J. Austral. Math. Soc. (Series A) 26 (1978), 26–30

A NOTE ON THE CHARACTERIZATION OF CM-FIELDS

P. E. BLANKSBY and J. H. LOXTON

Dedicated to Kurt Mahler on his 75th birthday

(Received 16 January 1978)

Communicated by J. H. Coates

Abstract

This note deals with some properties of algebraic number fields generated by numbers having all their conjugates on a circle. In particular, it is shown that an algebraic number field is a CM-field if and only if it is generated over the rationals by an element (not equal to ± 1) whose conjugates all lie on the unit circle.

Subject classification (Amer. Math. Soc. (MOS) 1970): 12 A 15, 12 A 40, 14 K 22.

1. Introduction

An interesting and important class of fields which arise in algebraic number theory and elsewhere are the so-called fields of complex multiplication, or CM-fields for short. These are defined as follows.

DEFINITION. *An algebraic number field is called a CM-field if it is a totally imaginary quadratic extension of a totally real algebraic number field.* (Here, an algebraic number field is a subfield of **C** which is also a finite extension of **Q**. As usual, **Q** and **C** denote the fields of rational and complex numbers respectively.)

The set of totally real fields and CM-fields go collectively under the designation J-fields (Gold (1974)), or almost real fields (Grossman (1976)).

CM-fields have a number of interesting characterizations. (See, for example, Shimura (1971), Győry (1975), Parry (1975).) In particular, the following proposition is well known and may be used as an alternative definition.

PROPOSITION. *A non-real algebraic number field K is a CM-field if and only if K is closed under the operation of complex conjugation and complex conjugation commutes with all the* **Q**-*monomorphisms of K into* **C**.

The aim of this paper is to add a further simple characterization of CM-fields which does not seem to have been exploited elsewhere.

The following piece of notation will be useful. If θ is an algebraic number of degree n, we denote the conjugates of θ by $\theta = \theta_1, \theta_2, \ldots, \theta_n$ and we write

$$\lceil\theta\rceil = \max_{1 \leqslant j \leqslant n} |\theta_j|.$$

THEOREM 1. *A necessary and sufficient condition that an algebraic number field be a CM-field is that it be generated over the rationals by an element* $\theta\,(\neq \pm 1)$ *for which* $\lceil\theta\rceil = 1$.

COROLLARY. *A necessary and sufficient condition that an algebraic number field be totally real is that it be generated over the rationals by an element of the form* $\theta + \bar{\theta}$ *where* $\lceil\theta\rceil = 1$.

Note that $\lceil\theta\rceil = 1$ implies θ is reciprocal and so $|\theta_j| = 1$ for $j = 1, 2, \ldots, n$. In the case that there exists such a generator θ which is an algebraic integer, then θ is a root of unity by a classical theorem of Kronecker, and so $\mathbf{Q}(\theta)$ is a cyclotomic field. The θ with $\lceil\theta\rceil = 1$ have a simple characterization. (See Ennola and Smyth (1974), Theorem 3.)

The necessity of the condition in Theorem 1 will be an immediate consequence of the following.

THEOREM 2. *A necessary and sufficient condition that a non-real algebraic number field be closed under the operation of complex conjugation is that it be generated over the rationals by an element* α *with* $|\alpha| = 1$.

2. Proof of Theorem 1

The sufficiency of the condition follows from the Proposition, since $\bar{\theta} = \theta^{-1}$ and $\theta \neq \pm 1$ imply that $K = \mathbf{Q}(\theta)$ is a non-real field which is closed under complex conjugation; and since $|\theta_j| = 1$ $(1 \leqslant j \leqslant n)$, we have for all **Q**-monomorphisms σ of K into **C**

$$\sigma(\bar{\theta}) = \sigma(\theta^{-1}) = \{\sigma(\theta)\}^{-1} = \overline{\sigma(\theta)},$$

$\sigma(\theta)$ being some conjugate of θ.

