PROCEEDINGS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 60, October 1976

THE ORDINARY QUATERNIONS OVER A PYTHAGOREAN FIELD[1]

BURTON FEIN AND MURRAY SCHACHER

ABSTRACT. Let L be a proper finite Galois extension of a field K and let D be a division algebra with center K. If every subfield of D properly containing K contains a K-isomorphic copy of L, it is shown that K must be Pythagorean, $L \cong K(\sqrt{-1})$, and D is the ordinary quaternions over K. If one assumes only that every maximal subfield of D contains a K isomorphic copy of L, then, under the assumption that $[D : K]$ is finite, it is shown that K is Pythagorean, $L = K(\sqrt{-1})$, and D contains the ordinary quaternions over K.

Let K be a field and L a finite-dimensional Galois extension of K. Suppose D is a division algebra with center K having the property that every maximal subfield of D contains a K-isomorphic copy of L. We ask what can be concluded about D, K, and L. In [1] Herstein considered the case where L is quadratic over K; he concluded then that K is Pythagorean, $L = K(\sqrt{-1})$, and $D \supset Q_K$, the ordinary quaternion algebra over K. A Pythagorean field is a field which is formally real in which every sum of squares is a square. The ordinary quaternion algebra Q_K is the K algebra $K + Ki + Kj + Kk$ subject to the relations: $i^2 = j^2 = k^2 = -1$, $ij = -ji = k, jk = -kj = i$, $ki = -ik = j$.

In this paper we prove the following two theorems, both of which should be viewed as generalizations of [1].

THEOREM 1. *Let L be a proper finite Galois extension of K and let D be a division algebra with center K, $Q \neq K$. Suppose that every subfield of D properly containing K contains a K-isomorphic copy of L. Then K is Pythagorean, $L = K(\sqrt{-1})$, and D is the ordinary quaternion algebra Q_K.*

THEOREM 2. *Let L be a proper finite Galois extension of K and let D be a finite-dimensional division algebra with center K, $D \neq K$. Suppose that every maximal subfield of D contains a K-isomorphic copy of L. Then K is Pythagorean, $L = K(\sqrt{-1})$, and D contains the ordinary quaternions over K.*

Before proving these results we need a lemma which is presumably well known, but for which we have not been able to find a convenient reference.

Received by the editors October 13, 1975.

AMS (MOS) subject classifications (1970). Primary 16A40.

Key words and phrases. Division algebra, Pythagorean field.

[1]The work of the first author was supported in part by NSF Grant MPS71-02969 while the work of the second author was supported by NSF Grant MPS71-2884. During much of this work the second author was a research fellow at the University of Pisa. He would like to thank the Italian National Research Council (CNR) for their support.

LEMMA 1. *Let K be a field. Then K is Pythagorean if and only if Q_K is a division algebra and every maximal subfield of Q_K is K-isomorphic to $K(\sqrt{-1})$.*

Suppose K is Pythagorean. Then Q_K is a division algebra since -1 is not a sum of two squares in K. Let $K(\sqrt{t})$ be a maximal subfield of Q_K. Then $K(\sqrt{t})$ splits Q_K and so -1 is a sum of two squares in $K(\sqrt{t})$. Thus $-1 = (a + b\sqrt{t})^2$ where $a, b, c, d, t \in K$, $\sqrt{t} \notin K$. Expanding and using the Pythagorean property of K we have $-1 = u^2 + u^2 t$, $u, v \in K$. Thus $t = -w^2$, $w \in K$, so $K(\sqrt{t}) = K(\sqrt{-1})$ as desired. Conversely, assume Q_K is a division algebra having, up to isomorphism, a unique maximal subfield. Let $t \in K$. Then since

$$-1 = -1 - t^2 + t^2 = \left(\sqrt{-(1 + t^2)}\right)^2 + t^2,$$

$K(\sqrt{-(1 + t^2)})$ splits Q_K. Thus $K(\sqrt{-(1 + t^2)})$ is a maximal subfield of Q_K and so $K(\sqrt{-(1 + t^2)}) = K(\sqrt{-1})$. This implies that $1 + t^2$ is a square in K for all $t \in K$. Thus if u, v are nonzero elements of K then $u^2 + v^2 = u^2(1 + v^2/u^2)$ is a square in K. It follows that K must be Pythagorean since Q_K is a division algebra.

