ACTA ARITHMETICA
XXXIX (1981)

Class numbers of binary quadratic lattices over algebraic number fields

by

O. KÖRNER (Ulm)

1. Introduction. In the sequel we shall use the terminology of O'Meara's book [6]. Additional concepts will be explained. Let F be an algebraic number field, $\mathfrak{o}$ its ring of integers and V a 2-dimensional regular quadratic space over F with the quadratic map Q. After scaling V suitably we may assume that $1 \in Q(V)$. Then V is isometric to its second Clifford algebra C^+ viewed as the quadratic space over F whose quadratic map equals the norm map $C^+ \to F$ (see [2], § 5, 1.). Therefore we may identify V with C^+. The structure of the commutative F-algebra C^+ is given by the following data: After embedding, F is a subalgebra of C^+, and C^+ has an F-basis of the form $1, \omega$, where $\omega^2 = -dV$ and 1 is the identity of F and C^+ (see [2]). Hence, if V is anisotropic, C^+ may be identified with the number field $F' = F(\sqrt{-dV})$. Let L be a lattice on V with respect to $\mathfrak{o}$ and denote by $h^+(L)$ the number of proper classes in the genus $\operatorname{gen} L$ of L. Apparently $h^+(L)$ does not change when V is scaled. For the case where F is totally real, V totally positive definite and L maximal Pfeuffer [8] and Shyr [9] independently found the formula:

$$h^+(L) = \frac{w'h'}{2^r(U' : U)h}. \tag{1}$$

Here w', h', U' denote the number of roots of unity, the class number and the group of units of F' respectively, and h, U are the class number and the group of units of F respectively, and r is the number of discrete spots of F which ramify in F'. Pfeuffer's proof of (1) essentially consists of computing the local densities in Siegel's formula [10] for the mass $m(L)$ of $\operatorname{gen} L$. Shyr uses an equivalent analytical device, namely the Tamagawa number of algebraic tori. Recently Peters [7] pointed out an arithmetical proof of (1) which is rather simple and rests essentially on the fact that the maximal lattices on V are just the fractional ideals of F' and that consequently the number of their similarity genera is explicitly known from the theory of quadratic field extensions [4]. It is the purpose of the

present paper to show that this arithmetical approach can be extended so that it yields a generalization of (1) to arbitrary F, V and L. As is customary and quite natural in the case of an arbitrary L, we interprete L as a proper ideal of a certain $\mathfrak{o}$-order $M = M_L$ of the algebra C^+ (see definitions in 2.). Let $\mathfrak{o}'$ be the maximal $\mathfrak{o}$-order of C^+. By simple group theoretical arguments Earnest and Estes [1] proved that

$$h^+(L) = h^+(M) \tag{2}$$

and that $h^+(M)/h^+(\mathfrak{o}')$ is essentially the product of indices of certain local unit groups in C^+. Modifying their method slightly we show that the indices can be replaced by indices of analogous groups in the local completions of C^+ (see Lemma 3). The latter indices can be computed explicitly by means of the results [5] on integral representations by binary quadratic forms over local fields. Since $h^+(\mathfrak{o}')$ can be evaluated by Peters' method, $h^+(L)$ is obtained in the desired shape (see Theorem 2); in particular, the fact that $h^+(L)$ depends only on F, dV and $\mathfrak{v}L(\mathfrak{n}L)^{-2}$ (which follows already from (2)) becomes more transparent. Of course, for the case where F is the field of rational numbers, the result for $h^+(L)$ is classical and due to Gauss, Dirichlet and Dedekind. At the end of this paper we shall indicate, for the sake of completeness, how the formula obtained for $h^+(L)$ can also be deduced from Pfeuffer's evaluation of $m(L)$ for the case where F is totally real, V totally positive definite, but L not necessarily maximal. The latter approach to $h^+(L)$ does not seem as natural, since there the relevance of the invariant $\mathfrak{v}L(\mathfrak{n}L)^{-2}$ can be exhibited only after some lengthy computations.

2. Notations, definitions and known consequences. According to the introduction we have $V = C^+$, i.e. V is simultaneously a quadratic space and an F-algebra. By σ we denote the non-trivial automorphism of the F-algebra V, i.e. $(a+b\omega)^\sigma = a-b\omega$ for all $a, b \in F$. Then the norm map and the trace map $V \to F$ are given by $Q(x) = xx^\sigma$ and $T(x) = x+x^\sigma$ ($x \in V$). Hence the bilinear form B of V associated with the quadratic map Q is

$$B(x, y) = \tfrac{1}{2}T(xy^\sigma) \quad (x, y \in V). \tag{3}$$

The anisotropic elements of V are just the units of the ring V, hence their set V_0 is an abelian group with respect to multiplication in V, its subgroup $V_1 = \{y \in V \mid Q(y) = 1\}$ will be also of interest. For $y \in V_1$ we denote by τ_y the map $V \to V$, defined by $\tau_y x = yx$ ($x \in V$). Apparently τ_y belongs to the group $O^+(V)$ of rotations of V; more precisely one knows (see [2], § 5, 1.) that

$$O^+(V) = \{\tau_y \mid y \in V_1\}, \tag{4}$$

in particular the assignment $y \mapsto \tau_y$ yields the group isomorphism

$$O^+(V) \cong V_1. \tag{5}$$

Note that for (4) one only needs that F is a field of characteristic $\neq 2$.