The necessity follows from Theorem 2, for if α is a member of a CM-field, then $|\alpha| = 1$ is equivalent to $\lceil\alpha\rceil = 1$.

https://doi.org/10.1017/S1446788700011460 Published online by Cambridge University Press

3. Proof of Theorem 2

The sufficiency of the condition is clear since $\alpha^{-1} = \bar{\alpha}$.

To prove the necessity, suppose $K = \mathbf{Q}(\beta)$. Then $\beta \neq \bar{\beta}$ and, since $K = \bar{K}$, we know $\bar{\beta}$ is in K. For r in $\mathbf{Q}$, define

$$\gamma_r = \frac{\beta + r}{\bar{\beta} + r},$$

and let σ_j $(1 \leqslant j \leqslant n)$ be the $\mathbf{Q}$-monomorphisms of $\mathbf{K}$ into $\mathbf{C}$. (Here, n is the degree of β and we take σ_1 to be the identity.) The field conjugates of γ_r are the

$$\sigma_j(\gamma_r) = \frac{\sigma_j(\beta) + r}{\sigma_j(\bar{\beta}) + r} \quad (1 \leqslant j \leqslant n).$$

We aim to show that for some r in $\mathbf{Q}$, γ_r generates K over $\mathbf{Q}$, and so, to the contrary, let us suppose that the degree of γ_r is strictly less than n for all r in $\mathbf{Q}$. Then there are distinct numbers r and s in $\mathbf{Q}$ and an integer t with $1 < t \leqslant n$ such that $\gamma_s = \sigma_t(\gamma_s)$ and $\gamma_r = \sigma_t(\gamma_r)$. That is

$$\frac{\beta + s}{\bar{\beta} + s} = \frac{\sigma_t(\beta) + s}{\sigma_t(\bar{\beta}) + s}, \quad \frac{\beta + r}{\bar{\beta} + r} = \frac{\sigma_t(\beta) + r}{\sigma_t(\bar{\beta}) + r}.$$

Now, by considering the generator $\beta + s$ in place of β, we may suppose $s = 0$. Thus, if we write $\delta = \sigma_t(\beta)$ and $\bar{\varepsilon} = \sigma_t(\bar{\beta})$, we have

$$\frac{\beta}{\bar{\beta}} = \frac{\delta}{\bar{\varepsilon}}, \quad \frac{\beta + r}{\bar{\beta} + r} = \frac{\delta + r}{\bar{\varepsilon} + r}.$$

Since $r \neq 0$, we deduce from these equations that

$$\beta - \bar{\beta} = \delta - \bar{\varepsilon} = (\bar{\varepsilon}/\bar{\beta})(\beta - \bar{\beta}).$$

But $\beta \neq \bar{\beta}$ so $\bar{\beta} = \bar{\varepsilon}$, whence $\beta = \delta$. This yields $\sigma_t(\beta) = \beta$, contradicting that $t > 1$. Thus there exists a number r such that γ_r has degree n, and since $|\gamma_r| = 1$, we may take $\alpha = \gamma_r$ and the necessity of the theorem is established.

4. Additional remarks

(a) Suppose that $\theta = \theta_1, \theta_2, \ldots, \theta_n$ are the conjugates of θ, and that

(1) $$|\theta_j|^2 = R \quad (1 \leqslant j \leqslant n).$$

Write $K = \mathbf{Q}(\theta)$ and let L be the normal closure of K in $\mathbf{C}$. We will dispense with the case $n = 2$ with the comment that K is totally real if θ is real and K is a CM-field if θ is not real.

https://doi.org/10.1017/S1446788700011460 Published online by Cambridge University Press

Suppose now that $n>2$. If σ is any $\mathbf{Q}$-automorphism of L, then since R is in L,

$$\sigma(R) = \sigma(\theta\bar{\theta}) = \sigma(\theta)\,\sigma(\bar{\theta}) = \frac{\sigma(\bar{\theta})}{\overline{\sigma(\theta)}}.R.$$

Thus $\sigma(R) = R$ if and only if $\sigma(\bar{\theta}) = \overline{\sigma(\theta)}$. Since θ has at least one non-real conjugate, we deduce that when θ satisfies (1) and $n>2$, then $\mathbf{Q}(\theta)$ is a CM-field if and only if R is in $\mathbf{Q}$.

