GENUS CHARACTER L-FUNCTIONS OF QUADRATIC ORDERS AND MAXIMAL ORDERS OF MATRIX ALGEBRAS

TOMOYOSHI IBUKIYAMA

Abstract. For a quadratic extension K of $\mathbb{Q}$, we consider orders O in K that are not necessarily maximal and the ideal class group $Cl^+(O)$ in the narrow sense of proper ideals of O. Characters of $Cl^+(O)$ of order at most two are traditionally called genus characters. Explicit description of such characters is known classically, but explicit L-functions associated to those characters are only recently obtained partially by Chinta and Offen and completely by Kaneko and Mizuno. As remarked in the latter paper, the present author also obtained the formula of such L-functions independently. Indeed, here we will give a simple and transparent alternative proof of the formula by rewriting explicit genus characters and their values in an adelic way starting from scratch. We also add an explicit formula for the genus number in the wide sense, which is maybe known but rarely treated. As an appendix we give an ideal-theoretic characterization of isomorphism classes of maximal orders of the matrix algebras $M_n(F)$ over a number field F up to $GL_n(F)$ and $GL_n^+(F)$ conjugation respectively, and apply genus numbers to count them when $n = 2$ and F is quadratic. Relations between classes and genera of ideals and quadratic forms are explained in the appendix. To avoid any misconception, we include some easy known details.

1. Introduction

The purpose of the paper is to give an alternative proof of the formula for the genus character L-functions associated with not necessarily maximal orders of quadratic fields, and to give a simple survey on the related genus theory. Such formulas for L-functions are given only recently in [5] except for some cases and in [12] for all the cases. As pointed out in the introduction of [12], the present author also gave an alternative proof of the formula independently (Theorem 4.3 in this paper). To give our proof, we describe proper ideals of non-maximal quadratic orders, their genus characters, and their values at ideals all explicitly in an adelic way. A global description of such objects is a classical result (see for example [6] or [18]). Anyway, this paper is

2020 *Mathematics Subject Classification.* 11R11, 11R37, 11R42.

This work was supported by JSPS Kakenhi Grant Number JP19K03424, JP23K03031 and JP20H00115.

more or less expository in nature, and our new point here is to treat everything adelically. This allows us to avoid the very complicated calculations in [12] and gives a simple group theoretic explanation. Almost from scratch except for an easy part of the class field theory, we give explicit formulas of genus characters and L-functions associated with it. Siegel described the genus theory for maximal quadratic orders completely in [17] in global language, including concrete description of genus characters and their values at ideals. Our method would give more transparent view to the whole theory including the case of non-maximal orders. When the quadratic order is not maximal, we do not know any reference treating this subject in this way, so we believe it is not useless to publish this. For readers' convenience, we add an appendix on relations between classes and genera of ideals and quadratic forms. (This is more or less well known but references would be rare. Also the definition of a genus of binary quadratic forms in the wide sense given here would be new.) We also add a formula for the genus number in the wide sense, which has application to conjugacy classes of maximal orders of 2×2 matrix algebras. Indeed in section 6, for general n and algebraic number fields F, we consider ideal theoretic characterization of the number of maximal orders of $M_n(F)$ up to $GL_n(F)$ conjugation and $GL_n^+(F)$ conjugation, where $GL_n^+(F)$ means those with totally positive determinants. The result for $GL_n(F)$ conjugation has been known in [2].

The paper is outlined as follows. In the next section, we review the theory of genus of cyclic extensions K of $\mathbb{Q}$ for orders O of K not necessarily maximal. This is a minor generalization of [11], where the case of maximal orders is treated. In section 3, we assume that K is quadratic, and explicitly describe proper ideals of non-maximal orders, the adelic subgroup corresponding to the genus, and genus characters. Then we give formulas of values of genus characters at ideals. In section 4, we give an explicit formula of L-functions associated to genus characters (see Theorem 4.3). In section 5, we give a formula for the genus number in the wide sense. In section 6, we give a general theory on the number of maximal orders of the matrix algebras over an algebraic number field. In case of a quadratic field K, we give an application of the genus numbers in the wide sense and in the narrow sense to the number of $GL_2(K)$ and $GL_2^+(K)$ conjugacy classes of maximal orders in $M_2(K)$. In section 7, we explain relations between the genus of ideals and the genus of binary quadratic forms.

