CLASS GROUPS, TOTALLY POSITIVE UNITS, AND SQUARES

H. M. EDGAR, R. A. MOLLIN\(^1\) AND B. L. PETERSON

Abstract. Given a totally real algebraic number field \(K\), we investigate when totally positive units, \(U^+_K\), are squares, \(U^2_K\). In particular, we prove that the rank of \(U^+_K/U^2_K\) is bounded above by the minimum of (1) the 2-rank of the narrow class group of \(K\) and (2) the rank of \(U^+_L/U^2_L\) as \(L\) ranges over all (finite) totally real extension fields of \(K\). Several applications are also provided.

1. Notation and preliminaries. Let \(K\) be an algebraic number field and let \(C_K\) denote the ideal class group in the ordinary or “wide” sense. Let \(C_K^{(+)}\) denote the “narrow” ideal class group of \(K\). Thus \(|C_K| = h_K\), the “wide” class number of \(K\), and \(|C_K^{(+)}| = h_K^{(+)}\), the “narrow” class number of \(K\). We denote the Hilbert class field of \(K\) by \(K^{(1)}\); i.e., \(\text{Gal}(K^{(1)}/K) \cong C_K\), and we denote the “narrow” Hilbert class field by \(K^{(+)}\); i.e., \(\text{Gal}(K^{(+)}/K) \cong C_K^{(+)}\). Moreover we adopt the “bar” convention to mean “modulo squares”; for example, \(\bar{C}_K = C_K/C_K^2\).

Let \(U_K\) denote the group of units of the ring of algebraic integers of \(K\). When \(K\) is totally real, we let \(U^+_K\) denote the subgroup of totally positive units; i.e., those units \(u\) such that \(u^a > 0\) for all embeddings \(\sigma\) of \(K\) into \(\mathbb{R}\). Finally, for any finite abelian group \(A\) with \(|A| = 2^d\), \(d\) is called the 2-rank of \(A\), which we denote by \(\dim_2 A\).

2. Results. We are concerned with the question:

\(\ast\) When is \(U^+_K = U^2_K\)?

We begin by observing that \(\dim_2(\bar{U}^+_K) = 0\) if and only if \(K^{(+)} = K^{(1)}\) [6, Theorem 3.1, p. 203]. In particular, when \(K\) is a real finite Galois extension of 2-power degree over \(Q\), then \(\dim_2(\bar{U}^+_K) = 0\) if and only if \(N(U_K) = \{ \pm 1\}\) [3, Theorem 1, p. 166]. For example, when \(K\) is a real quadratic field, then \(\dim_2(\bar{U}^+_K) = 0\) if and only if the norm of the fundamental unit is \(-1\). Necessary and sufficient conditions (in terms of the arithmetic of the underlying quadratic field \(K\)) for the existence of a fundamental unit of norm \(-1\) are unknown (see [8]). This indicates the difficulty of solving \(\ast\) for the simplest even degree case. In this regard one may ask whether \(\ast\) is equivalent to such a norm statement for other fields. In a recent letter to the authors, V. Ennola answered \(\ast\) for cyclic cubic fields \(K\) as follows: Let \(\varepsilon\) be a norm positive unit of \(K\) such that \(-1\) and the conjugates of \(\varepsilon\) generate the unit group. Then \(\dim_2(\bar{U}^+_K) = 0\) if and only if \(\varepsilon\) is not totally positive. However, as with

---

\(\ast\) This author’s research is supported by N.S.E.R.C. Canada.

©1986 American Mathematical Society

0002-9939/86 $1.00 + $.25 per page
the quadratic field case, the latter does not readily translate into arithmetic conditions on the underlying cyclic cubic field $K$. We have not been able to verify that such a norm condition holds for a larger class of fields. For example, it would be interesting to investigate this question for quartic fields. However, we do have the following result which gives an upper bound on $\tilde{U}_K^+$ in terms of $\tilde{U}_L^+$ for a totally real extension field $L$ of $K$. For example, this will allow us to translate the norm criterion from a quadratic field to any of its totally real number field extensions. We note that the following generalizes [3, Theorem 2, p. 168].