According to [6] any discrete spot or prime ideal of F is denoted by $\mathfrak{p}$, and $V_\mathfrak{p}$ is the completion of V at $\mathfrak{p}$. For any subset S of V we denote by $S_\mathfrak{p}$ its closure in the complete metric space $V_\mathfrak{p}$. For any fractional ideal $\mathfrak{a}$ of F or $F_\mathfrak{p}$ the absolute norm is abbreviated by $N(\mathfrak{a})$. For any $\mathfrak{p}$ we put $\chi(\mathfrak{p}) = 1$, if $V \neq F'$, otherwise $\chi(\mathfrak{p}) = 1$ or $= 0$ or $= -1$ according as $\mathfrak{p}$ splits or ramifies or is inert in F'. Let $\mathfrak{d}_\mathfrak{p}(a)$ denote the quadratic defect of any $a \in F_\mathfrak{p}$. For any subgroups K, L of the additive group V the *module product* KL is defined as usual as the subgroup of V generated by the set $\{kl \mid k \in K, l \in L\}$.

By an $\mathfrak{o}$-*lattice* we understand a lattice on V with respect to $\mathfrak{o}$ (i.e. a finitely generated submodule L of the $\mathfrak{o}$-module V with $FL = V$). According to [6] the symbols $\mathfrak{n}L$, $\mathfrak{s}L$, $\mathfrak{v}L$ denote the norm, the scale and the volume of any $\mathfrak{o}$-lattice L. If K and L are $\mathfrak{o}$-lattices, then KL is an $\mathfrak{o}$-lattice with $\mathfrak{n}(KL) = (\mathfrak{n}K)(\mathfrak{n}L)$.

The *maximal* $\mathfrak{o}$-*order* $\mathfrak{o}'$ of the algebra V is defined to be the set of all $x \in V$ with $Q(x)$ and $T(x)$ in $\mathfrak{o}$. We note that $\mathfrak{o}'$ is an $\mathfrak{o}$-lattice and a subring of V with $1 \in \mathfrak{o}'$, namely in the case $V = F'$ it is the ring of integers of the number field F', and in the case $V \neq F'$, i.e. $-dV \in \dot{F}^2$, we may assume that $-dV = 1$, putting $\eta = (\omega+1)/2$ we obtain because of $\eta^2 = \eta$, $\eta\eta^\sigma = 0$, $\eta+\eta^\sigma = 1$ a decomposition of the identity into orthogonal idempotents, hence

$$V = \eta F + \eta^\sigma F, \tag{6}$$

i.e. the algebra V as direct sum of the two fields ηF, $\eta^\sigma F$ both isomorphic to F, and then

$$\mathfrak{o}' = \eta\mathfrak{o} + \eta^\sigma\mathfrak{o} \tag{7}$$

as the direct sum of the two rings $\eta\mathfrak{o}$, $\eta^\sigma\mathfrak{o}$ both isomorphic to $\mathfrak{o}$. By an $\mathfrak{o}$-*order* we understand any $\mathfrak{o}$-lattice M which is a subring of $\mathfrak{o}'$ with $1 \in M$. For example, for any $\mathfrak{o}$-lattice L the set

$$M_L = \{x \in V \mid xL \subseteq L\}$$

is an $\mathfrak{o}$-order. All $\mathfrak{o}$-orders M are obtained this way, since $M = M_M$. An $\mathfrak{o}$-lattice L is called an *ideal* of an $\mathfrak{o}$-order M, if $M_L \supseteq M$. Such an ideal L is called *proper*, if $M_L = M$, it is called *invertible*, if $KL = M$ for some ideal K of M, and then K is also invertible and uniquely determined by L. Apparently every invertible ideal of M is a proper ideal of M. The converse of this statement is also true, but not as trivial (see [1]). Therefore the

set I_M of all proper ideals of M is an abelian group with respect to module multiplication. All $\mathfrak{o}$-orders and their proper ideals are characterized by (see [1]):

LEMMA 1. *An $\mathfrak{o}$-lattice M is an $\mathfrak{o}$-order if and only if*

$$M = \mathfrak{o} + \mathfrak{c}\mathfrak{o}' \quad (\textit{Symbol: } \mathfrak{c} = \mathfrak{c}(M)) \tag{8}$$

for some integral ideal $\mathfrak{c}$ of F, and then

$$\mathfrak{o}M = \mathfrak{c}^2\mathfrak{o}\mathfrak{o}'. \tag{9}$$

An $\mathfrak{o}$-lattice L is a proper ideal of an $\mathfrak{o}$-order M if and only if

$$\mathfrak{o}L(\mathfrak{n}L)^{-2} = \mathfrak{o}M. \tag{10}$$

A consequence is the known

LEMMA 2. *An $\mathfrak{o}$-lattice L is maximal if and only if L is an ideal of $\mathfrak{o}'$.*

Proof. If L is maximal, then $\mathfrak{o}'L$ is an ideal of $\mathfrak{o}'$ with $\mathfrak{n}L = \mathfrak{n}(\mathfrak{o}'L)$, $L \subseteq \mathfrak{o}'L$, hence $L = \mathfrak{o}'L$ because of the maximality. Conversely, if L is an ideal of $\mathfrak{o}'$, then there is a maximal $\mathfrak{o}$-lattice L^* with $\mathfrak{n}L = \mathfrak{n}L^*$, $L \subseteq L^*$ (see [6], 82: 18), hence by (10): $\mathfrak{o}L(\mathfrak{n}L)^{-2} = \mathfrak{o}\mathfrak{o}' \supseteq \mathfrak{o}M_{L^*} = \mathfrak{o}L^*(\mathfrak{n}L^*)^{-2}$, hence $\mathfrak{o}L \supseteq \mathfrak{o}L^*$, hence $L = L^*$. ∎

For later applications of (9) we note that

$$\mathfrak{o}\mathfrak{o}' = \tfrac{1}{4}D_{F'/F} \quad \text{or} \quad = \tfrac{1}{4}\mathfrak{o} \tag{11}$$

according as $V = F'$ or not. Here $D_{F'/F}$ denotes the discriminant of the field extension F'/F; namely for any $\mathfrak{p}$ and any $\mathfrak{o}_\mathfrak{p}$-basis x_1, x_2 of $\mathfrak{o}'_\mathfrak{p}$ we have $(\mathfrak{o}\mathfrak{o}')_\mathfrak{p} = \mathfrak{o}_\mathfrak{p} \det(B(x_i, x_k))$, hence (11) from (3) and (7).

