PROCEEDINGS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 87, Number 4, April 1983

TOTALLY POSITIVE UNITS AND SQUARES

I. HUGHES AND R. MOLLIN[1]

ABSTRACT. Let K be a finite cyclic extension of the rational number field Q, with Galois group $G(K/Q)$ of order p^a for an odd prime p. Armitage and Fröhlich [1] proved that if the order of 2 modulo p is even and the class number h_K of K is odd then $U_K^+ = U_K^2$, where U_K is the group of units of the ring of integers $\mathcal{O}_K$ of K, U_K^+ is the group of totally positive units, and U_K^2 is the group of unit squares. The purpose of this paper is to provide a generalization of this result to a larger class of abelian extensions of Q.[2]

1. We begin with some definitions and notation. Let K be a finite real abelian extension of Q. We define U_K^0 to be $\{u \in U_K\colon u \equiv k^2 \bmod(4)$ for some $k \in \mathcal{O}_K\}$, and set $\overline{U_K^0} = U_K^0/U_K^2$, where U_K is the group of units of the ring of integers $\mathcal{O}_K$ of K and U_K^2 is the group of unit squares. Similarly we set $\overline{U_K^+} = U_K^+/U_K^2$, where U_K^+ is the group of totally positive units. It is worth noting at this juncture that the units u in U_K^0 are precisely those units for which $K(\sqrt{u})/K$ is ramified at, at most, the infinite K-primes when $|K\colon Q|$ is odd. This fact follows from Hecke [5] and Kummer theory considerations.

We let F_K denote the group of cyclotomic units a la Leopoldt [8]. We caution the reader that these are *not* Hasse's circular units, C_K (see [4]). F_K is a subgroup of U_K related to C_K, and Leopoldt has obtained the result $|U_K\colon F_K| = h_K Q_G$ where Q_G is an integer depending on the structure of $G(K/Q)$ and h_K is the class number of K. For the reader who is interested in an easily understood exposition of Leopoldt's work in this direction we suggest Oriat's description [10] as an alternative to [8]. Now, F_K^+, F_K^0, $\overline{F_K^+}$ and $\overline{F_K^0}$ are defined in an analogous fashion to that of U_K.

We let $K^{(1)}$ denote the Hilbert class field of K; i.e., $|K^{(1)}\colon K| = h_K$; and we let $K^{(+)}$ denote the "*narrow*" class field of K; i.e., $G(K^{(+)}/K)$ is the quotient group of ideals of $\mathcal{O}_K$ modulo totally positive principal ideals. We note that asking when $U_K^+ = U_K^2$ is equivalent to asking when $K^{(+)} = K^{(1)}$. This fact, for real K, is the statement of [7, Theorem 3.1, p. 203], the proof of which uses the Artin map.

2. To prove the main result we first need two lemmas. The first lemma is provided in its most general form since it may be of independent interest.

In the following lemma $\mathbb{Z}_2$ denotes the field of 2 elements.

Received by the editors October 15, 1981 and, in revised form, July 13, 1982.

1980 *Mathematics Subject Classification*. Primary 12A65, 12A95.

Key words and phrases. Totally positive units, squares, cyclotomic units, class field theory.

[1]This author's research is supported by N.S.E.R.C. Canada University research fellowship #U0077.

[2]Kummer began the investigation of U_K^+ and U_K^2 for $K = Q(\zeta_p + \zeta_p^{-1})$ where ζ_p denotes a primitive pth root of unity. The classification of those p for which $U_K^+ = U_K^2$ remains unsolved. Our main result advances the solution of this problem as well.

0002-9939/82/0000-0736/$02.00

LEMMA 1. *Let* $|K^{(1)}: Q|$ *be odd where* K *is Galois over* Q. *Then*
(1) $\dim_{\mathfrak{F}_2} \overline{U_K^+} = \dim_{\mathfrak{F}_2} \overline{U_K^0}$ *and*
(2) $\overline{U_K^+} \cap \overline{U_K^0} = \{1\}$.