For a history of the genus of quadratic forms and ideals, see [6], [18], [3] or [1] for example. In fact, this paper would be read as an appendix to (the Japanese version of) [1], where everything was treated globally. For some old history of the genus theory, see [15], and further generalization of the notion of the genus, see [9] and the references there.

2. Definition of a genus for cyclic extensions over $\mathbb{Q}$

Our main concern is a quadratic order, but in this section we review the genus theory of cyclic extensions of $\mathbb{Q}$ based on [11], since it would make our points clearer. Here the only difference from [11] is that we describe the theory for orders O not necessarily maximal. For reader's convenience, we repeat some arguments there.

Let V be any finite dimensional vector space over $\mathbb{Q}$. A free $\mathbb{Z}$ submodule L of V is said to be a lattice if it contains a basis of V over $\mathbb{Q}$. When K is an algebraic number field, regarding K as a vector space over $\mathbb{Q}$, a subring O of K that contains 1 and is a lattice of K is called an order of K. It is clear that any element of O is an algebraic integer, so $O \subset O_{max}$, where O_{max} is the maximal order of K. While O_{max} is a Dedekind domain, the order $O \subsetneqq O_{max}$ is not Dedekind since it is not integrally closed. So there is no prime ideal decomposition of ideals of O. Besides, for an ideal $\mathfrak{a}$ of O, there is no inverse ideal in general. This means that if we want to define ideal classes, we must restrict ideals to a smaller set of ideals of O. According to the usual habit, a lattice L of K with $OL \subset L$ is called a fractional ideal of O. If $L \subset O$ besides, we say that L is an integral ideal, or just an ideal of O. We write $V_p = V \otimes_{\mathbb{Q}} \mathbb{Q}_p$ for any prime p where $\mathbb{Q}_p$ is the field of p-adic numbers. For any submodule L of V and a prime p, we write $L_p = L \otimes_{\mathbb{Z}} \mathbb{Z}_p \subset V_p$, where $\mathbb{Z}_p$ is the ring of p-adic integers.

Definition 2.1. *We say that a fractional ideal $\mathfrak{a}$ of O is locally principal if $\mathfrak{a}_p = O_p a_p$ for some $a_p \in K_p$ for every prime p.*

Here we note that $K_p = K \otimes_{\mathbb{Q}} \mathbb{Q}_p$ is a direct sum of fields according to the decomposition of p in K and not a field in general. The ring O_p is not necessarily decomposed into a direct sum of orders of the fields, and it is not suitable to consider each place of K over p separately when O is not maximal. The relation between $\mathfrak{a}$ and the collection of $\mathfrak{a}_p$ for any p is given by the proposition given below. Any $\mathbb{Z}_p$ submodule L of V_p is called a lattice of V_p if $L = \mathbb{Z}_p\omega_1 + \cdots + \mathbb{Z}_p\omega_n$ for some basis $\{\omega_1, \ldots, \omega_n\}$ of V_p over $\mathbb{Q}_p$.

Proposition 2.2. *Notation being as above, let $\{N_p\}_{p:prime}$ be a family of lattices in V_p and L be a lattice in V. Assume that $L_p = N_p$ for almost all p. Then there exists a lattice M in V such that $N_p = M \otimes_{\mathbb{Z}} \mathbb{Z}_p$ and*

$$M = \bigcap_{p:prime} (V \cap N_p).$$

For the proof, see Weil [19] p.84 Theorem 2.

We denote by $K_A^\times$ the group of ideles of K. For any element $a = (a_v) \in K_A^\times$, we may define a locally principal fractional ideal $\mathfrak{a}$ of O by

$$\mathfrak{a} = \bigcap_{p:prime} (a_p O_p \cap K), \qquad (a_p = (a_v)_{v|p} \in K_p).$$