Whereas in the case $V = F'$ the group $I_{\mathfrak{o}'}$ equals the group of fractional ideals of the number field F', we have in the case $V \neq F'$ from (6) and (7):

$$I_{\mathfrak{o}'} = \{\eta\mathfrak{a} + \eta^\sigma\mathfrak{b} \mid \mathfrak{a}, \mathfrak{b} \in I(F)\}, \tag{12}$$

where $I(F)$ denotes the group of fractional ideals of F.

For any $\mathfrak{o}$-order M we denote by $U(M)$ the group of units of the ring M, and we put $E(M) = U(M) \cap V_1$ and $U' = U(\mathfrak{o}')$, $E' = E(\mathfrak{o}')$. For any $\mathfrak{o}$-lattice L the isomorphism (5) induces the isomorphism

$$O^+(L) \cong E(M_L). \tag{13}$$

3. Groups of genera. It follows from (4) that for any $\mathfrak{o}$-lattice L:

$$\mathrm{cls}^+L = \{xL \mid x \in V_1\} \tag{14}$$

and (see [6], 81: 14):

$$\mathrm{gen}L = \Big\{\bigcap_\mathfrak{p}(V \cap x_\mathfrak{p}L_\mathfrak{p}) \mid x_\mathfrak{p} \in V_1(\mathfrak{p})\forall\mathfrak{p};\ x_\mathfrak{p} = 1 \text{ for almost all } \mathfrak{p}\Big\}, \tag{15}$$

where $V_1(\mathfrak{p}) = \{x \in V_\mathfrak{p} \mid Q(x) = 1\}$. For any $\mathfrak{o}$-order M we infer from (10), (14) and (15) that $\mathrm{gen}\,M$ is a subgroup of I_M and cls^+M a subgroup of $\mathrm{gen}\,M$ and that $\mathrm{gen}L = L\,\mathrm{gen}\,M$ for every proper ideal L of M. This implies in view of $h^+(M) = (\mathrm{gen}\,M : \mathrm{cls}^+M)$ that (2) holds.

Denote by $U(M_\mathfrak{p})$ the group of units of the ring $M_\mathfrak{p}$ for any $\mathfrak{p}$ and put $E(M_\mathfrak{p}) = U(M_\mathfrak{p}) \cap V_1(\mathfrak{p})$.

LEMMA 3. *If M is any $\mathfrak{o}$-order, then*

$$h^+(M)\big(E' : E(M)\big) = h^+(\mathfrak{o}') \prod_{\mathfrak{p}\mid\mathfrak{c}(M)} \big(E(\mathfrak{o}'_\mathfrak{p}) : E(M_\mathfrak{p})\big).$$

Proof. Via (14) and (15) we see that the map f: $\mathrm{gen}\,M \to \mathrm{gen}\,\mathfrak{o}'$, defined by $L \mapsto \mathfrak{o}'L$, is an epimorphism of groups, taking cls^+M onto $\mathrm{cls}^+\mathfrak{o}'$. Therefore f induces an epimorphism g: $\mathrm{gen}\,M/\mathrm{cls}^+M \to \mathrm{gen}\,\mathfrak{o}'/\mathrm{cls}^+\mathfrak{o}'$, and the kernels $\ker(f)$ and $\ker(g)$ of f and g satisfy

$$\ker(g) \cong \ker(f)/\big(\ker(f) \cap \mathrm{cls}^+M\big). \tag{16}$$

In view of (15) we have

$$\ker(f) = \Big\{\bigcap_\mathfrak{p}(V \cap x_\mathfrak{p}M_\mathfrak{p}) \mid x_\mathfrak{p} \in E(\mathfrak{o}'_\mathfrak{p})\forall\mathfrak{p}\Big\}. \tag{17}$$

In (17) we may suppose that always $x_\mathfrak{p} = 1$ for $\mathfrak{p} \nmid \mathfrak{c}(M)$, since $M_\mathfrak{p} = \mathfrak{o}'_\mathfrak{p}$ for such $\mathfrak{p}$ because of (8). Therefore the map $\prod_{\mathfrak{p}\mid\mathfrak{c}(M)} E(\mathfrak{o}'_\mathfrak{p}) \to \ker(f)$, defined by

$$\prod_{\mathfrak{p}\mid\mathfrak{c}(M)} x_\mathfrak{p} \mapsto \bigcap_\mathfrak{p}(V \cap x_\mathfrak{p}M_\mathfrak{p}) \quad \text{with} \quad x_\mathfrak{p} = 1 \text{ for } \mathfrak{p} \nmid \mathfrak{c}(M),$$

is an epimorphism whose kernel equals $\prod_{\mathfrak{p}\mid\mathfrak{c}(M)} E(M_\mathfrak{p})$, hence

$$\ker(f) \cong \prod_{\mathfrak{p}\mid\mathfrak{c}(M)} E(\mathfrak{o}'_\mathfrak{p})/E(M_\mathfrak{p}). \tag{18}$$