(b) In general, when θ satisfies (1), we have $R^{\frac{1}{2}n}$ in $\mathbf{Q}$. Let k be the least positive integer such that R^k is in $\mathbf{Q}$ and write $K_1 = \mathbf{Q}(\theta^k)$. Since $|\theta_j^k|^2$ is in $\mathbf{Q}$, we deduce as in (a) that either K_1 is a real quadratic extension of $\mathbf{Q}$ or K_1 is a CM-field. Now $K = K_1(\theta)$ is a pure root extension of K_1. The conjugates of θ over K_1 are of the form $\theta\zeta$ where $\zeta^k = 1$. If $[K: K_1] = d$ so that $d \leqslant k$, then $N_{K/K_1}\theta$ is an element of K_1 with all its conjugates on the circle $|z|^2 = R^d$, and since K_1 is CM or real quadratic, we deduce that R^d is in $\mathbf{Q}$ and so $d = k$. Thus K is a pure root extension of K_1 of degree k.

(c) More generally again, suppose (1) is replaced by

$$|\theta_j - \gamma|^2 = R \quad (1 \leqslant j \leqslant n), \tag{2}$$

where as before we need only consider $n>2$. Then γ is real, and indeed γ is in L. (For if $\theta_1, \bar{\theta}_1, \theta_2$, say, are distinct conjugates then $|\theta_1 - \gamma| = |\theta_2 - \gamma|$ implies that γ is in $\mathbf{Q}(\theta_1, \bar{\theta}_1, \theta_2, \bar{\theta}_2) \subseteq L$.)

Suppose that $K = \mathbf{Q}(\theta)$ is a CM-field and let σ be any $\mathbf{Q}$-automorphism of L. Then

$$\sigma(R) = (\sigma(\theta_j) - \sigma(\gamma))(\sigma(\bar{\theta}_j) - \sigma(\gamma)) = |\sigma(\theta_j) - \sigma(\gamma)|^2.$$

Thus the $\sigma(\theta_j)$ $(1 \leqslant j \leqslant n)$, that is the θ_i $(1 \leqslant i \leqslant n)$, lie on the circle $|z - \sigma(\gamma)|^2 = \sigma(R)$. Since $n>2$, we deduce that $\sigma(\gamma) = \gamma$ and $\sigma(R) = R$. This holds for all σ, so γ and R are in $\mathbf{Q}$. Conversely, if γ and R are in $\mathbf{Q}$, then K is a CM-field. So when θ satisfies (2) and $n>2$, then $\mathbf{Q}(\theta)$ is a CM-field if and only if γ and R are in $\mathbf{Q}$.

References

V. Ennola and C. J. Smyth (1974), "Conjugate algebraic numbers on a circle", *Annales Acad. Scientiarum Fennicae, Ser. A* **582**, 1–31.

R. Gold (1974), "The non-triviality of certain Z_l-extensions", *J. Number Theory* **6**, 369–373.

E. H. Grossman (1976), "On the solutions of diophantine equations in units", *Acta Arith.* **30**, 137–143.

K. Györy (1975), "Sur une classe des corps de nombres algébriques et ses applications", *Publ. Math. Debrecen* **22**, 151–175.

C. J. Parry (1975), "Units of algebraic number fields", *J. Number Theory* **7**, 385–388.
G. Shimura (1971), *Introduction to the Arithmetic Theory of Automorphic Functions*, Publications of the Math. Soc. Japan **11** (Princeton University Press).

Department of Pure Mathematics
The University of Adelaide
Adelaide
South Australia 5001

School of Mathematics
University of New South Wales
Kensington
New South Wales 2033