So locally principal fractional ideals correspond with $K_{A,fin}^{\times}/\prod_p O_p^{\times}$, where $K_{A,fin}^{\times}$ is the finite part of the ideles, i.e. the group of ideles whose components at infinite places are all 1. For a locally principal fractional ideal $\mathfrak{a}$ of O as above, we may define an inverse ideal by

$$\mathfrak{a}^{-1} = \bigcap_{p:prime} (a_p^{-1} O_p \cap K).$$

Then we have $\mathfrak{a}\mathfrak{a}^{-1} = O$ and locally principal fractional ideals of O form a group. We say that locally principal fractional ideals $\mathfrak{a}$ and $\mathfrak{b}$ are equivalent in the wide sense if $\mathfrak{b} = \mathfrak{a}\alpha$ for some $\alpha \in K^{\times}$. Equivalence in the narrow sense is defined by imposing a condition that $\alpha \in K_+^{\times}$, where K_+ is the set of totally positive elements α of K, that is, α is positive under embeddings of K into the real field at all infinite real places and no condition at complex places. We denote by $Cl(O)$ (resp. $Cl^+(O)$) the group of classes of locally principal fractional ideals in the wide sense (resp. in the narrow sense). We will mainly consider $Cl^+(O)$. As usual, $K^{\times}$ is diagonally embedded in $K_A^{\times}$, and we denote the image by the same letter $K^{\times}$. Let r_1 and r_2 be the number of real places and complex places of K, respectively. We put

$$U_{\infty} = (\mathbb{R}^{\times})^{r_1} \times (\mathbb{C}^{\times})^{r_2} \text{ and } U_{\infty,+} = (\mathbb{R}_+^{\times})^{r_1} \times (\mathbb{C}^{\times})^{r_2},$$

where $\mathbb{R}_+^{\times}$ is the set of positive real numbers. (If $K/\mathbb{Q}$ is Galois, we have $r_2 = 0$ if $K \subset \mathbb{R}$ and $r_1 = 0$ if not.) We put $U(O) = U_{\infty} \prod_{p:prime} O_p^{\times}$ and $U_+(O) = U_{\infty,+} \prod_{p:prime} O_p^{\times}$. Then we have

$$Cl(O) \cong K_A^{\times}/K^{\times}U(O),$$
$$Cl^+(O) \cong K_A^{\times}/K^{\times}U_+(O) \cong U_{\infty,+}K_{A,fin}/K_+^{\times}U_+(O).$$

The last isomorphism comes from the fact that K contains elements of any signature at infinite places.

Here we shortly review the class field theory over $\mathbb{Q}$.

Lemma 2.3 (Class field theory)**.** *The set of finite abelian extensions K of $\mathbb{Q}$ in the algebraic closure of $\mathbb{Q}$ is bijective to the set of finite index subgroups H of $\mathbb{Q}_A^{\times}$ containing $\mathbb{Q}^{\times}$. Here, denoting by $N_{K/\mathbb{Q}}$ the norm from K to $\mathbb{Q}$ and by $Gal(K/\mathbb{Q})$ the Galois group of K over $\mathbb{Q}$, the correspondence is given by*

$$H = \mathbb{Q}^{\times} N_{K/\mathbb{Q}}(K_A^{\times}), \qquad Gal(K/\mathbb{Q}) \cong \mathbb{Q}_A^{\times}/H.$$

The following direct product decomposition is well known and easy to see.

$$\mathbb{Q}_A^{\times} = \mathbb{Q}^{\times} \times \mathbb{R}_+^{\times} \times \prod_{p:prime} \mathbb{Z}_p^{\times}. \tag{1}$$

The Galois group of the maximal abelian extension of $\mathbb{Q}$ (that is, the union of all cyclotomic fields) is given by $\prod_p \mathbb{Z}_p^{\times} = \varprojlim_N (\mathbb{Z}/N\mathbb{Z})^{\times}$. The

relation of this fact to the class field theory is as follows. By the direct product (1), we see that any H in the lemma can be written as

$$H = \mathbb{Q}^\times \times (\mathbb{R}_+^\times \times H_0), \qquad H_0 \subset \prod_{p:prime} \mathbb{Z}_p^\times.$$

Then we see that

$$\mathbb{Q}_A^\times / H \cong \left(\prod_p \mathbb{Z}_p^\times \right) / H_0.$$