(Here $\prod$ means the direct product for groups.) Furthermore we obtain from (17) and (14) that $\ker(f) \cap \mathrm{cls}^+M = \{xM \mid x \in E'\}$, hence the map $E' \to \ker(f) \cap \mathrm{cls}^+M$, defined by $x \mapsto xM$, is an epimorphism whose kernel equals $E(M)$, consequently

$$\ker(f) \cap \mathrm{cls}^+M \cong E'/E(M). \tag{19}$$

Since $h^+(M) = \big(\ker(g) : 1\big)h^+(\mathfrak{o}')$, the assertion of Lemma 3 follows from (16), (18) and (19). ∎

4. The evaluation of $h^+(\mathfrak{o}')$. The aim of this section is

THEOREM 1. *If L is any maximal $\mathfrak{o}$-lattice, then $h^+(L) = h^+(\mathfrak{o}')$ and*

$$h^+(\mathfrak{o}') = \frac{2^{n_1+n_2+1-r-u}h'}{(U' : UE')h} \quad \textit{or} \quad = h$$

according as $-dV \notin \dot{F}^2$ *or* $\in \dot{F}^2$. *Here* n_1, n_2, u *denote for* F *respectively the number of real archimedian spots, the number of complex archimedian spots and the number of those real archimedian spots at which* dV *is positive. Furthermore,* $E' = \{x \in U' |\ xx^\sigma = 1\}$.

Remark. If F is totally real and V totally positive definite, Theorem 1 immediately reduces to (1), namely then $n_1 = u$, $n_2 = 0$ and $(E' : 1) < \infty$ because of $E' \cong O^+(\mathfrak{o}')$ (see (13)), hence E' is the group of all roots of unity in F', hence

$$(U' : UE') = (U' : U)/(UE' : U) = (U' : U)/(E' : E' \cap U) = (U' : U)2/w'.$$

The relation $h^+(L) = h^+(\mathfrak{o}')$ is clear from Lemma 2 and (2). Furthermore from Lemma 2 and [6], 102 : 3 we know that for every $L \in I_{\mathfrak{o}'}$:

$$\operatorname{gen} L = \{K \in I_{\mathfrak{o}'} |\ \mathfrak{n}K = \mathfrak{n}L\}. \tag{20}$$

Now the case $-dV \in \dot{F}^2$ of Theorem 1 can be settled as follows: From (12) and (20) we infer that $\operatorname{gen}\mathfrak{o}' = \{\eta\mathfrak{a} + \eta^\sigma\mathfrak{a}^{-1} |\ \mathfrak{a} \in I(F)\}$. Since by (4) and (6) any two lattices $\eta\mathfrak{a} + \eta^\sigma\mathfrak{a}^{-1}$ and $\eta\mathfrak{b} + \eta^\sigma\mathfrak{b}^{-1}$ with $\mathfrak{a}, \mathfrak{b} \in I(F)$ are properly isometric if and only if $\mathfrak{a} = c\mathfrak{b}$ for some $c \in \dot{F}$, we obtain $h^+(\mathfrak{o}') = h$.

Therefore in the remainder of this section we may assume that $V = F'$. Any two $\mathfrak{o}$-lattices K, L are called *similar* or in the same *similarity class*, if $K = xL$ for some $x \in V_0$. The *similarity genus* $\overline{\operatorname{gen} L}$ of L is defined to be the set of all $\mathfrak{o}$-lattices which are similar to at least one lattice from $\operatorname{gen} L$. From (20) it follows for every $L \in I_{\mathfrak{o}'}$ that

$$\overline{\operatorname{gen} L} = \{K \in I_{\mathfrak{o}'} |\ \mathfrak{n}K = Q(x)\mathfrak{n}L \text{ for some } x \in V_0\}. \tag{21}$$

In particular, $\overline{\operatorname{gen}\mathfrak{o}'}$ is a subgroup of $I_{\mathfrak{o}'}$, and the similarity class H of $\mathfrak{o}'$ is a subgroup of $\overline{\operatorname{gen}\mathfrak{o}'}$ and just the group of principal ideals of F', furthermore $\overline{\operatorname{gen} L} = L\overline{\operatorname{gen}\mathfrak{o}'}$ for all $L \in I_{\mathfrak{o}'}$. Now h' is the number of similarity classes in $I_{\mathfrak{o}'}$. Therefore, if $\bar{h}$ denotes the number of similarity classes in $\overline{\operatorname{gen}\mathfrak{o}'}$ and $\bar{g}$ the number of similarity genera in $I_{\mathfrak{o}'}$, we obtain

$$\bar{h} = h'/\bar{g}. \tag{22}$$

Lemma 4. *With the abbreviation* $V_U = \{x \in V |\ Q(x) \in U\}$ *the relation* $h^+(\mathfrak{o}') = (V_U : U'V_1)\bar{h}$ *holds.*

Proof. Let $\{A_i |\ i \in I\}$ be any complete system of representatives for the similarity classes in $\overline{\operatorname{gen}\mathfrak{o}'}$. After replacing A_i by a suitable similar lattice, we may assume that each A_i is in $\operatorname{gen}\mathfrak{o}'$. Now take any complete system $\{x_j |\ j \in J\}$ of representatives for the cosets of $U'V_1$ in the group V_U (viewed as subgroup of V_0). From (4) and (20) it follows easily that $\{x_jA_i |\ j \in J,\ i \in I\}$ is a complete system of representatives for the proper classes in $\operatorname{gen}\mathfrak{o}'$, hence $h^+(\mathfrak{o}') = (V_U : U'V_1)\bar{h}$. ∎