We now turn to the theorems.

PROOF OF THEOREM 1. Since every subfield of D containing K contains a K-isomorphic copy of L, we must have $[L : K] = p$, a prime. Let $\alpha \in D$ such that $K(\alpha)$ is K-isomorphic to L and let σ generate the Galois group of $K(\alpha)$ over K. By the Skolem-Noether theorem [2, Theorem 4.3.1, p. 99], there is a $\delta \in D$ such that $\delta^{-1}\alpha\delta = \sigma(\alpha)$. Since $L \neq K$, $\sigma(\alpha) \neq \alpha$. We write $\operatorname{Irr}(\alpha, K)$ for the irreducible polynomial of α over K. Since $[K(\alpha) : K] = p$, δ^p commutes with α. If $\delta^p \notin K$, then $K(\delta^p)$ contains a K-isomorphic copy of L and so $\operatorname{Irr}(\alpha, K)$ splits into linear factors in $K(\delta^p)$. Since $K(\alpha, \delta^p)$ is a field and α is a root of $\operatorname{Irr}(\alpha, K)$ in $K(\alpha, \delta^p)$ we must have $\alpha \in K(\delta^p)$. But $K(\delta^p) \subset K(\delta)$ so $\alpha \in K(\delta)$ and $\delta^{-1}\alpha\delta = \alpha$, a contradiction. Thus $\delta^p \in K$. Let $D_0 = \{\sum_{i=0}^{p-1} a_i\delta^i \mid a_i \in K(\alpha)\}$. Then $D_0 \subset D$ and D_0 is K-isomorphic to the cyclic algebra $(K(\alpha)/K, \sigma, \delta^p)$.

Let $C_D(D_0)$ denote the centralizer in D of D_0. By [2, Theorem 4.4.2, p. 112], $D \cong D_0 \otimes_K C_D(D_0)$. If $C_D(D_0) \neq K$, then $C_D(D_0)$ is a nontrivial division ring. Let E be a maximal subfield of $C_D(D_0)$. Then E contains a K-isomorphic copy of L and so $D \supset K(\alpha) \otimes_K L$. Since $K(\alpha) \cong L$, $D \supset L \otimes_K L$. This is a contradiction since $L \otimes_K L$ has zero divisors. Thus $C_D(D_0) = K$ and so $D = D_0$. We have established that $[D : K] = p^2$ and $D = (K(\alpha)/K, \sigma, \delta^p)$. In particular, $K(\delta)$ is a maximal subfield of D and so $K(\delta) \cong L$. Since $\delta^p \in K$, the characteristic of K cannot be p. Since $K(\delta)$ is a Galois extension of K of degree p and $\delta^p \in K$, K must contain a primitive pth root of unity. Also, $\operatorname{Irr}(\delta, K) = x^p - \delta^p$. Since $K(\alpha)$ is K-isomorphic to $K(\delta)$, some element of $K(\alpha)$ is a root of $\operatorname{Irr}(\delta, K)$. We clearly may assume that this element is α and so $\alpha^p = \delta^p$. Since $\delta^{-1}\alpha\delta \in K(\alpha)$ and $\delta^{-1}\alpha\delta$ is a root of $\operatorname{Irr}(\alpha, K)$, we must have $\delta^{-1}\alpha\delta = \zeta\alpha$ where ζ is a primitive pth root of unity in K. An easy induction proves that $(\alpha\delta^{-1})^n = \zeta^{n(n-1)/2}\alpha^n\delta^{-n}$ for

