division rings having precisely the same set of subfields such that only one of the division rings can be embedded in a Q -division ring.

Let K be a field. By a K -division ring we mean a finite-dimensional division algebra with center K . If D is a K -division ring and k is a field, $k \subset K$, we say that D is k -adequate if D can be embedded in a k -division ring. Similarly, if L is a field, we say that L is k -adequate if L is a subfield of some k -division ring. Clearly, if D is k -adequate then so is every subfield of D . In [4] the converse was raised: if every subfield of D is k -adequate, must D be k -adequate? We show that the answer to this question is no by exhibiting two K -division rings D_1 and D_2 having precisely the same set of subfields and such that D_1 is k -adequate (and so every subfield of D_2 is also k -adequate) but D_2 is not k -adequate.

Throughout this paper K will denote an algebraic number field. We will use freely the classification theory of K -division algebras by means of Hasse invariants. The reader is referred to [3] for the relevant theory. If \mathcal{P} is a prime of K and D is a K -division ring, we denote the Hasse invariant of D at \mathcal{P} by $\text{inv}_{\mathcal{P}} D$. The order of $\text{inv}_{\mathcal{P}} D$ in Q/Z is denoted by $\text{l.i.}_{\mathcal{P}} D$. Here Q denotes the field of rational numbers and Z is the ring of ordinary integers. We denote the completion of K at the prime \mathcal{P} by $K_{\mathcal{P}}$. The dimension of D over K is denoted by $[D:K]$; we use the same notation for the dimension of field extensions.

We begin by establishing criteria for two K -division rings to have precisely the same set of subfields.

THEOREM 1. *Let D_1 and D_2 be K -division rings. Then D_1 and D_2 have precisely the same set of subfields if and only if $\text{l.i.}_{\mathcal{P}} D_1 = \text{l.i.}_{\mathcal{P}} D_2$ for all primes \mathcal{P} of K .*

Received by the editors July 19, 1971.

AMS 1970 subject classifications. Primary 16A40; Secondary 12A65.

Key words and phrases. Rational division algebra, Hasse invariant, Grünwald-Wang theorem.

¹ The preparation of this paper was supported in part by NSF Grant GP-29068.

PROOF. Suppose D_1 and D_2 have precisely the same set of subfields but for some prime \mathcal{P} of K we have $\text{l.i.}_{\mathcal{P}} D_1 = n > m = \text{l.i.}_{\mathcal{P}} D_2$. Using the Grünwald-Wang theorem [2, Theorem 5, p. 105] we can construct a cyclic extension L of K of degree $[D_2:K]^{1/2}$ such that L is a splitting field for D_2 and such that the local degree of L over K at \mathcal{P} equals m . It follows that L is a subfield of D_2 [1, Theorem 27, p. 61] and so L is a subfield of D_1 . Since D_1 and D_2 have the same maximal subfields, L is a maximal subfield of D_1 . But then n divides m , the local degree of L over K at \mathcal{P} by [4, (0.1), p. 413]. This establishes the result in one direction. Conversely, suppose $\text{l.i.}_{\mathcal{P}} D_1 = \text{l.i.}_{\mathcal{P}} D_2$ for all primes \mathcal{P} of K . We need only check that D_1 and D_2 have the same set of maximal subfields. Let L be a maximal subfield of D_1 . Then $\text{l.i.}_{\mathcal{P}} D_1$ divides $[L_{\mathcal{Y}}:K_{\mathcal{P}}]$ for every prime \mathcal{Y} of L extending \mathcal{P} (see (0.1) of [4]). Thus L also splits D_2 .

Since the index of D_1 equals the least common multiple of $\{\text{l.i.}_{\mathcal{P}} D_1\}$, it follows that $[D_1:K] = [D_2:K]$ and so L is a maximal subfield of D_2 . This proves the theorem.

COROLLARY 2. *Let D_1 and D_2 be quaternion algebras over K . Then $D_1 \cong D_2$ if and only if D_1 and D_2 have precisely the same set of subfields.*

PROOF. Since D_i is quaternion, $\text{l.i.}_{\mathcal{P}} D_i = 1$ or 2 . Thus $\text{l.i.}_{\mathcal{P}} D_1 = \text{l.i.}_{\mathcal{P}} D_2$ implies $\text{inv}_{\mathcal{P}} D_1 = \text{inv}_{\mathcal{P}} D_2$ and the result now follows from [3, Satz 8, p. 119].

The following result is implicit in [4].