It remains to compute $\bar{g}$. By its definition and (21) we have

$$\bar{g} = (I_{\mathfrak{o}'} : G), \tag{23}$$

where $G = \{L \in I_{\mathfrak{o}'} |\ \mathfrak{n}L = \mathfrak{n}P \text{ for some } P \in H\}$. Since $\mathfrak{n}L$ equals the norm of the fractional ideal L of F' relative to F for any $L \in I_{\mathfrak{o}'}$, the theory of quadratic extensions of algebraic number fields yields (see [4], § 13, Satz 13):

$$(I_{\mathfrak{o}'} : G) = h\big(Q(V_U) : U^2\big)2^{r+u-n_1-n_2-1}. \tag{24}$$

The consideration of the epimorphism $V_U \to Q(V_U)$, defined by $x \mapsto Q(x)$, with the kernel V_1 shows that

$$\big(Q(V_U) : U^2\big) = (V_U : UV_1). \tag{25}$$

From Lemma 4 and (22)–(25) it follows that

$$h^+(\mathfrak{o}') = 2^{n_1+n_2+1-r-u}h'/\big(h(U'V_1 : UV_1)\big).$$

Since $(U'V_1 : UV_1) = (U' : U' \cap UV_1) = \big(U' : U(U' \cap V_1)\big) = (U' : UE')$, the proof of Theorem 1 is finished.

5. The general case. According to (2), Lemma 3 and Theorem 1 it suffices to compute the index

$$i(M, \mathfrak{p}) = \big(E(\mathfrak{o}'_\mathfrak{p}) : E(M_\mathfrak{p})\big),$$

where M is any $\mathfrak{o}$-order and $\mathfrak{p} | \mathfrak{c}(M)$. Since the epimorphism $U(\mathfrak{o}'_\mathfrak{p}) \to Q\big(U(\mathfrak{o}'_\mathfrak{p})\big)$, defined by $x \mapsto Q(x)$, has the kernel $E(\mathfrak{o}'_\mathfrak{p})$, we obtain

$$i(M, \mathfrak{p}) = \big(U(\mathfrak{o}'_\mathfrak{p}) : U(M_\mathfrak{p})\big)/\big(Q\big(U(\mathfrak{o}'_\mathfrak{p})\big) : Q\big(U(M_\mathfrak{p})\big)\big). \tag{26}$$

Consider the subgroup $U_1(M_\mathfrak{p}) = \{x \in \mathfrak{o}'^*_\mathfrak{p} |\ x \equiv 1 \bmod \mathfrak{c}(M)\mathfrak{o}'_\mathfrak{p}\}$ of $U(M_\mathfrak{p})$. Then

$$\big(U(\mathfrak{o}'_\mathfrak{p}) : U(M_\mathfrak{p})\big) = \big(U(\mathfrak{o}'_\mathfrak{p}) : U_1(M_\mathfrak{p})\big)/\big(U(M_\mathfrak{p}) : U_1(M_\mathfrak{p})\big). \tag{27}$$

In view of (8) we have

$$\big(U(M_\mathfrak{p}) : U_1(M_\mathfrak{p})\big) = N\big(\mathfrak{c}(M)_\mathfrak{p}\big)\big(1 - N(\mathfrak{p})^{-1}\big). \tag{28}$$

Furthermore, in the case $V \neq F'$ it follows from (7) that

$$\big(U(\mathfrak{o}'_\mathfrak{p}) : U_1(M_\mathfrak{p})\big) = \big(N\big(\mathfrak{c}(M)_\mathfrak{p}\big)\big(1 - N(\mathfrak{p})^{-1}\big)\big)^2, \tag{29}$$

and in the case $V = F'$ algebraic number theory also shows that

$$\big(U(\mathfrak{o}'_\mathfrak{p}) : U_1(M_\mathfrak{p})\big) = N\big(\mathfrak{c}(M)_\mathfrak{p}\big)^2 \prod_\mathfrak{P} \big(1 - \mathfrak{N}(\mathfrak{P})^{-1}\big), \tag{30}$$

where $\mathfrak{P}$ runs over all discrete spots of F' with $\mathfrak{P} | \mathfrak{p}$, and $\mathfrak{N}(\mathfrak{P})$ denotes the absolute norm of $\mathfrak{P}$. Since

$$\prod_\mathfrak{P} \big(1 - \mathfrak{N}(\mathfrak{P})^{-1}\big) = \big(1 - N(\mathfrak{p})^{-1}\big)\big(1 - \chi(\mathfrak{p})N(\mathfrak{p})^{-1}\big),$$

we obtain from (27)–(30) for all cases:

$$(31)\qquad \big(U(\mathfrak{o}_\mathfrak{p}') : U(M_\mathfrak{p})\big) = N\big(\mathfrak{c}(M)_\mathfrak{p}\big)\big(1-\chi(\mathfrak{p})N(\mathfrak{p})^{-1}\big).$$

LEMMA 5. *Let $\mathfrak{u}_\mathfrak{p}$ be the group of units of the ring $\mathfrak{o}_\mathfrak{p}$ and put*

$$(32)\qquad \psi(M,\mathfrak{p}) = \begin{cases} \operatorname{ord}_\mathfrak{p}\mathfrak{v}M, & \text{if } \operatorname{ord}_\mathfrak{p}\mathfrak{v}M \text{ is odd},\\ \min\left\{\operatorname{ord}_\mathfrak{p}\left(\dfrac{\mathfrak{v}M}{dV}\mathfrak{d}_\mathfrak{p}(-dV)\right),\ \tfrac{1}{2}\operatorname{ord}_\mathfrak{p}(4\mathfrak{v}M)\right\}, & \text{otherwise.}\end{cases}$$

