CHARACTERIZING THE MULTIPLICATIVE GROUP
OF A REAL CLOSED FIELD IN TERMS OF ITS
DIVISIBLE MAXIMAL SUBGROUP

M. MAHDAVI-HEZAVEHI

Communicated by Jamshid Moori

Abstract. Let $F$ be a field and $M$ be a maximal subgroup of the
multiplicative group $F^* = F \setminus \{0\}$ of index $p$. It is proved that
if $M$ is divisible, then $Br(F)_p \neq 0$ if and only if $p = 2$ and $F$ is
Euclidean. Furthermore, it is shown that in this case $F^*$ contains
a divisible maximal subgroup if and only if $F^*$ is isomorphic to the
multiplicative group of a real closed field.

1. Introduction

Given the field of real numbers $\mathbb{R}$, denote by $\mathbb{R}^+$ and $\mathbb{R}^+$
the multiplicative group of real numbers and the multiplicative group of positive
real numbers, respectively. We recall that a nontrivial multiplicative
abelian group $G$ is divisible if and only if $G$ has no maximal subgroup
if and only if $G = G^p$ for each prime $p$. It is easily seen that $\mathbb{R}^+$ is a
divisible maximal subgroup of index 2 in $\mathbb{R}^+$ and $\mathbb{R}$ is Euclidean. The
object of this note is to show that this property on the multiplicative
group of a field $F$ implies that $Br(F)_p \neq 0$ if and only if $p = 2$ and $F$
is Euclidean, where $Br(F)_p$ is the $p$-primary component of the Brauer
group of $F$. Furthermore, if $R$ is a real closed field, then it is easily seen

MSC(2000): Primary: 12J15, 16K40; secondary: 16K50
Keywords: Maximal, divisible subgroup.
Received: 15 July 2008. Accepted: 3 September 2008
*Corresponding author
© 2009 Iranian Mathematical Society.
that (cf. Theorem A below) \( R^* \) contains a unique maximal subgroup which is divisible. Here, we also characterize the multiplicative group of a real closed field in terms of its divisible maximal subgroup. To be more precise, it is proved that \( F^* \) contains a divisible maximal subgroup if and only if \( F^* \) is isomorphic to the multiplicative group of a real closed field.

2. Divisible maximal subgroups

We begin our investigation with the following easy lemma.

Lemma 2.1. Let \( G \) be a multiplicative abelian group and \( M \) be a maximal subgroup of \( G \). If \( M \) is divisible, then \( M \) is the unique maximal subgroup of \( G \).

Proof. Assume that \( M_1 \neq M \) is another maximal subgroup of \( G \). Then, we have \( G = MM_1 \) and hence \( G/M_1 \cong M/M \cap M_1 \); i.e., \( M \cap M_1 \) is a maximal subgroup of \( M \). Since \( M \) is divisible, then we conclude that \( M \cap M_1 = 1 \). Therefore, \( G/M_1 \cong M \cong C_q \) for some prime number \( q \), where \( C_q \) is the cyclic group of \( q \) elements. This last relation also leads to a contradiction since a finite group cannot be divisible, and so \( M = M_1 \) as required.

We shall also need the following theorem to prove our main result.

Theorem A ([1], p. 107) If \( F \) is a real closed field, then \( F^* \cong \mathbb{Z}_2 \times \mathbb{Q}^{|F|} \). Conversely, for any infinite cardinal \( \lambda \), the group \( \mathbb{Z}_2 \times \mathbb{Q}^\lambda \) is isomorphic to the multiplicative group of a suitable real closed field.

Theorem 2.2. Let \( M \) be a maximal subgroup of \( F^* \) of index \( p \). Then, we have:
(1) If \( M \) is divisible, then \( Br(F)_p \neq 0 \) if and only if \( p = 2 \) and \( F \) is Euclidean.
(2) If \( F \) is Euclidean, then \( F^* \) contains a divisible maximal subgroup of index 2 if and only if \( F^* \) is isomorphic to the multiplicative group of a real closed field.