PROOF. (1) Let $\{\bar{u}_1, \ldots, \bar{u}_n\}$ be an $\mathfrak{F}_2$-basis of $\overline{U_K^0}$ where $u_i \in U_K^0$ for $i = 1, 2, \ldots, n$. Let $\bar{K}$ be the subfield of $K^{(+)}$ such that $|\bar{K}: K| =$ the 2-power part of $|K^{(+)}: K|$. Since the elements of U_K^0 are precisely the units of $\mathcal{O}_K$ such that $K(\sqrt{u})$ is ramified at, at most, the infinite K-primes then $K(\sqrt{u_1}, \sqrt{u_2}, \ldots, \sqrt{u_n}) \subseteq \bar{K}$. Moreover, if $K(\sqrt{u_1 u_2 \cdots u_r}) = K$ for some r with $1 \leq r \leq n$ then $u_1 \cdots u_r \in U_K^2$; i.e., $\bar{u}_1 \cdots \bar{u}_r = 1$ which is a contradiction since the $\bar{u}_i$'s are linearly independent as an $\mathfrak{F}_2$-basis for $\overline{U_K^0}$.

Now, since h_K is odd then by class field theory any quadratic extension of K in $\bar{K}$ is obtainable by taking roots of units of K. Hence $\bar{K} = K(\sqrt{u_1}, \ldots, \sqrt{u_n})$. Since $|\overline{U_K^0}| = |\bar{K}: K| = |K^{(+)}: K^{(1)}| = |\overline{U_K^+}|$ we have secured (1).

(2) Let $1 \neq u \in U_K^+ \cap U_K^0$. Since $u \in U_K^+$ then $K(\sqrt{u})/K$ is unramified at all infinite K-primes. By Kummer theory the only other possibility for ramification in $K(\sqrt{u})/K$ is at K-primes above 2. But $u \in U_K^0$ precludes this possibility. Thus $K(\sqrt{u})$ is in $K^{(1)}$, contradicting that h_K is odd. Q.E.D.

LEMMA 2. *Let* $|K^{(1)}: Q|$ *be odd where* K *is abelian over* Q. *Then* $\overline{U_K^+} \cong \overline{F_K^+}$.

PROOF. We have $|U_K^+ : U_K^2| = |U_K: U_K^2| / |U_K: U_K^+|$. Moreover,

$$|F_K^+ : F_K^2| = |U_K: F_K^2| / |U_K: F_K^+| = |U_K: U_K^2| \cdot |U_K^2: F_K^2| / |U_K: F_K| \cdot |F_K: F_K^+|$$
$$= |U_K: U_K^2| / |F_K: F_K^+|.$$

Now we show that $|F_K: F_K^+| = |U_K: U_K^+|$. By Leopoldt [**8**] (see also [**10**, Proposition IV(b), p. 28]) we have that $|U_K: F_K|$ is odd because h_k is odd (see §1). Now let U_K' denote the group of absolute values of U_K; i.e., U_K' may be identified with $U_K/\{\pm 1\}$. Similarly let F_K' denote the group of absolute values of F_K. Thus U_K' may be viewed as a free $\mathbf{Z}$-module of dimension $n - 1$ where $|K: Q| = n$. Therefore there is a basis $u_1, u_2, \ldots, u_{n-1}$ for U_K' such that $u_1^{v_1}, \ldots, u_{n-1}^{v_{n-1}}$ is a basis for F_K' where the v_i's are positive integers, and so we have $|U_K: F_K| = |U_K': F_K'| = v_1 \cdots v_{n-1}$. Hence $|U_K: U_K^+| = |F_K: F_K^+|$. Q.E.D.

We need one more result in order to prove the main theorem. It is easily seen, and interesting to note, that a well-known paper by Iwasawa [**6**] in fact holds for the *narrow* class number $h_K^{(+)} = |K^{(+)}: K|$ (although [**6**] is only stated for h_K, the proof holds for $h_K^{(+)}$ mutatis mutandis). The revised result is:

(*) If K/k is a finite Galois extension of number fields and some *finite* k-prime is fully ramified in K then $h_k^{(+)} \mid h_K^{(+)}$. Furthermore, if K/k is cyclic p-power and no other *finite* prime ramifies in K then $p \mid h_K^{(+)}$ implies $p \mid h_k^{(+)}$.

As far as $h_K^{(+)}$ is concerned, the latter part of (*) is only interesting for $p = 2$, as we shall see. From (*) it is immediate that:

(**) If K is a finite real Galois extension of Q and $k \subseteq K$ such that $G(K/k)$ is cyclic of 2-power order with *exactly* one k-prime ramified in K then $\overline{U_k^+} = \{1\}$ if and only if $\overline{U_K^+} = \{1\}$.