Of course H_0 is in general bigger than $\prod_{p:prime}(H_0 \cap \mathbb{Z}_p^\times)$, where $\mathbb{Z}_p^\times$ is identified with the subset of $\mathbb{Q}_A^\times$ whose components at places $v \neq p$ are all 1 while components at p are in $\mathbb{Z}_p^\times$. If we write

$$e_p = [\mathbb{Z}_p^\times ; \mathbb{Z}_p^\times \cap H_0],$$

then e_p is the ramification index of p in K. Indeed, for $a \in \mathbb{Q}^\times N_{K/\mathbb{Q}}(K_A^\times)$ written as $a = cu_\infty u_0$ with $c \in \mathbb{Q}^\times$, $u_\infty \in \mathbb{R}_+^\times$ and $u_0 = (u_{0,q}) \in H_0$, assume that $u_{0,q} = 1$ unless $q \neq p$. Denote by θ the reciprocity map of $\mathbb{Q}_A^\times$ to $Gal(K/\mathbb{Q})$. Then we have $\theta(b) = \prod_v \theta_v(b_v)$ for any $b = (b_v) \in \mathbb{Q}^\times$, where θ_v is the reciprocity map from $\mathbb{Q}_v^\times$ to $Gal(K_w/\mathbb{Q}_v)$ for any place w of K over a place v. So we have $\theta(u_0) = \theta_p(u_{0,p})$. But since $\theta(a) = \theta(c) = \theta(u_\infty) = 1$ by definition, we have $\theta_p(u_{0,p}) = 1$. This means $u_{0,p} \in N_{K_\mathfrak{p}/\mathbb{Q}_p}(K_v^\times)$ where $\mathfrak{p}$ is any prime of K over p. So $e_p = [\mathbb{Z}_p^\times : \mathbb{Z}_p^\times \cap N_{K_\mathfrak{p}/\mathbb{Q}_p}(K_\mathfrak{p}^\times)]$. Here $e_p = 1$ for almost all p.

In particular, if K is cyclic over $\mathbb{Q}$, then $[K : \mathbb{Q}]$ is the least common multiple n of e_p defined above. Indeed, take a character χ_K of $\prod_q \mathbb{Z}_q^\times$ such that $Ker(\chi_K) = H_0$. If we decompose χ_K as $\chi_K = \prod_p \chi_{K,p}$ by characters $\chi_{K,p}$ on $\mathbb{Z}_q^\times / (\mathbb{Z}_q^\times \cap H_0)$, then $\chi_{K,p}$ is of order e_p, and the order of χ_K is n.

From here until the end of this section, we assume that K is a cyclic extension of $\mathbb{Q}$. We fix a generator σ of $Gal(K/\mathbb{Q})$. For an order O of K which is not necessarily maximal, we put

$$U_+(O) = U_{\infty,+} \prod_p O_p^\times.$$

To define a genus of O, we prepare the following proposition.

Proposition 2.4. *Notation being as above, for $a \in K_A^\times$, the following conditions (1) and (2) are equivalent.*
(1) $N_{K/\mathbb{Q}}(a) \in \mathbb{Q}^\times N_{K/\mathbb{Q}}(U_+(O))$.
(2) There exists $b \in K_A^\times$, $u \in U_+(O)$ and $c \in K^\times$ such that

$$a = b^{1-\sigma} uc.$$

Proof. This is essentially Theorem 3 in [11] except for the point that we do not assume that O is maximal. It is trivial that (2) implies (1). So we prove (2) assuming (1). First of all, we give an idelic version of Hilbert Satz 90 stated as follows:

For any $a \in K_A^\times$ with $N_{K/\mathbb{Q}}(a) = 1$, there exists $b \in K_A^\times$ such that $a = b^{1-\sigma}$.

This is claimed in [11] without proof, so we give here a proof. We have $K_p = F \oplus \cdots \oplus F$ for some field F over $\mathbb{Q}_p$ (isomorphic to the completion of K at any place of K over p). Let $\mathfrak{p}$ be a prime ideal in K over p and $\tau = \sigma^m$ a generator the decomposition group of $\mathfrak{p}$. Each component of K_p corresponds with the embedding associated to $\mathfrak{p}^{\sigma^i}$ with some $i \in \{0, \ldots, m-1\}$. For $x = (x_1, \ldots, x_m) \in F^m = K_p$, we may regard

