ON THE NORMS OF UNITS IN QUADRATIC FIELDS

H. F. TROTTER

Let R be the ring of algebraic integers in the quadratic extension $Q(\sqrt{d})$ of the rationals, where d is a positive square-free integer. The group of units of R is isomorphic to $Z_2 \oplus Z$ and generated by -1 and the *fundamental unit* η. The norm of η, $\eta\bar{\eta}$, is of course ± 1; it is -1 if and only if the equation

$$x^2 - dy^2 = -1 \tag{1}$$

has a solution in integers. (This and other basic facts stated here without proof can be found in various texts on number theory such as [1].) An obvious necessary condition for (1) to have a solution is that no factor of d be congruent to 3 modulo 4. The result that this condition is sufficient if d is prime goes back to Legendre; the general problem has been investigated by a number of authors. (See the introduction and list of references in [2].)

The theorem we give below does not seem to have been noted explicitly. It is quite elementary and leads directly to various sufficient conditions for the solvability of (1). The theorem and its proof were suggested by the proof given in [1, p. 185] for the case that d is a prime.

THEOREM. *Let $d = p_1 \cdots p_n$ be the product of distinct primes, none of which is congruent to 3 modulo 4. Let R be the ring of algebraic integers in $Q(\sqrt{d})$ and η its fundamental unit. Then the following three conditions are equivalent.*

(i) $\eta\bar{\eta} = -1$.

(ii) *None of the ideals $[r, \sqrt{d}]$ is principal, where r is a proper non-trivial factor of d.*

(iii) *The equation*

$$|rx^2 - sy^2| = 4 \tag{2}$$

has no solution in integers with $rs = d$ and neither r nor s equal to ± 1.

PROOF. We use greek letters for elements of R and reserve latin letters for rational integers. For each prime p_i dividing d the ideal (p_i) factors as the square of the self-conjugate ideal $[p_i, \sqrt{d}]$, which is the unique ideal with norm p_i. Hence for any r dividing d there is a unique ideal of norm $|r|$, which is easily seen to be $[r, \sqrt{d}]$. It is principal if and only if there exists an α with norm $\alpha\bar{\alpha} = \pm r$. For any

Received by the editors September 17, 1968.

α, $2\alpha = u + v\sqrt{d}$ where u and v have the same parity and are both even if d is. Then $4\alpha\bar{\alpha} = u^2 - dv^2$ and there exists α with $\alpha\bar{\alpha} = \pm r$ if and only if

$$|u^2 - dv^2| = 4|r| \tag{3}$$

has a solution in integers. (The parity conditions on u, v are automatically satisfied for any solution of (3).) For any solution of (2), $u = rx$ and $v = y$ gives a solution of (3). Conversely, for any solution of (3), r divides u (since r divides d and is square-free) and $s = d/r$, $x = u/r$, $y = v$ gives a solution of (2). Hence conditions (ii) and (iii) are equivalent.

Now suppose $r|d$ and $[r, \sqrt{d}]$ is the principal ideal (α). Since the ideal is self-conjugate, $\bar{\alpha} = \epsilon\alpha$ for some unit ϵ. Obviously $\epsilon\bar{\epsilon} = 1$. If (i) holds then either ϵ or $-\epsilon$ is an even power of η and so $\epsilon = \pm\delta^2$ for some unit δ. Then $\pm r = \alpha\bar{\alpha} = \epsilon\alpha^2 = \pm\delta^2\alpha^2$ and $|r|$ is a perfect square in R. Hence $|r| = 1$ or d. We have shown that (i) implies (ii).

If $\eta\bar{\eta} = +1$ then by Hilbert's Theorem 90 [1, p. 185], $\eta = \alpha/\bar{\alpha}$ for some α; we may assume that α and $\bar{\alpha}$ have no common factor. Since η is a unit, $(\alpha) = (\bar{\alpha})$ and is a self-conjugate ideal. Any ideal times its conjugate is a principal ideal generated by a rational integer. The self-conjugate prime ideals are those generated by rational primes which remain prime in R, and the ideals $[p_i, \sqrt{d}]$. Thus any self-conjugate ideal is the product of a principal ideal generated by a rational integer and a product of the $[p_i, \sqrt{d}]$. A rational integral factor of (α) would be a common factor of α and $\bar{\alpha}$, so (α) is either R or the product of some subset of the $[p_i, \sqrt{d}]$. In other words, $(\alpha) = [r, \sqrt{d}]$ for some r dividing d. If $r = 1$ or d, $\alpha = \epsilon$ or $\epsilon\sqrt{d}$ with $\epsilon\bar{\epsilon} = 1$. Then $\eta = \pm\epsilon^2$, contradicting the assumption that η is a fundamental unit. Consequently r is a proper nontrivial divisor of d. Thus (ii) implies (i) and the proof is complete.