3. The stage is now set for the main result which is a generalization of [**1**, IV, p. 94] for the odd class number case. In what follows Q_2 denotes the completion of Q at 2.

THEOREM. *Let K be a real finite abelian extension of Q. Suppose $L \subseteq K$ with $|L:Q|$ odd, $G(L/Q) = G$ of exponent n, and $G(K/L)$ cyclic of 2 power order. If $K \neq L$ then we assume that exactly one L-prime ramifies in K. If h_L is odd and -1 is congruent to a power of 2 modulo n then $U_K^+ = U_K^2$.*

PROOF. From (**) it suffices to show that $\overline{U_L^+} = \{1\}$. From [**3**, Théorème III.2, p. 187] we have that if $\overline{F_L^+} = \oplus_i \mathfrak{F}_2 G e_i$ (where the e_i's are idempotents) is a decomposition of $\overline{F_L^+}$ into simple submodules then $\overline{F_L^0} = \oplus_i \mathfrak{F}_2 G \psi(e_i)$ where ψ is the standard involution of $\mathfrak{F}_2 G$ given by $\psi(g) = g^{-1}$ for all $g \in G$. Since h_L is odd then by Lemma 2 we have $\overline{U_L^+} \cong \overline{F_L^+}$. Hence it follows that $\overline{U_L^+}$ is mapped onto $\overline{U_L^0}$ under ψ.

Now suppose that $\mathfrak{F}_2 Ge$ is a simple component of $\mathfrak{F}_2 G$ corresponding to an absolutely irreducible character χ of G; and let m = the order of χ in the group of absolutely irreducible characters of G. Then $G(Q_2(\varepsilon_m)/Q_2)$ is isomorphic to $H = \{\bar{2}, \bar{2}^2, \ldots, \bar{2}^f\}$ in $(Z/mZ)^*$, where f = the order of 2 modulo m. Hence $-1 \in H$ if and only if χ is conjugate to χ^{-1} if and only if $\mathfrak{F}_2 Ge = \mathfrak{F}_2 G\psi(e)$. Since -1 is congruent to a power of 2 modulo n by hypothesis then we must have $\overline{U_L^+} = \overline{U_L^0}$. By Lemma 1 we get $\overline{U_L^+} = \{1\}$. Q.E.D.

We note that if -1 is not a power of 2 modulo n then the theorem fails. For example if K is the subfield of $Q(\varepsilon_{29})$ of degree 7 over Q then $h_K = 1$ but $\overline{U_K^+} \neq \{1\}$ (see [**2**, Example 1, p. 380]).

When h_K is even the proof of the theorem fails to be valid. For example if $|K:Q| = 3$ where $K \subseteq Q(\varepsilon_{163})$ then h_K is even, $\overline{F_K^+} \neq \{1\}$ and $\overline{U_K^+} = \{1\}$ (see [**3**, p. 188 and **2**, p. 383]).

4. Applications of the theorem. (1) The Armitage-Fröhlich result [**1**] for the odd class number case is immediate.

(2) Let $K = Q(\varepsilon_p + \varepsilon_p^{-1})$. As mentioned above it remains an unsolved problem as to the determination of those primes p for which $U_K^+ = U_K^2$. The following, however, advances the solution. If $F \subseteq K$ with $|F^{(1)}:Q|$ odd and $|K:F|$ is a 2-power then whenever -1 is congruent to a power of 2 modulo the exponent of $G(F/Q)$ we have $U_K^+ = U_K^2$.

In particular if p is a *Fermat prime* then $F = Q$ and so $U_K^+ = U_K^2$ (see also [**9**]).

(3) If K is a real subfield of $Q(\varepsilon_{2^a})$ then $U_K^+ = U_K^2$. This is Weber's theorem (see [**11**]). In fact if K is any real cyclic 2-power extension of Q with exactly one ramified prime K then $U_K^+ = U_K^2$ (see also [**9**]).

(4) If $K = Q(\sqrt{p})$ for a prime $p \equiv 1 \pmod 4$ then $U_K^+ = U_K^2$. We note that in the real quadratic field $K = Q(\sqrt{d})$ case, asking when $U_K^+ = U_K^2$ is equivalent to asking whether there exists a $u \in U_K$ with norm -1 (see [**7**]). This is currently an unsolved problem.