$$x^\sigma = (x_m^\tau, x_1, x_2 \ldots, x_{m-1}).$$

So we have

$$x^{1-\sigma} = (x_1/x_m^\tau, x_2/x_1, \ldots, x_m/x_{m-1}).$$

For $y = (y_1, \ldots, y_m) \in F^m = K_p$, we have

$$N_{K/\mathbb{Q}}(y) = N_{F/\mathbb{Q}}(y_1 \cdots y_m).$$

The condition that

$$y = x^{1-\sigma}$$

is

$$y_1 = x_1/x_m^\tau, \quad y_2 = x_2/x_1, \quad \ldots, \quad y_m = x_m/x_{m-1},$$

so $y_1 \cdots y_m = x_m^{1-\tau}$. Since we assumed $N_{K/\mathbb{Q}}(y) = N_{F/\mathbb{Q}}(y_1 \cdots y_m) = 1$, there exists $x_0 \in F^\times$ such that $y_1 \cdots y_m = x_0^{1-\tau}$ by the usual Hilbert Satz 90 for cyclic extensions. If we put $x_m = x_0$ and define x_i inductively by $x_i = x_{i+1} y_{i+1}^{-1}$ for any $1 \leq i \leq m-1$, then for $x = (x_1, \ldots, x_m)$, we have $y = x^{1-\sigma}$. Now we must show that x is in $K_A^\times$. For almost all primes p, we have $O_p = O_{max,p}$ and p is unramified in K. For such p, any element of the maximal order O_F of F is written as $x_0 = p^e \epsilon$ for some $\epsilon \in O_F^\times$. Since $x_0^{1-\tau} = \epsilon^{1-\tau}$, we may take $x_0 = \epsilon$. By definition of ideles, we have $y_i \in O_F^\times$ for almost all p, so $x_i = x_{i+1} y_{i+1}^{-1}$ is also in $O_F^\times$. So for almost all p, we may assume $y = x^{1-\sigma}$ for $x \in O_p^\times$. This means that for any $a \in K_A^\times$ with $N_{K/\mathbb{Q}}(a) = 1$, we have $a = b^{1-\sigma}$ for some $b \in K_A^\times$. So the idelic version of Satz 90 is proved. Now assume (1) in Proposition for $a \in K_A^\times$. Then we have $N_{K/\mathbb{Q}}(au^{-1}) \in \mathbb{Q}^\times$ for some $u \in U_+(O)$. For a cyclic extension, by the Hasse norm theorem, an element of $\mathbb{Q}$ is a local norm if and only if it is a global norm (e.g. [11] quoted [4]), so we have $c \in K^\times$ such that $N_{K/\mathbb{Q}}(au^{-1}c^{-1}) = 1$. So we have $au^{-1}c^{-1} = b^{1-\sigma}$ for some $b \in K_A^\times$. □

Definition 2.5. *The subgroup of $H(O)$ of elements of $K_A^\times$ that satisfy (1) and (2) in Proposition 2.4 is said to be a principal genus of O. A coset in $K_A^\times / H(O)$ is called a genus of O. We call the number of these cosets a genus number in the narrow sense.*

More classical explanation is given as follows. As we have explained, we have

$$Cl^+(O) \cong K_A^\times / K^\times U_+(O) \cong U_{\infty,+} K_{A,fin}^\times / K_+^\times U_+(O).$$

Here by definition we have

$$K^\times U_+(O) \subset H(O) \subset K_A^\times,$$

so $H(O)/K^\times U_+(O)$ is a subgroup of $Cl^+(O) \cong K_A^\times/K^\times U_+(O)$. Elements in this subgroup are called the "principal genus classes" in the narrow sense and a genus is a coset of ideal classes in the narrow sense divided by these classes. (When K is quadratic, obviously the principal genus classes consists of square classes by the condition (2) above. The purpose of Proposition 2.4 is to compare the condition (1) with the classical setting. For non-cyclic extensions, only the condition (1) is often used for the definition of the principal genus classes. See for example [9].) A character of the group $K_A^\times/K^\times U_+(O) \cong Cl^+(O)$ which is trivial on $H(O)/K^\times U_+(O)$ is called a genus character.

