ROCKY MOUNTAIN
JOURNAL OF MATHEMATICS
Volume 19, Number 3, Summer 1989

IDEAL CLASS GROUPS OF EXPONENT TWO AND ONE-CLASS GENERA OF BINARY QUADRATIC LATTICES

A.G. EARNEST

Let K/K_0 be a relative quadratic extension of algebraic number fields. K equipped with the relative norm mapping forms a binary quadratic space over K_0. If R and R_0 denote the rings of algebraic integers of K and K_0, respectively, then R can be considered as a binary quadratic R_0-lattice on the quadratic space K. In this note, we will consider the relationship between the following two statements:

(A) R has genus class number one as quadratic R_0-lattice;

(B) all squares in the ideal class group of K are trivial.

In the classical case that K_0 is the rational number field and K is an imaginary quadratic field, (A) and (B) are equivalent by the Principal Genus Theorem of Gauss and the well-known correspondence between equivalence classes of integral binary quadratic forms and equivalence classes of ideals of R. We will show here that, in general, neither statement (A) nor (B) implies the other, and that the distinction between the two statements arises primarily from the nontriviality of the ideal class group of the ground field K_0.

Chowla proved in 1934 [**1**] that there exist only finitely many imaginary quadratic fields for which either of the equivalent conditions (A) or (B) hold. This finiteness for the number of fields satisfying (A) has been generalized to broader classes of fields by Pfeuffer [**9**]. In fact, under the assumption of the validity of either the generalized Riemann hypothesis or the Artin conjecture, there exist only finitely many CM-fields K (that is, totally imaginary quadratic extensions K of a totally real subfield K_0) for which (A) holds. The unproven hypothesis can be removed if one restricts either to the class of such fields having bounded degree, or to those which can be reached from the rational number field by a tower of relatively normal extensions.

Research partially supported by a Summer Research Fellowship from Southern Illinois University.

On the other hand, only much weaker results have been obtained for fields satisfying (B). Of course, it is not even known whether the special case in which the ideal class group itself is trivial occurs finitely often among CM-fields. The largest class of such fields on which this finiteness is known is the class of imaginary abelian fields [**11**]. However, even on this more restricted class, finiteness of the number of fields satisfying (B) remains unproven. Partial results in this direction are obtained in [**2**] and [**4**].

Let us fix some notations to be used in the remainder of this paper. K, K_0, R and R_0 will be as described in the opening paragraph, and U and U_0 will be the groups of units in R and R_0, respectively. $\mathcal{I}$ will denote the multiplicative group of fractional ideals of $K, \mathcal{P}$ the subgroup of $\mathcal{I}$ consisting of principal ideals, and $\mathcal{C}$ the ideal class group $\mathcal{I}/\mathcal{P}$. Similarly, $\mathcal{I}_0, \mathcal{P}_0$ and $\mathcal{C}_0$ will be the corresponding objects for the field K_0. Let $\mathcal{G}$ denote the genus of R as quadratic R_0-lattice; so $\mathcal{G} = \{X^{1-\sigma} : X \in \mathcal{I}\}$, where σ denotes the nontrivial K_0-automorphism of K (see, e.g., [**3**, Proposition 2.6]). We denote by cls R the proper isometry class of R, cls $R = \{\lambda R : \lambda \in K, N(\lambda) = 1\}$, where N denotes the relative norm from K to K_0. Finally, let $\mathcal{A}$ and $\mathcal{A}^*$ be the subgroups of $\mathcal{I}$ consisting of ambiguous and weakly ambiguous ideals, respectively; that is, $\mathcal{A} = \{X \in \mathcal{I} : X = X^\sigma\}$ and $\mathcal{A}^* = \{X \in \mathcal{I} : X^{1-\sigma} \in \mathcal{P}\}$.

Consider the group homomorphism $\theta : \mathcal{I} \to \mathcal{G}/\text{cls } R$ defined by $\theta(X) = X^{1-\sigma}$ cls R. If $X \in \ker\theta$, then there exists $\lambda \in K$ with $N(\lambda) = 1$ such that $X^{1-\sigma} = \lambda R$. By Hilbert's Theorem 90, there exists $\beta \in K$ such that $\lambda = \beta^{1-\sigma}$. It follows that $\ker\theta = \mathcal{A}\mathcal{P}$. So the sequence

$$1 \to \mathcal{A}\mathcal{P} \to \mathcal{I} \xrightarrow{\theta} \mathcal{G}/\text{cls}\, R \to 1$$

is exact. This proves the following

LEMMA. *$\mathcal{H}(R) = (\mathcal{I} : \mathcal{A}\mathcal{P})$, where $\mathcal{H}(R) = (\mathcal{G} : \text{cls}\, R)$.*