COROLLARY. *The fundamental unit η has norm -1 if there is no nontrivial factorization $d = rs$ such that r and s are quadratic residues of each other.*

PROOF. Immediate from condition (iii) of the theorem. (The absolute value signs are irrelevant since -1 is a quadratic residue of all the prime factors of d.)

The corollary gives easy sufficient conditions that $\eta\bar{\eta} = -1$ when d is the product of just two primes, since then there is only one proper factorization of d. If $d = 2p$, $p \equiv 5 \pmod 8$, then 2 is a nonresidue (mod p) and $\eta\bar{\eta} = -1$. Similarly if $d = pq$, $p \equiv q \equiv 1 \pmod 4$, p and q

primes such that the Legendre symbol $(p|q) = -1$, then $\eta\bar{\eta} = -1$. (The example $d = 145 = 5.29$ shows that this sufficient condition is not necessary. Although $(5|29) = 1$, $\eta = 12+\sqrt{145}$ and $\eta\bar{\eta} = (12+\sqrt{145}\,(12-\sqrt{145}) = -1$.)

Suppose $d = p_1 \cdots p_n$, with $p_i \equiv 1 \pmod 4$ for all i, and define $t_{ij} = (p_i|p_j) = (p_j|p_i)$. A proper factorization of d corresponds to a partition of $\{1, \cdots, n\}$ into two sets A and B with $r = \prod_{i\in A} p_i$, $s = \prod_{j\in B} p_j$. Define $T_A(j) = \prod_{i\in A} t_{ij}$ for $j\in B$ and $T_B(i) = \prod_{j\in B} t_{ij}$ for $i\in A$. Then r and s are quadratic residues of each other if and only if $T_A(j) = 1$ for all $j\in B$ and $T_B(i) = 1$ for all $i\in A$. In any particular case it is easy to check whether there is a partition having this property. Various general cases can also be handled. Those listed below were suggested by examples given in [2], which are there derived as consequences of deeper theorems that are considerably more complicated than the theorem of this paper. Specifically, (3.14), (3.22), and (3.26) of [2] are special cases of (a), (3.20) is a special case of (c) and (3.24) and (3.25) are special cases of (b). (There seems to be a misprint in the statement of (3.25), which presumably should read, in part, "$(q_2|q_3) = (q_4|q_5) = -1$" but which appears without the minus sign.)

PROPOSITION. *Let d be the product of distinct primes $p_1 \cdots p_n$ with $p_i \equiv 1 \pmod 4$ for all i, and set $t_{ij} = (p_i|p_j) = (p_j|p_i)$ for $i \neq j$. Each of the following is a sufficient condition that the fundamental unit of $Q(\sqrt{d})$ have norm -1.*

(a) *n is odd and $t_{ij} = -1$ with the exception of 0 or more disjoint pairs $\{i, j\}$ for which $t_{ij} = 1$.*

(b) *$t_{1j} = -1$ for all $j \neq 1$, and $t_{ij} = 1$ for $i, j \neq 1$ except for 0 or more disjoint pairs $\{i, j\}$ for which $t_{ij} = -1$.*

(c) *n is even, $t_{12} = -1$, $t_{1j} = 1$ for $j > 2$, and all other $t_{ij} = -1$ except for 0 or more disjoint pairs $\{i, j\}$ for which $t_{ij} = 1$.*

PROOFS. We let A, B stand for an arbitrary partition of $\{1, \cdots, n\}$, and use the notations T_A, T_B defined above. In each case we show that for every A, B either there is $i\in A$ with $T_B(i) = -1$ or there is $j\in B$ with $T_A(j) = -1$, so the hypothesis of the corollary is satisfied.

(a) We may suppose A contains an odd number of elements, and B an even number. If $j\in B$ belongs to no exceptional pair, or belongs to one whose other member is also in B then $T_A(j) = -1$. On the other hand, if $\{i, j\}$ is an exceptional pair, $i\in A$, $j\in B$, then $T_B(i) = -1$.

(b) We may suppose $1\in A$. The rest of the argument follows word for word as in the last two sentences of (a).

(c) If 1 and 2 are separated in the partition then either $T_A(1)$ or $T_B(1)$ is equal to -1. Otherwise every factor t_{1j} appearing in any product T_A or T_B is $+1$, so p_1 is irrelevant and the problem reduces to case (a).

References

1. H. Cohn, *A second course in number theory*, Wiley, New York, 1962.

2. D. Pumplün, *Über die Klassenzahl und die Grundeinheit des reelquadratischen Zahlkörpers*, J. Reine Angew. Math. **230** (1968), 167–210.

Princeton University