5. Open questions. We close with some questions, the answers to which would provide a means of generating more examples (which are needed to gain evidence for advancing the theorem).

Suppose F_1 and F_2 are finite real abelian extensions of Q. It can be easily shown that $\overline{U_{F_1}^+} \times \overline{U_{F_2}^+}$ injects into $\overline{U_{F_1F_2}^+}$. A natural question to ask is:

(a) Is $\overline{U_{F_1}^+} \times \overline{U_{F_2}^+}$ isomorphic to $\overline{U_{F_1F_2}^+}$? or

(b) If (a) has a negative answer then: What restrictions can be made in terms of the arithmetic of F_1 and F_2 to guarantee that $\overline{U_{F_1}^+} \times \overline{U_{F_2}^+}$ and $\overline{U_{F_1F_2}^+}$ are isomorphic?

We leave the reader with an example, pertaining to (a) and (b), which we feel is worth investigating toward the possibility of finding a counterexample to (a) or, at worst, providing further evidence that (a) has an affirmative answer. Moreover, it would add to the quite short list of available examples.

Consider the prime $p = 18121$. Let K be the subfield of $Q(\varepsilon_p)$ of degree 15 over Q. Let $F_i \subseteq K$ for $i = 1, 2$ with $|F_1 : Q| = 3$ and $|F_2 : Q| = 5$. By Gras [3, Remark IV.4, p. 189] h_{F_i} is odd for $i = 1, 2$. Therefore since -1 is a power of 2 modulo both 3 and 5, then by our theorem $\overline{U_{F_i}^+} = \{1\}$ for $i = 1, 2$. However -1 is not a power of 2 modulo 15. Moreover by Gras [3] h_K is even (in fact divisible by 8) so we cannot say anything about $\overline{U_{F_1F_2}^+}$. Is $\overline{U_{F_1F_2}^+} = \{1\}$?

ACKNOWLEDGEMENTS. The authors welcome the opportunity to thank the referee for suggestions and questions which led to strengthening the paper's results as well as making the paper more self-contained.

Author R. Mollin wishes to thank Professor Fröhlich for his encouragement to continue work on the problem while the author was on an invited visit to the University of Illinois at Urbana-Champaign in September 1981. Also, thanks must go to John McKay for pointing out the problem to the author in Montreal, 1975.

REFERENCES

1. J. V. Armitage and A. Fröhlich, *Class numbers and unit signatures*, Mathematica **14** (1967), 94–98.

2. D. Garbanati, *Unit signatures, and even class numbers, and relative class numbers*, J. Reine Angew. Math. **274/275** (1975), 376–384.

3. G. Gras, *Critère de parité du nombre de classes*, Bull. Soc. Math. France **103** (1975), 177–190.

4. H. Hasse, *Über die Klassenzahl abelscher Zahlkorper*, Akademie-Verlag, Berlin, 1952.

5. E. Hecke, *Vorlesungen über die Theorie der algebaischen Zahlen*, Chelsea, New York, 1948.

6. K. Iwasawa, *A note on class numbers of algebraic number fields*, Abh. Math. Sem. Univ. Hamburg **20** (1956), 257–258.

7. G. J. Janusz, *Algebraic number fields*, Academic Press, New York, 1973.

8. H. W. Leopoldt, *Über Einheitengruppe und Klassenzahl reeller abelscher Zahlkörper*, Abh. Deutsch. Akad. Wiss. Berlin, Math.-Nat. Kl. **1953**, no. 2, (1954).

9. R. Mollin, *Class numbers and a generalized Fermat theorem*, J. Number Theory (to appear).

10. B. Oriat, *Sur l'article de Leopoldt intitulé (über Einheitengruppe und Klassenzahl reeller abelscher Zahlkorper)*, Publ. Math. de la Faculté des Sciences de Besançon, Théorie des nombres (1974–75).

11. H. Weber, *Lehubuch der Algebra*. Vol. II, Aufl. Braunschweig, 1899; reprinted by Chelsea, New York, 1966.

DEPARTMENT OF MATHEMATICS AND STATISTICS, QUEEN'S UNIVERSITY, KINGSTON, ONTARIO, CANADA K7L 3N6

DEPARTMENT OF MATHEMATICS, UNIVERSITY OF CALGARY, CALGARY, ALBERTA, CANADA T2N 1N4