The calculations of the group indices $(\mathcal{A}^* : \mathcal{P})$ and $(\mathcal{A}^* : \mathcal{A}\mathcal{P})$ are classical and can be found in the work of Hasse [**5**]. Using this information, the lemma can be used to produce an explicit formula for $\mathcal{H}(R)$ in terms of the ideal class numbers of K and K_0, the groups U and U_0, and the ramification of primes in the extension K/K_0. The formula in this generality appears in a paper of Körner [**6**, Theorem 1]. In the case that K is a CM-field (so R is a totally positive definite quadratic R_0-lattice), this formula specializes to that found by Shyr [**10**], Pfeuffer [**8**] and Peters [**7**] using Tamagawa numbers, the Minkowski-Siegel mass formula, and arithmetical arguments, respectively.

In order to describe $|\mathcal{C}^2|$ in terms of $\mathcal{H}(R)$, we introduce the subgroups $\mathcal{E} = \{XR : X \in \mathcal{I}_0\}$ and $\mathcal{S} = \{X^2 : X \in \mathcal{I}\}$ of $\mathcal{I}$. Let N denote the standard norm mapping $N : \mathcal{I} \to \mathcal{I}_0$. Note that, due to the identity $N(X)R = X^{1+\sigma}$ for $X \in \mathcal{I}$, we have $\mathcal{GE} = \mathcal{SE}$.

THEOREM. $|\mathcal{C}^2| = \mathcal{H}(R) \cdot \frac{(\mathcal{E}:\mathcal{E}\cap\mathcal{GP})}{(\mathcal{A}^*:\mathcal{AP})(\mathcal{E}:\mathcal{E}\cap\mathcal{SP})}$.

PROOF.

$$\begin{aligned}
|\mathcal{C}^2| &= (\mathcal{SP} : \mathcal{P}) = (\mathcal{GEP} : \mathcal{P})(\mathcal{E} : \mathcal{E} \cap \mathcal{SP})^{-1} \\
&= (\mathcal{GP} : \mathcal{P})(\mathcal{E} : \mathcal{E} \cap \mathcal{GP})(\mathcal{E} : \mathcal{E} \cap \mathcal{SP})^{-1} \\
&= (\mathcal{I} : \mathcal{A}^*)(\mathcal{E} : \mathcal{E} \cap \mathcal{GP})(\mathcal{E} : \mathcal{E} \cap \mathcal{SP})^{-1} \\
&= \mathcal{H}(R)(\mathcal{A}^* : \mathcal{AP})^{-1}(\mathcal{E} : \mathcal{E} \cap \mathcal{GP})(\mathcal{E} : \mathcal{E} \cap \mathcal{SP})^{-1},
\end{aligned}$$

where all equalities follow in a straightforward manner from the standard isomorphism theorems of group theory. □

If we now specialize to the situation where K is a CM-field with maximal totally real subfield K_0, the group index factors appearing in the theorem can in some cases be explicitly evaluated. This becomes possible due to the understanding of the extension and norm mappings, $\mathcal{I} : \mathcal{C}_0 \to \mathcal{C}$ and $N : \mathcal{C} \to \mathcal{C}_0$, respectively, relating the class groups of K and K_0 in this setting. Specifically, it follows from general theorems from class field theory that N is surjective and $|\ker \mathcal{I}| \leq 2$ [**12**; Theorems 10.1 and 10.3].

COROLLARY 1. *Suppose K is a* CM-*field with maximal totally real subfield K_0. If $\mathcal{H}(R) = 1$, then $|\mathcal{C}^2| = |\mathcal{I}(\mathcal{C}_0)| = 2^{-\mathcal{T}}\mathcal{H}_0$, where $\mathcal{T} \in \{0,1\}$, and $\mathcal{H}_0 = |\mathcal{C}_0|$.*