$n \geqslant 1$. If p is odd, then $\zeta^{p(p-1)/2} = 1$ and so $(\alpha\delta^{-1})^p = \alpha^p\delta^{-p} = 1$. Since K contains all pth roots of unity, $\alpha\delta^{-1} \in K$ and so $\alpha\delta = \delta\alpha$. This is a contradiction and so $p = 2$. In this case we have $(\alpha\delta^{-1})^2 = -\alpha^2\delta^{-2} = -1$. Since $\alpha\delta^{-1} \notin K$, $K(\sqrt{-1})$ is a subfield of D and so $L \cong K(\sqrt{-1})$. Without loss of generality we may assume that $\alpha^2 = -1$ and so $\delta^2 = -1$. Since $(\alpha\delta^{-1})^2 = -1$, $\alpha\delta^{-1} = -\delta^{-1}\alpha$ and so D is the ordinary quaternions over K. Finally, since all maximal subfields of D are K-isomorphic to $L \cong K(\sqrt{-1})$, K is Pythagorean by the lemma. This proves Theorem 1.

Proof of Theorem 2. If every subfield of D properly containing K contains a K-isomorphic copy of L, we are finished by Theorem 1. Assume that E is a subfield of D, E, properly containing K, and E is maximal with respect to not containing a K-isomorphic copy of L. E exists because $[D : K]$ is finite. Then $C_D(E)$ satisfies the hypotheses of Theorem 1 and so E is Pythagorean, $EL = E(\sqrt{-1})$, and $C_D(E)$ is the ordinary quaternions over E, $C_D(E) = Q_E$. Since $Q_E \cong Q_Q \otimes_Q E$, $Q_E \supset Q_Q \otimes_Q K = Q_k$ and so $D \supset Q_K$. K is formally real since E is. Suppose $L \ncong K(\sqrt{-1})$. Then take F a subfield of D, $F \supset K(\sqrt{-1})$, F maximal with respect to not containing a K-isomorphic copy of L. Then $C_D(F)$ satisfies the hypotheses of Theorem 1 so $C_D(F) = Q_F$. But $\sqrt{-1} \in F$ so Q_F has zero divisors. Thus $C_D(F)$ has zero divisors, a contradiction. It follows that $L \cong K(\sqrt{-1})$. Finally, we must show that K is Pythagorean. In view of the results already obtained and the lemma, we need only show that every maximal subfield of Q_K is K-isomorphic to $K(\sqrt{-1})$. Let V be a maximal subfield of Q_K. If $V \ncong K(\sqrt{-1})$ we may take W a subfield of D, $W \supset V$, W maximal with respect to $\sqrt{-1} \notin W$. Since $L \cong K(\sqrt{-1})$ $C_D(W)$ satisfies the hypotheses of Theorem 1 so $C_D(W) = Q_W$. But $W \supset V$ and V splits Q_K so Q_W has zero divisors. This contradiction completes the proof of Theorem 2.

The following corollary is immediate from Theorem 1.

Corollary 3. *Let D be a division algebra finite dimensional over its center K. If all maximal subfields of D are Galois over K and are K-isomorphic, then K is Pythagorean and D is the ordinary quaternions over K.*

There are some natural questions open to generalization concerning the results above. Among these the most tantalizing seem to be:

(1) Can the assumption of normality of L in Theorems 1 and 2 be eliminated?

(2) Can the assumption of finite-dimensionality be eliminated from Theorem 2?

References

1. I. N. Herstein, *On a theorem of Albert*, Scripta Math. **29** (1972), 391–394.

2. ———, *Noncommutative rings*, Carus Math. Monographs, vol. 15, Math. Assoc. Amer., distributed by Wiley, New York, 1968. MR **37** #2790.

Department of Mathematics, Oregon State University, Corvallis, Oregon 97331

Department of Mathematics, University of California, Los Angeles, California 90024