Proof. (1) Assume that \( M \) is a maximal subgroup of \( F^* \) with \( F^* / M \cong C_p \) for some prime \( p \). We first claim that if \( p \) is odd, then there exists
a unique cyclic field extension $K/F$ of degree $p$ such that $N(K^*) = F^*$, where $N$ is the norm of $K$ to $F$. To see this, we know, by Lemma 2.1 that $M$ is the unique maximal subgroup of $F^*$ such that $F^*/M \cong C_p$. Since $M$ is divisible and maximal in $F^*$, then by (4.1.4) of [3], we have $F^* \cong M \times C_p$. This means that $F$ contains a primitive $p$-th root of unity. Now, it is easily seen that there is an element $a \in F$ such that the equation $x^p - a = 0$ has no solutions in $F$. Since $F$ has a primitive $p$-th root of unity, then we obtain a cyclic extension $K = F(b)$ of degree $p$ over $F$ with $b^p - a = 0$. By Kummer theory and the Prüfer-Baer Theorem (cf. [3], p. 105), the Galois group $Gal(K/F)$ is isomorphic with a subgroup of $F^*/F^{*p} \cong C_p$. Therefore, $K/F$ is the only cyclic extension of degree $p$ over $F$; i.e., we may take $a = \omega$ a primitive $p$-th root of unity. Since $p$ is odd, then we have $N(b) = (-1)^{p+1}\omega = \omega$. Furthermore, because $M$ is divisible, then we obtain $M = M^p \subset N(K^*)$ and hence $N(K^*) = F^*$, as claimed. Now, assume that $Gal(K/F)$ is generated by the automorphism $\sigma$ of order $p = [K : F]$. Fix an element $\lambda \in F^*$ and a symbol $y$. We set $D = K1 \oplus Ky \oplus \cdots \oplus Ky^{p-1}$, and multiply elements of $D$ by using distributive law, and the rules $y^p = \lambda$, $yk = \sigma(k)y$ for all $k \in K$. This way, we obtain the cyclic algebra $(K/F, \sigma, \lambda)$. Now, since $F^* = N(K^*)$, then we conclude that $\lambda \in N(K^*)$. Thus, by Corollary 4 of [2], p. 82, $[D]$ is trivial in $Br(F)$. If $Br(F)_p \neq 0$, then there is an $F$-central simple algebra, say $A$, such that $[A] \neq 0$ with $p[A] = 0$. By Theorem 1 of [2], p. 119, $[A] = \oplus[C_i]$, where $C_i$ is a cyclic algebra of index $p$. From the above argument, we know that $[C_i] = 0$ for each $i$. Thus, $[A] = 0$ which is a contradiction. Thus, we must have $p = 2$. Now, we have $F^* \cong M \times C_2$, which shows that $-1 \notin M$. The equation $x^2 + 1 = 0$ over $F$ has no root in $F$, since $a^2 = -1$ with $a \in F$ implies that $-1 \in M$, which is false. Now, consider the extension $L = F(i)$ with $i^2 = -1$. The above proof shows that $N_{L/F}(L^*) = M$. We claim that $M$ defines a positive cone for $F$. It is clear that $M \cap -M = \emptyset$, $MM \subseteq M$, and $M \cup -M \cup \{0\} = F$. To show that $M + M \subseteq M$, take $\alpha, \beta \in M$. Since $M = F^{*2}$, then there exist $\lambda, \mu \in F^*$ such that $\alpha = \lambda^2, \beta = \mu^2$. Now, consider the element $x = \lambda + \mu i \in L$. We have $N_{L/F}(x) = \lambda^2 + \mu^2 = \alpha + \beta \in M$, since $N(L^*) = M$. Therefore, $F$ is formally real and since $M = F^{*2}$, then we conclude that $F$ is Euclidean. On the other hand, since $F$ is Euclidean, then take the quaternion algebra $Q$ over $F$. Because $-1$ is not a sum of squares, then we conclude that $Q$ is a division algebra and hence $Br(F)_2 \neq 0$. 
(2) One way is clear from Theorem A. If $M$ is the divisible maximal subgroup of $F^*$, then from the proof of (1) we have $F^* \cong M \times C_2$. Since $M$ is divisible from the theory of divisible abelian groups we know that $M$ is a direct product of quasi-cyclic and full rational groups (cf. [1], p. 96). We claim that $M$ contains no primitive $p$-th root of unity. Since $-1$ is not in $M$, then it suffices to consider $p > 2$. If $\omega$ is a primitive $p$-th root of unity, then for $p \neq 2$ we have $1^2 + \omega^2 + \cdots + \omega^{2(p-1)} = (\omega^{2p} - 1)/(\omega^2 - 1) = 0$, which is not possible in a formally real field (by (1)). Thus, we cannot have any copy of a quasi-cyclic group in our decomposition of $M$ and hence $M \cong \mathbb{Q}^\lambda$ for some cardinal $\lambda$. Since $\mathbb{Q}$ is of torsion-free rank 1, $\lambda$ is the torsion-free rank of $F^*$. Now, because $\text{Char} F = 0$, then we have $\mathbb{Q}^\times \subset F^*$, and hence $\lambda$ is infinite by Lemma 4.1.16 of [1], which asserts that $\mathbb{Q}^\times \cong \mathbb{Z}_2 \times \mathbb{Z}^\kappa$. Therefore, we have $M \cong \mathbb{Q}^\lambda$ for some infinite cardinal $\lambda$. Now, by Theorem A, we obtain the result.

We observe that in the conclusion of the theorem, $F$ need not necessarily be real closed. In fact, if $F$ is obtained from the rationals $\mathbb{Q}$ by iteratively adjoining roots of positive real algebraic numbers, then the positive cone of the resulting field $F$ is such a maximal subgroup. But $F$ is not real closed.

Acknowledgments

The author thanks the Research Council of Sharif University of Technology for support. Also, he wishes to thank M.G. Mahmudi and M. Motiee for a useful discussion on the proof of the main theorem.

References


M. Mahdavi-Hezavehi
Department of Mathematical Sciences, Sharif University of Technology, P.O. Box 11365-9415, Tehran, Iran.
Email: mahdavih@sharif.edu