**Theorem 2.1.** Suppose $Q \subseteq K \subseteq L$ with $L$ totally real and finite over $Q$. Then $\dim_2 \tilde{U}_K^+ \leq \dim_2 \tilde{U}_L^+$.

**Proof.** First we show that $K^{(1)} \subseteq L^{(1)}$ and $K^{(+)} \subseteq L^{(+)}$. Both $K^{(1)}L/L$ and $K^{(+)}L/L$ are Galois extensions with abelian Galois groups, since $\text{Gal}(K^{(1)}L/L) \cong \text{Gal}(K^{(1)}/(K^{(1)} \cap L))$, which is a subgroup of the class group $C_K = \text{Gal}(K^{(1)}/K)$, and $\text{Gal}(K^{(+)}L/L) \cong \text{Gal}(K^{(+)}/K^{(+)} \cap L)$, which is a subgroup of the narrow class group $C_K^{(+)} = \text{Gal}(K^{(+)}/K)$. By [1] we have that all $L$-primes are unramified in $K^{(1)}L$ and all finite $L$-primes are unramified in $K^{(+)}L$. It follows that $K^{(1)} \subseteq K^{(1)}L \subseteq L^{(1)}$ and $K^{(+)} \subseteq K^{(+)}L \subseteq L^{(+)}$.

We show next that $K^{(+)} \cap L^{(1)} = K^{(1)}$. The inclusion $K^{(1)} \subseteq K^{(+)} \cap L^{(1)}$ is clear. Since $K \subseteq K^{(+)} \cap L^{(1)} \subseteq K^{(+)}$, we see that $K^{(+)} \cap L^{(1)}$ is an abelian extension of $K$ and that every finite $K$-prime is unramified in $K^{(+)} \cap L^{(1)}$. Moreover, since $L$ is totally real, then $L^{(1)}$ is totally real, and since $K^{(+)} \cap L^{(1)} \subseteq L^{(1)}$, then all infinite $K^{(+)} \cap L^{(1)}$-primes are real. Hence $K^{(+)} \cap L^{(1)} \subseteq K^{(1)}$, and we have shown that $K^{(+)} \cap L^{(1)} = K^{(1)}$.

The following diagram illustrates our situation.

Since $K^{(+)} \cap L^{(1)} = K^{(1)}$ and $K^{(+)}/K^{(1)}$ is Galois, the extensions $K^{(+)}/K^{(1)}$ and $L^{(1)}/K$ are linearly disjoint, and $|K^{(+)}L^{(1)}; L^{(1)}| = |K^{(+)}; K^{(1)}|$. Thus $2 \dim_2 \tilde{U}_K^+ = |K^{(+)}; K^{(1)}| = |K^{(+)}L^{(1)}; L^{(1)}|$ divides $|L^{(+)}; L^{(1)}| = 2 \dim_2 \tilde{U}_L^+$, and so $\dim_2 \tilde{U}_K^+ \leq \dim_2 \tilde{U}_L^+$. Q.E.D.
With $L$ and $K$ as in Theorem 2.1 we have the following

**Corollary 2.2.** Let $p$ be a prime and let $K$ be a subfield of $L = Q(\zeta_p + \zeta_p^{-1})$. If the class number of $Q(\zeta_p)$ is odd, then $\dim_2 \overline{U}_x^+ = \dim_2 \overline{U}_L^+ = 0$.

**Proof.** A classical result of Kummer (for example see [8, p. 128]) is that $\dim_2 \overline{U}_L^+ = 0$ whenever the class number of $Q(\zeta_p)$ is odd. Therefore the result now follows from Theorem 2.1. Q.E.D.

It is worth noting at this juncture that as a result of recent work of Shimura [10] Kummer's classical result cited in the proof of Corollary 2.2 is now extended to $\dim_2 (\overline{U}_L^+) = 0$ if and only if the class number of $Q(\zeta_p)$ is odd. Here $L = Q(\zeta_p + \zeta_p^{-1})$ as in Corollary 2.2.

Furthermore, by [3, p. 175], if $L = Q(\zeta_f + \zeta_f^{-1})$, where $f$ is composite, then $\dim_2 \overline{U}_L^+ > 0$, and $N(\overline{U}_L) = \{1\}$.