Then

$$(33)\qquad Q\big(U(M_\mathfrak{p})\big) = Q(V_\mathfrak{p})\cap \mathfrak{u}_\mathfrak{p}^2\big(1+\mathfrak{p}^{\psi(M,\mathfrak{p})}\big).$$

Proof. Note that $Q\big(U(M_\mathfrak{p})\big) = Q(M_\mathfrak{p})\cap\mathfrak{u}_\mathfrak{p}$ and that $\psi(M,\mathfrak{p})>0$, since $\mathfrak{p}|\mathfrak{c}(M)$. Therefore (33) is a special case of Theorem 1 in [5], if $\mathfrak{p}$ is dyadic. If $\mathfrak{p}$ is non-dyadic, then for any $a\in\mathfrak{u}_\mathfrak{p}$ we have $a\in Q(M_\mathfrak{p})$ if and only if $\langle a\rangle \perp \langle a^{-1}dM_\mathfrak{p}\rangle \cong M_\mathfrak{p}$, hence Lemma 2 of [5] implies (33). ∎

LEMMA 6. *The relation $Q\big(U(\mathfrak{o}_\mathfrak{p}')\big) = Q(V_\mathfrak{p})\cap\mathfrak{u}_\mathfrak{p}$ holds.*

Proof. Again note that $Q\big(U(\mathfrak{o}_\mathfrak{p}')\big) = Q(\mathfrak{o}_\mathfrak{p}')\cap\mathfrak{u}_\mathfrak{p}$. Take any $a\in Q(V_\mathfrak{p})\cap\mathfrak{u}_\mathfrak{p}$. Then there exists a lattice K on $V_\mathfrak{p}$ (with respect to $\mathfrak{o}_\mathfrak{p}$) with $\mathfrak{n}K=\mathfrak{o}_\mathfrak{p}$ and $a\in Q(K)$. By [6], 82 : 18 we may assume K to be maximal. By Lemma 2 and [6], § 82 K, the lattice $\mathfrak{o}_\mathfrak{p}'$ on $V_\mathfrak{p}$ is also maximal, hence $\mathfrak{o}_\mathfrak{p}'\cong K$ by [6], 91 : 2, hence $a\in Q(\mathfrak{o}_\mathfrak{p}')$. ∎

From the Lemmas 5 and 6 we obtain with the abbreviation $\mathfrak{u}_\mathfrak{p}(M) = 1+\mathfrak{p}^{\psi(M,\mathfrak{p})}$ because of $\mathfrak{u}_\mathfrak{p}^2\subseteq Q(V_\mathfrak{p})\cap\mathfrak{u}_\mathfrak{p}$ that

$$\begin{aligned}(34)\qquad &\big(Q\big(U(\mathfrak{o}_\mathfrak{p}')\big) : Q\big(U(M_\mathfrak{p})\big)\big)\\ &= \big(\big(Q(V_\mathfrak{p})\cap\mathfrak{u}_\mathfrak{p}\big)\mathfrak{u}_\mathfrak{p}^2\mathfrak{u}_\mathfrak{p}(M) : \mathfrak{u}_\mathfrak{p}^2\mathfrak{u}_\mathfrak{p}(M)\big)\\ &= \big(\big(Q(V_\mathfrak{p})\cap\mathfrak{u}_\mathfrak{p}\big)\mathfrak{u}_\mathfrak{p}(M) : \mathfrak{u}_\mathfrak{p}^2\mathfrak{u}_\mathfrak{p}(M)\big)\\ &= \frac{\big(\mathfrak{u}_\mathfrak{p} : \mathfrak{u}_\mathfrak{p}^2\mathfrak{u}_\mathfrak{p}(M)\big)\big(\big(Q(V_\mathfrak{p})\cap\mathfrak{u}_\mathfrak{p}\big)\mathfrak{u}_\mathfrak{p}(M) : \big(Q(V_\mathfrak{p})\cap\mathfrak{u}_\mathfrak{p}\big)\big)}{\big(\mathfrak{u}_\mathfrak{p} : \big(Q(V_\mathfrak{p})\cap\mathfrak{u}_\mathfrak{p}\big)\big)}\\ &= a(M,\mathfrak{p})b(M,\mathfrak{p})/c(M,\mathfrak{p}),\end{aligned}$$

where

$$\begin{aligned} a(M,\mathfrak{p}) &= \big(\big(\mathfrak{u}_\mathfrak{p}/\mathfrak{u}_\mathfrak{p}(M)\big) : \big(\mathfrak{u}_\mathfrak{p}/\mathfrak{u}_\mathfrak{p}(M)\big)^2\big),\\ b(M,\mathfrak{p}) &= \big(\mathfrak{u}_\mathfrak{p}(M) : \big(\mathfrak{u}_\mathfrak{p}(M)\cap Q(V_\mathfrak{p})\big)\big),\\ c(M,\mathfrak{p}) &= \big(\mathfrak{u}_\mathfrak{p} : \big(\mathfrak{u}_\mathfrak{p}\cap Q(V_\mathfrak{p})\big)\big).\end{aligned}$$

From the structure of the group $\mathfrak{u}_\mathfrak{p}/(1+\mathfrak{p}^l)$ for $l>0$, as determined in algebraic number theory ([3], page 236), we know that

$$(35)\qquad a(M,\mathfrak{p}) = N(\mathfrak{p})^{[\psi(M,\mathfrak{p})/2]} \quad\text{or}\quad = 2N(\mathfrak{p})^{\operatorname{ord}_\mathfrak{p}2}$$

according as $\psi(M,\mathfrak{p})\leqslant \operatorname{ord}_\mathfrak{p}4$ or not. For $x\in\dot F_\mathfrak{p}$ put $k(x) = \left(\dfrac{x,\ -dV}{\mathfrak{p}}\right)$.

