Bull. Aust. Math. Soc. **96** (2017), 398–399
doi:10.1017/S0004972717000661

CM FIELDS WITHOUT UNIT-PRIMITIVE ELEMENTS

CORNELIUS GREITHER✉ and TOUFIK ZAÏMI

(Received 15 May 2017; accepted 7 June 2017; first published online 20 September 2017)

Abstract

This is an addendum to a recent paper by Zaïmi, Bertin and Aljouiee ['On number fields without a unit primitive element', *Bull. Aust. Math. Soc.* **93** (2016), 420–432], giving the answer to a question asked in that paper, together with some historical connections.

2010 *Mathematics subject classification*: primary 11R27; secondary 12F05.

Keywords and phrases: primitive elements, units, CM fields.

This note is an addendum to the recent paper [2] by Zaïmi, Bertin and Aljouiee. Recall that a number field K is said to admit a unit primitive element (UPE) if there exists a unit $\theta \in \mathcal{O}_K^*$ such that $K = \mathbb{Q}(\theta)$. (Here, as usual, $\mathcal{O}_K^*$ is the group of units in the ring $\mathcal{O}_K$ of integers of K.) Recall also that every non-CM field admits a UPE. The following question (labelled 1.8) was asked in [2]: Given any totally real field R, does there exist a CM field K (or even infinitely many such fields) which has no UPE and for which R is equal to K^+, the maximal totally real subfield of K?

It has turned out that the answer is not too hard to find. We will give it here, and then we will tell the underlying story. The answer is given in the following theorem.

Theorem 1. *For every totally real field R there are infinitely many CM extensions K/R with $R = K^+$, without a unit primitive element.*

This positive answer to the question will follow from the two separate statements (A) and (B) below. The letter R will always denote a totally real number field.

(A) *For any given R, there exist infinitely many CM extensions K/R with $K^+ = R$.*

(B) *For any given R, the number of such CM extensions K/R admitting a UPE is finite.*

Proof of Theorem 1. (A) This is very easy to see; it suffices to consider $K = R(\sqrt{-p})$ for primes p that do not divide the discriminant of R, and so cannot ramify in $R/\mathbb{Q}$.

(B) The proof of (B) is not too difficult either. Look at the case where the number m of roots of unity in K is strictly larger than 2. If we let ζ_m denote a primitive mth root of unity, then $K = R(\zeta_m)$ and $\varphi(m) \leq [K : \mathbb{Q}] = 2[R : \mathbb{Q}]$. As there are only finitely many m satisfying this inequality, there are only finitely many fields K of this kind. Therefore, we may assume from now on that $m = 2$. This means that the unit index $Q = [O_K^* : \Omega_K O_R^*]$ equals $[O_K^* : O_R^*]$, where Ω_K denotes the group of roots of unity in K; on the other hand it is well known that $Q = 1$ or $Q = 2$. If $Q = 1$, then obviously K has no UPE. If $Q = 2$, then K arises from R by adjoining the square root of a unit of R. This adjunction only depends on the class of this unit modulo squares, and since O_R^* is finitely generated by Dirichlet's theorem, the number of such extensions K/R is finite. □

Now for the story. The argument given above is a synthesis of three (closely related) arguments: one by Zaïmi, one by C. Greither (found while writing a review of [2] for *Mathematical Reviews*), and, last but not least, one by Robert Remak in [1]. The existence of the latter argument was discovered and communicated to Marie José Bertin by W. Narkiewicz after Zaïmi had found his proof. (To be accurate, Remak proved (B) only, but (A) is very easy.) It is remarkable that Remak's argument is contained in his last article, which appeared in 1954. Even more remarkably and sadly, this article was published posthumously more than 10 years after Remak's disappearance and presumed death in Auschwitz. That paper is connected with two other famous mathematicians: after the galley proofs were lost in the war, it was reconstructed from Remak's shorthand by van der Waerden's wife, and the review in *Mathematical Reviews* was written by Kenkichi Iwasawa.

Acknowledgement

We thank Marie José Bertin for her kind and helpful correspondence, and we hope that these short remarks fulfil their double purpose: explaining the fairly straightforward solution of Question 1.8 in [2] and honouring Remak's memory.

References

[1] R. Remak, 'Über algebraische Zahlkörper mit schwachem Einheitsdefekt', *Compositio Math.* **12** (1954), 35–80.

[2] T. Zaïmi, M. J. Bertin and A. M. Aljouiee, 'On number fields without a unit primitive element', *Bull. Aust. Math. Soc.* **93** (2016), 420–432.

CORNELIUS GREITHER, Institut für Theoretische Informatik und Mathematik,
Universität der Bundeswehr, München, 85577 Neubiberg,
Germany
e-mail: cornelius.greither@unibw.de

TOUFIK ZAÏMI, Department of Mathematics and Statistics, College of Science,
Al Imam Mohammad Ibn Saud Islamic University (IMSIU),
PO Box 90950, Riyadh 11623, Saudi Arabia
e-mail: tmzaemi@imamu.edu.sa