An application of Theorem 2.1 is the following

**Example 2.3.** Let $K = Q(\alpha)$ where the minimal polynomial of $\alpha$ over $Q$ is $x^3 - x^2 - 234x + 729$. Then $K$ has conductor 703; i.e., the minimal cyclotomic field containing $K$ is $Q(\zeta_{703})$, so $K \subseteq L = Q(\zeta_{703} + \zeta_{703}^{-1})$. It can be shown that $\dim_2 \overline{U}_K^+ = 2$. Thus by Theorem 2.1 $\dim_2 \overline{U}_L^+ \geq 2$. For a list of such examples of cyclic cubic fields the reader may consult [2].

Next we prove

**Proposition 2.4.** Let $K$ be a totally real algebraic number field. Then $\dim_2 \overline{U}_x^+ \leq \dim_2 C_K^{(+)}$.

**Proof.** From [6, Theorem 3.1, p. 203] we have that

$$\dim_2 (\overline{U}_x^+) = \dim_2 Gal(K^{(+)} / K^{(1)}) \leq \dim_2 Gal(K^{(+)} / K) = \dim_2 (C_K^{(+)}) \text{.}$$

Q.E.D.

We note that, in general, it is not correct to claim that $\dim_2 \overline{U}_x^+ \leq \dim_2 C_K$. For example, if $K = Q(\sqrt{3})$, then $\dim_2 C_K = 0$. However, $K(\sqrt{-1})$ is unramified except at the real primes of $K$, and in fact $K^{(+)} = K(\sqrt{-1})$ [6, Theorem 3.10, p. 210]. Thus $\dim_2 (\overline{U}_K^+) = \dim_2 C_K^{(+)} = 1$. However, under more restrictive hypotheses it is possible to achieve $\dim_2 (\overline{U}_K^+) \leq \dim_2 C_K$.

**Theorem 2.5 (Oriat [9]).** Let $K$ be a finite real Galois extension of $Q$ with Galois group of odd exponent $n$ and suppose that $-1$ is congruent to a power of 2 modulo $n$. Then $\dim_2 \overline{U}_x^+ \leq \dim_2 C_K$. Moreover $\dim_2 C_K^{(+)} = \dim_2 C_K$.

In particular, when $h_K$ is odd, we have $\dim_2 \overline{U}_x^+ = 0$. (See [5] for an independent proof of this fact, distinct from that of [9]. The authors of [5] were unaware of the existence of [9] at the time of that writing.)

In the presence of Proposition 2.4, $\dim_2 \overline{U}_x^+ \leq \dim_2 C_K$ is of course an immediate consequence of $\dim_2 C_K = \dim_2 C_K^{(+)}$.

We now exhibit a proof of Theorem 2.5 in the case where $K$ is abelian. This is a simple proof based on the self-duality results established in [11]. Before so doing we need to set the stage with some additional notation and concepts.
Let $O_K$ denote the ring of integers of an algebraic number field $K$. We define $\alpha \in O_K$ to be singular if the ideal $(\alpha)$ is the square of an ideal. Moreover $\alpha$ is called odd if $(\alpha)$ is relatively prime to $(2)$. Furthermore, $\alpha$ is called primary if it is odd and $\alpha \equiv \xi^2 \pmod{4}$ for some $\xi \in O_K$. (For details and further development on these concepts we refer the reader to Hecke [4, pp. 217–237].) We denote by $O_K^0$ the singular primary numbers and note that by [4, Theorem 120, p. 137] we have $\mu \in O_K^0$ with $\mu \notin O_K^2$ if and only if $K \nsubseteq K(\sqrt{\mu}) \subseteq K^{(+)}$. It follows that $|K^{(+)}:K| = |\overline{O}_K^0|$, where $K^{(+)}$ is the maximal abelian extension of $K$ unramified at the finite primes such that $\text{Gal}(K^{(+)}/K)$ is a direct sum of copies of $\mathbb{Z}/2\mathbb{Z}$. Thus by Kummer theory we have that $K^{(+)}$ is the maximal subfield of $K^{(+)}$ of the form $K(\sqrt{\mu_1}, \ldots, \sqrt{\mu_r})$ for some $\mu_i \in K$, $i = 1, 2, \ldots, r$. Similarly, define $K^{(1)}$ as the maximal abelian extension of $K$ unramified at all primes with $\text{Gal}(K^{(1)}/K)$ being a direct sum of copies of $\mathbb{Z}/2\mathbb{Z}$. Therefore $K^{(1)}$ is the maximal subfield of $K^{(1)}$ of the form $K(\sqrt[4]{\alpha_1}, \ldots, \sqrt[4]{\alpha_s})$ for some $\alpha_i \in K$, $i = 1, 2, \ldots, s$. Furthermore, we note that $K^{(1)} = K^{(+)} \cap K^{(1)}$.