PROPOSITION 3. *Let K be a normal extension of k and let D be a K -division ring. Suppose there is a prime \mathcal{P} of k such that $\text{inv}_{\mathcal{Y}_1} D \neq \text{inv}_{\mathcal{Y}_2} D$ for two primes \mathcal{Y}_1 and \mathcal{Y}_2 of K extending \mathcal{P} . Then D is not k -adequate.*

PROOF. Suppose $D \subset D_0$, D_0 a k -division ring. As in the proof of [4, Theorem 1, p. 415], we have $\text{Cent}_{D_0}(K) \cong D \otimes_K D'$, where $\text{Cent}_{D_0}(K)$ is the centralizer of K in D_0 and D' is a K -division ring. By Lemma 1 of [4], $\text{Cent}_{D_0}(K) \sim D_0 \otimes_k K$. Since $K|k$ is normal, $[K_{\mathcal{Y}_1}:k_{\mathcal{P}}] = [K_{\mathcal{Y}_2}:k_{\mathcal{P}}]$. Thus $\text{inv}_{\mathcal{Y}_1} \text{Cent}_{D_0}(K) = \text{inv}_{\mathcal{Y}_2} \text{Cent}_{D_0}(K)$. This yields $\text{inv}_{\mathcal{Y}_1} D' - \text{inv}_{\mathcal{Y}_2} D' \equiv \text{inv}_{\mathcal{Y}_2} D - \text{inv}_{\mathcal{Y}_1} D \not\equiv 0 \pmod{1}$. We conclude that for $i = 1$ or 2 , there is a prime q dividing $\text{l.i.}_{\mathcal{Y}_i} D'$ such that q also divides $\text{l.i.}_{\mathcal{Y}_j} D$ for some j . This contradicts (0.4) of [4].

We can now exhibit our example.

EXAMPLE. Let K be a cyclic extension of Q of degree 5 and let p be a prime of Q splitting completely in K . Let r, s , and t be primes of Q that remain prime in K . Such primes exist (see [2, Chapter 5, Theorem 3]). Let D_1 be the K -division ring having $\text{inv}_r D_1 = \frac{1}{5}$, $\text{inv}_s D_1 = \frac{4}{5}$, $\text{inv}_{\mathcal{P}} D_1 = \frac{1}{5}$ for all primes \mathcal{P} of K extending p , and $\text{inv}_{\mathcal{P}} D_1 = 0$ for all other primes \mathcal{P}

of K . Let D be the Q -division ring with $\text{inv}_p D = \frac{1}{5}$, $\text{inv}_r D = \frac{1}{25}$, $\text{inv}_s D = \frac{2}{25}$, $\text{inv}_t D = \frac{4}{5}$, and $\text{inv}_q D = 0$ for all other primes q of Q . These division algebras exist by [3, Satz 9, p. 119]. Let L be a cyclic extension of K of degree 5 having local degree 5 at all primes of K extending p , r , and s . The existence of L is guaranteed by the Grünwald-Wang theorem. Since $[D:Q]^{1/2} = 25 = [L:Q]$, L is a maximal subfield of D by (0.1) of [4]. Thus $K \subset D$. Let $\text{Cent}_D(K)$ be the centralizer of K in D . This is a K -division ring by the double centralizer theorem and has the same invariants as D_1 by [4, Lemma 1, p. 413]. Thus $\text{Cent}_D(K) \cong D_1$ so D_1 is Q -adequate. Let D_2 be the K -division ring having $\text{inv}_r D_2 = \frac{1}{5}$, $\text{inv}_s D_2 = \frac{4}{5}$, $\text{inv}_{p_1} D_2 = \frac{1}{5}$, $\text{inv}_{p_2} D_2 = \frac{3}{5}$, $\text{inv}_{p_3} D_2 = \text{inv}_{p_4} D_2 = \text{inv}_{p_5} D_2 = \frac{2}{5}$, where p_1, p_2, p_3, p_4 , and p_5 are the primes of K extending p , and $\text{inv}_{\mathcal{P}} D_2 = 0$ for all other primes \mathcal{P} of K . By Theorem 1, D_1 and D_2 have precisely the same set of subfields. Proposition 3 shows that D_2 is not Q -adequate.

We note that the above argument can be generalized so as to yield two K -division rings D_1 and D_2 having the same subfields with only one of D_1 or D_2 being k -adequate whenever K is a cyclic extension of k of prime power degree p^r with $p^r > 2$.

REFERENCES

1. A. A. Albert, *Structure of algebras*, Amer. Math. Soc. Colloq. Publ., vol. 24, Amer. Math. Soc., Providence, R.I., 1939. MR 1, 99.
2. E. Artin and J. Tate, *Class field theory*, Harvard Univ. Press, Cambridge, Mass., 1961. (Cf. MR 36 #6383.)
3. M. Deuring, *Algebren*, Ergebnisse der Mathematik und ihrer Grenzgebiete, Band 41, Springer-Verlag, New York, 1968. MR 37 #4106.
4. B. Fein and M. Schacher, *Embedding finite groups in rational division algebras. I*, J. Algebra 17 (1971), 412-428.

DEPARTMENT OF MATHEMATICS, OREGON STATE UNIVERSITY, CORVALLIS, OREGON 97331