Consider the homomorphisms $\mathfrak{u}_\mathfrak{p}\to\{1,-1\}$ and $\mathfrak{u}_\mathfrak{p}(M)\to\{1,-1\}$ of multiplicative groups, defined by $x\mapsto k(x)$. The kernels are $\mathfrak{u}_\mathfrak{p}\cap Q(V_\mathfrak{p})$ and $\mathfrak{u}_\mathfrak{p}(M)\cap Q(V_\mathfrak{p})$. Therefore $c(M,\mathfrak{p})=1$ or 2 according as $k(x)=1$ for all $x\in\mathfrak{u}_\mathfrak{p}$ or not; and $b(M,\mathfrak{p})=1$ or 2 according as $k(x)=1$ for all $x\in\mathfrak{u}_\mathfrak{p}(M)$ or not. If $V\neq F'$, then obviously $c(M,\mathfrak{p})=b(M,\mathfrak{p})=1$. Now the case $V=F'$ remains.

(a) Let $\mathfrak{p}$ be unramified in F'. Then $\operatorname{ord}_\mathfrak{p}dV$ is even and $\mathfrak{d}_\mathfrak{p}(-dV)\subseteq 4\mathfrak{o}_\mathfrak{p}dV$. Therefore by [6], 63 : 11a and the Local Square Theorem: $c(M,\mathfrak{p}) = b(M,\mathfrak{p}) = 1$.

(b) Let $\mathfrak{p}$ be ramified in F' and $\operatorname{ord}_\mathfrak{p}dV$ be even. Then $\mathfrak{p}$ is dyadic and $\mathfrak{d}_\mathfrak{p}(-dV)\supset 4\mathfrak{o}_\mathfrak{p}dV$. Therefore $c(M,\mathfrak{p})=2$ by Lemma 1 of [5], and that lemma implies also that $b(M,\mathfrak{p})=1$ or 2 according as $\mathfrak{d}_\mathfrak{p}(-dV)\mathfrak{p}^{\psi(M,\mathfrak{p})}\subset 4\mathfrak{o}_\mathfrak{p}dV$ or not.

(c) Let $\mathfrak{p}$ be ramified in F' and $\operatorname{ord}_\mathfrak{p}dV$ be odd. Then by [6], 63 : 11a we have $k(\Delta)=-1$ for every $\Delta\in\mathfrak{u}_\mathfrak{p}$ with $\mathfrak{d}_\mathfrak{p}(\Delta)=4\mathfrak{o}_\mathfrak{p}$. Therefore $c(M,\mathfrak{p})=2$. If $\psi(M,\mathfrak{p})>\operatorname{ord}_\mathfrak{p}4$, then $\mathfrak{u}_\mathfrak{p}(M)\subseteq\mathfrak{u}_\mathfrak{p}^2$ by the Local Square Theorem, hence $b(M,\mathfrak{p})=1$. If $\psi(M,\mathfrak{p})\leqslant\operatorname{ord}_\mathfrak{p}4$, then there exists a $\Delta\in\mathfrak{u}_\mathfrak{p}(M)$ with $\mathfrak{d}_\mathfrak{p}(\Delta)=4\mathfrak{o}_\mathfrak{p}$, hence $b(M,\mathfrak{p})=2$.

Collecting the results (26), (31), (34), (35) and (a)–(c), inserting these in Lemma 3 and observing (2) and Lemma 1, we arrive at

THEOREM 2. *Let L be any $\mathfrak{o}$-lattice and $M=M_L$. Then*

$$h^+(L) = \frac{h^+(\mathfrak{o}')N\big(\mathfrak{c}(M)\big)}{\big(E' : E(M)\big)}\prod_{\mathfrak{p}|\mathfrak{c}(M)}\frac{e(M,\mathfrak{p})}{a(M,\mathfrak{p})}\left(1-\frac{\chi(\mathfrak{p})}{N(\mathfrak{p})}\right).$$

Here $h^+(\mathfrak{o}')$ is given by Theorem 1, and $\mathfrak{c}(M)$ is the integral ideal and $\mathfrak{v}M$ the fractional ideal of F determined by $\mathfrak{c}^2(M)\mathfrak{v}\mathfrak{o}' = \mathfrak{v}M = \mathfrak{v}L(\mathfrak{n}L)^{-2}$, and $\mathfrak{v}\mathfrak{o}'$ is given by (11), *and $a(M,\mathfrak{p})$ by* (35), *and $\psi(M,\mathfrak{p})$ by* (32). *$e(M,\mathfrak{p})=2$, if all of the following conditions are satisfied: $-dV\notin\dot F^2$, $\mathfrak{p}$ ramifies in F', either $2|\operatorname{ord}_\mathfrak{p}dV$, $\mathfrak{d}_\mathfrak{p}(-dV)\mathfrak{p}^{\psi(M,\mathfrak{p})}\subset 4\mathfrak{o}_\mathfrak{p}dV$ or $2\nmid\operatorname{ord}_\mathfrak{p}dV$, $\psi(M,\mathfrak{p})>\operatorname{ord}_\mathfrak{p}4$. In all other cases $e(M,\mathfrak{p})=1$.*