Now if $O_K^+$ denotes the subgroup of $O_K$ consisting of totally positive integers, then $\mu \in O_K^+ \cap O_K^0$ with $\mu \notin O_K^2$ if and only if $K \nsubseteq K(\sqrt{\mu}) \subseteq K^{(1)}$, from which it follows that $|K^{(1)}:K| = |\overline{O}_K|$. Now we are in a position to prove Theorem 2.5 under the assumption that $K$ is a finite real extension of $Q$ with abelian Galois group $G$.

**Proof.** Let $M$ be a simple $F_2G$-module where $F_2$ is the field of two elements. Then by Schur’s lemma $M \cong F_2Ge$ for some idempotent $e$. Now let $\psi$ be the standard involution of $F_2G$ given by $\psi(g) = g^{-1}$ for all $g \in G$. Then by the same argument as in the proof of [5, Theorem, p. 615] we have that $F_2Ge \cong F_2G\psi(e)$, resulting from $-1$ being a power of 2 modulo $n$. Hence we have shown that all simple $F_2G$-modules are self-dual. Therefore from [11, Corollary 1, p. 157] we have that $\dim_{F_2}U_K = \dim_{F_2}C_K$.

By the self-duality established above, we may use exactly the same reasoning as used by Taylor on $\overline{U}_K^+$ and $\overline{U}_K^0$ in [11, (*), p. 157] to establish $\overline{O}_K^+ = \overline{O}_K^0$. Hence by the discussion preceding the proof, we have $K^{(1)} = K^{(+)}$, i.e., $\dim_{F_2}C_K = \dim_{F_2}C_K^{(+)}$.

Q.E.D.

In what follows, the signature map from $U_K$ to $F_2G$ is defined by $\text{sgn}(u) = \sum_{s \in G} s(u^0)$, where $s$ is called the signature of $u$ with $s: K^* \rightarrow F_2$ defined by $s(k) = 0$ if $k > 0$ and $s(k) = 1$ if $k < 0$.

It is interesting to note that Lagarias [7] has proved the equivalence of

(2.7) $\dim_{F_2}C_K = \dim_{F_2}C_K^{(+)}$.

(2.8) All odd singular integers $\alpha$ have their signature type determined by the congruence class of $\alpha$ modulo 4.

(2.9) There are $\alpha$ of all signature types with $\alpha$ an odd singular integer.

(2.10) $K^{(+)}$ is totally real.

Thus, it would be of interest to investigate those totally real algebraic number fields $K$ for which the Sylow 2-subgroup of $\text{Gal}(K^{(+)}/K)$ is elementary abelian. It is not enough to know that the Sylow 2-subgroup of $\text{Gal}(K^{(1)}/K)$ is elementary abelian. For example in [2] we see that “most” of the Sylow 2-subgroups of $\text{Gal}(K^{(1)}/K)$ are elementary abelian where $K$ is a cyclic cubic field. However, there
are no instances known to the authors in the cyclic cubic case where \( \text{Gal}(K^{(+)}/K) \) has elementary abelian Sylow 2-subgroup.

**References**


**Department of Mathematics, San Jose State University, San Jose, California 95192** (Current address of H. M. Edgar and B. L. Peterson)

**Department of Mathematics, University of Calgary, Calgary, Alberta, T2N 1N4, Canada** (Current address of R. A. Mollin)