Algebraic Integers on the Unit Circle

Ryan C. Daileda

March 22, 2005

Department of Mathematics, 6188 Bradley Hall, Dartmouth College, Hanover, NH 03755-3551

Abstract

By computing the rank of the group of unimodular units in a given number field, we provide a simple proof of the classification of the number fields containing algebraic integers of modulus 1 that are not roots of unity.

For a number field K, let V_K denote the set of algebraic integers in K of modulus 1. Such numbers are necessarily units in K: if $u \in K$ is integral and $|u| = 1$, then $\overline{u} = u^{-1}$ is also an integral element of K. Therefore V_K is a subgroup of the unit group U_K of K. Since U_K is a finitely generated abelian group, so too is V_K. According to Dirichlet's unit theorem, the rank of U_K is determined in a simple way by the signature of K, and one is led to wonder whether there is an equally simple way to determine the rank of V_K. In this note we show that this is indeed the case.

A natural question to ask is when V_K properly contains the group W_K of roots of unity in K. That is, when does K contain algebraic integers of modulus 1 that are not roots of unity? In 1975, MacCluer and Parry [2] partially answered this question by proving that if K is a Galois extension of $\mathbb{Q}$ then $W_K \neq V_K$ if and only if K is imaginary and not a CM-field (defined below). That same year Parry [3] extended this result, with slightly more complicated hypotheses, to all number fields. It turns out that both of these results are easy consequences of our computation of the rank of V_K, and we are thus able to provide dramatically simplified proofs.

In addition to the notation already established, let $R_K = U_K \cap \mathbb{R}$ denote the group of real units in K. We will find it convenient to omit the subscripts from our notation when there is no risk of confusion. Our main observation is the following.

Theorem 1. *Let K be a number field closed under complex conjugation, and let U, V and R be as above. Then*

$$\operatorname{rank} V + \operatorname{rank} R = \operatorname{rank} U.$$

Proof. By hypothesis, if $u \in U$, then $\bar{u} \in U$ as well. Therefore, $u\bar{u} = |u|^2 \in R$ and $u/\bar{u} \in V$. This means that

$$u^2 = |u|^2 \frac{u}{\bar{u}} \in RV. \tag{1}$$

Hence $U^2 \subset RV \subset U$, so that $\operatorname{rank} U = \operatorname{rank} U^2 = \operatorname{rank}(RV)$. It is clear that $R \cap V = \{\pm 1\}$, giving $\operatorname{rank} RV = \operatorname{rank} R + \operatorname{rank} V$, so we're done. □

The decomposition of equation (1) already appears in [1], but is utilized only in the case $V = W$. We also note that an imaginary number field K is closed under complex conjugation if and only if it is of degree 2 over its maximal real subfield, a condition which appears as a hypothesis in [1].

Corollary 1. *Let K be a number field closed under complex conjugation. Let $F = K \cap \mathbb{R}$ be the maximal real subfield of K. Then*

$$\operatorname{rank} V_K = \operatorname{rank} U_K - \operatorname{rank} U_F.$$

Proof. Since $U_F = U_K \cap \mathbb{R} = R_K$, this follows immediately from the theorem. □

A number field K contains unimodular units that are not roots of unity precisely when $W \neq V$. Since the torsion part of V is W, we will have $W \neq V$ if and only if $\operatorname{rank} V > 0$. Corollary 1 can therefore be restated as follows.

Corollary 2. *Let K be a number field, closed under complex conjugation, and let $F = K \cap \mathbb{R}$. Then K contains unimodular units that are not roots of unity if and only if* $\operatorname{rank} U_K > \operatorname{rank} U_F$.

Let F be any proper subfield of the number field K. If we denote by $r(L)$ and $s(L)$ the number of real and complex places (resp.) of the number field L, then $\operatorname{rank} U_F = \operatorname{rank} U_K$ if and only if

$$\begin{aligned} r(K) + s(K) &= r(F) + s(F), \\ r(K) + 2s(K) &= [K\colon F](r(F) + 2s(F)). \end{aligned}$$

It is easy to show that these equations are simultaneously satisfied if and only if $[K\colon F] = 2$, $r(K) = s(F) = 0$ and $r(F) = s(K)$ (see [3]). In this case, K is said to be a CM-field. Combining this observation with Corollary 2, we obtain the next result.

Theorem 2. *Let K be a number field closed under complex conjugation. Then K contains unimodular units that are not roots of unity if and only if K is imaginary and not a CM-field.*

Since every Galois extension of $\mathbb{Q}$ is closed under complex conjugation, we have recovered MacCluer's and Parry's result. Turning now to the general case, let $\overline{K}$ denote the image of K under complex conjugation.

Theorem 3. *Let K be a number field and $L = K \cap \overline{K}$. Then K contains unimodular units that are not roots of unity if and only if L is imaginary and not a CM-field.*

Proof. Note that $V_K = V_L$, since if $u \in K$ has modulus 1 then $u = \overline{1/u} \in \overline{K}$, so that $u \in L$. Therefore, K will contain unimodular units that are not roots of unity if and only if L does. Since L is closed under complex conjugation, Theorem 2 finishes the proof. □

This is essentially Parry's classification. However, the statement of Theorem 3 differs from Parry's Corollary 2 of (the correction to) [3] in that it makes explicit the nature of the field L.

Acknowledgements

I would like to thank Carl Pomerance for his helpful comments and suggestions, and Bill Duke for bringing the reference [2] to my attention.

References

[1] P. Dénes, Über Einheiten von algebraischen Zahlkörpern (German), Monatsh. Math. **55** (1951), 161-163

[2] C. R. MacCluer, C. J. Parry, Units of Modulus 1, J. Number Theory **7** (4) (1975), 371-375

[3] C. J. Parry, Units of Algebraic Number Fields, J. Number Theory **7** (4) (1975), 385-388; corr. **9** (2) (1977), 278