Remarks. (a) In the case $-dV\notin\dot F^2$ it follows from (8) that

$$E(M) = \{x\in\mathfrak{o}+\mathfrak{c}(M)\mathfrak{o}' \mid Q(x)=1\}.$$

(b) In the case $-dV\in\dot F^2$ it follows from (7) and (8) that

$$E(M) = \{\eta u+\eta^\sigma u^{-1} \mid u\in U,\ u^2\equiv 1 \bmod \mathfrak{c}(M)\},$$

hence

$$\big(E' : E(M)\big) = \big(U : U_1(M)\big), \text{ where } U_1(M) = \{u\in U \mid u^2\equiv 1 \bmod \mathfrak{c}(M)\}.$$

(c) In the case where F is totally real and V totally positive definite Theorem 1 yields

$$\frac{h^+(\mathfrak{o}')}{\big(E' : E(M)\big)} = \frac{\big(E(M) : 1\big)h'}{2^r(U' : U)h}.$$

In the special case considered in the last remark we want to indicate now how $h^+(L)$ can also be obtained from Pfeuffer's evaluation of $m(L)$. Since by (13) and Lemma 1 we have $O^+(K) \cong E(M)$ for all $K \in \operatorname{gen} L$, the definition of $m(L)$ implies

$$h^+(L) = 2\big(E(M):1\big)m(L). \tag{36}$$

For later evaluation we use

LEMMA 7. *If* $\mathfrak{p}$ *is dyadic, then the weight* $\mathfrak{w}L_\mathfrak{p}$ *of* $L_\mathfrak{p}$ *satisfies*

$$\mathfrak{w}L_\mathfrak{p} = \mathfrak{d}_\mathfrak{p}(-dL_\mathfrak{p})(\mathfrak{n}L_\mathfrak{p})^{-1} + 2\mathfrak{s}L_\mathfrak{p}. \tag{37}$$

Proof. (a) Let $L_\mathfrak{p}$ be modular. Then $\mathfrak{d}_\mathfrak{p}(-dL_\mathfrak{p}) \subseteq (\mathfrak{n}L_\mathfrak{p})(\mathfrak{w}L_\mathfrak{p})$ by [6], 93:17. Therefore (37) is clear, if $\mathfrak{w}L_\mathfrak{p} = 2\mathfrak{s}L_\mathfrak{p}$. If $\mathfrak{w}L_\mathfrak{p} \neq 2\mathfrak{s}L_\mathfrak{p}$, then $\mathfrak{w}L_\mathfrak{p} \supset 2\mathfrak{s}L_\mathfrak{p}$ by the definition of the weight, hence $\mathfrak{d}_\mathfrak{p}(-dL_\mathfrak{p}) = (\mathfrak{n}L_\mathfrak{p})(\mathfrak{w}L_\mathfrak{p})$ by [6], 93:17 and 93:10, hence (37) follows.

(b) Let $L_\mathfrak{p}$ be non-modular, then $L_\mathfrak{p} \cong \langle a\rangle \perp \langle b\rangle$ with $a, b \in F_\mathfrak{p}$, $a\mathfrak{o}_\mathfrak{p} = \mathfrak{n}L_\mathfrak{p}$, hence by [6], § 94: $\mathfrak{w}L_\mathfrak{p} = a\mathfrak{d}_\mathfrak{p}(b/a) + 2\mathfrak{s}L_\mathfrak{p}$. This implies (37). ∎

Inserting Pfeuffer's formula [8] for $m(L)$ into (36) yields $h^+(L)$ in a form almost as explicit as in Theorem 2. The essential difference lies in the appearance of the additional genus invariants $\mathfrak{w}L_\mathfrak{p}$ at those dyadic spots $\mathfrak{p}$ where $L_\mathfrak{p}$ is modular. Now, expressing $\mathfrak{w}L_\mathfrak{p}$ in the form (37) and using $\mathfrak{d}_\mathfrak{p}(-dL_\mathfrak{p}) = (\mathfrak{v}L)\mathfrak{d}_\mathfrak{p}(-dV)/dV$ leads, after some easy, though lengthy calculations, to the shape of $h^+(L)$ as formulated in Theorem 2.

References

[1] A. G. Earnest and D. R. Estes, *Class groups in the genus and spinor genus of binary quadratic lattices*, Proc. London Math. Soc., 3 ser., 40 (1980), pp. 40–52.

[2] M. Eichler, *Quadratische Formen und orthogonale Gruppen*, Berlin–Göttingen–Heidelberg 1952.

[3] H. Hasse, *Zahlentheorie*, 2nd ed., Berlin 1963.

[4] — *Bericht über neuere Untersuchungen und Probleme aus der Theorie der algebraischen Zahlkörper*, Teil I, Ia, 2nd ed., Würzburg–Wien 1965.

[5] O. Körner, *Integral representations over local fields and the number of genera of quadratic forms*, Acta Arith. 24 (1973), pp. 301–311.

[6] O. T. O'Meara, *Introduction to Quadratic Forms*, Berlin–Göttingen–Heidelberg 1963.

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

[8] H. Pfeuffer, *Darstellungsmaße binärer quadratischer Formen über totalreellen algebraischen Zahlkörpern*, Acta Arith. 34 (1978), pp. 103–111.

[9] J. M. Shyr, *Class numbers of totally positive binary forms over totally real number fields*, Bull. Amer. Math. Soc. 83 (1977), pp. 286–288.

[10] C. L. Siegel, *Über die analytische Theorie der quadratischen Formen III*, Ann. of Math. 38 (1937), pp. 212–291.

ABTEILUNG FÜR MATHEMATIK IV DER UNIVERSITÄT ULM, GFR

Received on 25. 11. 1978
and in revised form on 8. 2. 1979 (1117)