PROOF. $(\mathcal{A}^* : \mathcal{AP}) \leq (\mathcal{I} : \mathcal{AP}) = \mathcal{H}(R) = 1$. Also, $\mathcal{H}(R) = 1$ implies that $\mathcal{G} \subset \mathcal{P}$. So $\mathcal{GP} = \mathcal{P}$ and $(\mathcal{E} : \mathcal{E} \cap \mathcal{GP}) = (\mathcal{E} : \mathcal{E} \cap \mathcal{P}) = |\mathcal{I}(\mathcal{C}_0)| = 2^{-\mathcal{T}}\mathcal{H}_0$ with $\mathcal{T} \in \{0,1\}$. Finally, consider $(\mathcal{E} : \mathcal{E} \cap \mathcal{SP})$. Let $XR \in \mathcal{E}, X \in \mathcal{I}_0$. Since $N : \mathcal{C} \to \mathcal{C}_0$ is surjective, there exists $Y \in \mathcal{I}$ such that $N(Y)\mathcal{P}_0 = X\mathcal{P}_0$. So $(XR)\mathcal{P} = Y^{1+\sigma}\mathcal{P} = (Y^\sigma)^2 Y^{1-\sigma}\mathcal{P} \in \mathcal{SGP} \subset \mathcal{SP}$. Thus, $\mathcal{E} \subset \mathcal{SP}$ and $(\mathcal{E} : \mathcal{E} \cap \mathcal{SP}) = 1$. □

COROLLARY 2. *Suppose K is a* CM-*field with maximal totally real subfield K_0. If $|\mathcal{C}^2| = 1$, then $\mathcal{H}(R) = 2^{q-s-t}\mathcal{H}_0$, where $(N(K) \cap U_0 : U_0^2) = 2^q$, $(N(U) : U_0^2) = 2^s$ and $t \in \{0,1\}$.*

PROOF. The evaluation $(\mathcal{A}^* : \mathcal{AP}) = 2^{q-s}$ can be extracted from [**5**]. $|\mathcal{C}^2| = 1$ implies that $\mathcal{SP} = \mathcal{P}$ and hence $(\mathcal{E} : \mathcal{E} \cap \mathcal{SP}) = (\mathcal{E} : \mathcal{E} \cap \mathcal{P}) = |i(\mathcal{C}_0)| = 2^{-t}\mathcal{H}_0, t \in \{0,1\}$. Finally, consider $XR \in \mathcal{E}, X \in \mathcal{I}_0$. Since $N : \mathcal{C} \to \mathcal{C}_0$ is surjective, there exists $Y \in \mathcal{I}$ such that $N(Y\mathcal{P}) = N(Y)\mathcal{P}_0 = X\mathcal{P}_0$. So $(XR)\mathcal{P} = (N(Y)R)\mathcal{P} = Y^{1+\sigma}\mathcal{P}$. Since $|\mathcal{C}^2| = 1, Y^{1+\sigma}\mathcal{P} = Y^{1-\sigma}\mathcal{P} \in \mathcal{GP}$. Hence, $\mathcal{E} \subset \mathcal{GP}$ and $(\mathcal{E} : \mathcal{E} \cap \mathcal{GP}) = 1$.
□

REFERENCES

1. S. Chowla, *An extension of Heilbronn's class number theorem,* Quart. J. Math., Oxford Ser. **5** (1934), 304-307.

2. A.G. Earnest, *Exponents of the class groups of imaginary abelian number fields,* Bull. Austral. Math. Soc. **35** (1987), 231-246.

3. ——— and D.R. Estes, *Class groups in the genus and spinor genus of binary quadratic lattices,* Proc. London Math. Soc. **40** (1980), 40-52.

4. ——— and O.H. Körner, *On ideal class groups of* 2-*power exponent,* Proc. Amer. Math. Soc. **86** (1982),196-198.

5. H. Hasse, *Bericht über neuere Untersuchungen und Probleme aus der Theorie der algebraischen Zahlkörpern,* Teil I, Ia, 2 Aufl., Würzburg-Wien, 1965.

6. O.H. Körner, *Class numbers of binary quadratic lattices over algebraic number fields,* Acta Arith. **39** (1981), 269-279.

7. M. Peters, *Class numbers of maximal binary lattices over totally real number fields,* Arch. Math. **30** (1978), 398-399.

8. H. Pfeuffer, *Darstellungsmasse binärer quadratischer Formen über totalreelen algebraischen Zahlkörpern,* Acta Arith. **34** (1978), 103-111.

9. ———, *On a conjecture about class numbers of totally positive quadratic forms in totally real algebraic number fields,* J. Number Theory **11** (1979), 188-196.

10. J.M. Shyr, *Class numbers of totally positive binary forms over totally real number fields,* Bull. Amer. Math. Soc. **83** (1977), 286-288.

11. K. Uchida, *Class numbers of imaginary abelian number fields,* I, Tôhoku Math. J. **23** (1971), 97-104.

12. L.C. Washington, *Introduction to Cyclotomic Fields,* Springer-Verlag, New York-Heidelberg-Berlin, 1982.

DEPARTMENT OF MATHEMATICS, SOUTHERN ILLINOIS UNIVERSITY, CARBONDALE, IL 62901