If we consider the map

$$K_A^\times \overset{N_{K/\mathbb{Q}}}{\longrightarrow} \mathbb{Q}_A^\times \longrightarrow \mathbb{Q}_A^\times/\mathbb{Q}^\times,$$

then since $K/\mathbb{Q}$ is cyclic, the kernel is $K^\times$. So we see that

$$K_A^\times/H(O) \cong (K_A^\times/K^\times)/(H(O)/K^\times) \cong \mathbb{Q}^\times N_{K/\mathbb{Q}}(K_A^\times)/\mathbb{Q}^\times N_{K/\mathbb{Q}}(U_+(O)).$$

So the genus number g of O in the narrow sense is given by

$$\begin{aligned} g &= [K_A^\times : H(O)] = [\mathbb{Q}^\times N_{K/\mathbb{Q}}(K_A^\times) : \mathbb{Q}^\times N_{K/\mathbb{Q}}(U_+(O))] \\ &= [\mathbb{Q}_A^\times : \mathbb{Q}^\times N_{K/\mathbb{Q}}(U_+(O)]/[\mathbb{Q}_A^\times : \mathbb{Q}^\times N_{K/\mathbb{Q}}(K_A^\times)]. \end{aligned}$$

By the class field theory we have

$$[\mathbb{Q}_A^\times : \mathbb{Q}^\times N_{K/\mathbb{Q}}(K_A^\times)] = [K : \mathbb{Q}].$$

On the other hand, we have

$$[\mathbb{Q}_A^\times : \mathbb{Q}^\times N_{K/\mathbb{Q}}(U_+(O))] = \prod_p [\mathbb{Z}_p^\times : N_{K/\mathbb{Q}}(O_p^\times)].$$

So writing $e_p = [\mathbb{Z}_p^\times : N_{K/\mathbb{Q}}(O_p^\times)]$, we have

$$g = \left(\prod_p e_p\right)/[K : \mathbb{Q}].$$

Here since O might not be maximal, e_p might not be the ramification index of $K/\mathbb{Q}$. The abelian extension of $\mathbb{Q}$ corresponding to $\mathbb{Q}^\times N_{K/\mathbb{Q}}(U_+(O))$ by the class field theory is called the genus field of $H(O)$.

We denote by $X(O)$ the set of characters ϕ of $\prod_p \mathbb{Z}_p^\times$ such that the p component ϕ_p is a character of $\mathbb{Z}_p^\times/N_{K/\mathbb{Q}}(O_p^\times)$. We can naturally prolong ϕ to the character of $\mathbb{Q}_A^\times$ by setting so that it is trivial on $\mathbb{Q}^\times \times \mathbb{R}_+^\times$. Now we denote by χ_K one of non-trivial characters of $\mathbb{Q}_A^\times$ trivial on $\mathbb{Q}^\times N_{K/\mathbb{Q}}(K_A^\times)$. This is called a character corresponding to $K/\mathbb{Q}$. Of course this is trivial on $\mathbb{Q}^\times \times \mathbb{R}_+^\times$, so it can be regarded as a character of $\prod_p \mathbb{Z}_p^\times$. Then the p component $\chi_{K,p}$ of χ_K on $\mathbb{Z}_p^\times$ is

a character of $\mathbb{Z}_p^\times/N_{K/\mathbb{Q}}(O_{max,p}^\times)$. Since $O_p^\times \subset O_{max,p}^\times$, the character $\chi_{K,p}$ can be regarded as a character of $\mathbb{Z}_p^\times/N_{K/\mathbb{Q}}(O_p^\times)$ and we have $\chi_K \in X(O)$. If χ is a genus character of O, then the value $\chi(a)$ for $a \in K_A^\times$ depends only on $\mathbb{Q}^\times N_{K/\mathbb{Q}}(a)$, and (any power of) χ_K is trivial on the latter elements. So genus characters of O corresponds bijectively with

$$X(O)/\{\chi_K^i; 0 \leq i \leq n-1\}, \qquad n = [K:\mathbb{Q}].$$

For a genus character χ of O corresponding to $\phi \in X(O)$ and $a = (a_p) \in K_A^\times$ with $a_p = (a_v)_{v|p}$ such that $N(a) \in \mathbb{R}_+^\times \prod_p \mathbb{Z}_p^\times$, we have $\chi(a) = \phi(N(a)) = \prod_p \phi_p(N(a_p))$ by definition. But in general, $N(a)$ belongs to $\mathbb{R}_+^\times \prod_p \mathbb{Z}_p^\times$ only after multiplying an element of $\mathbb{Q}^\times$, and in order to give exact values of $\chi(a)$, we need this kind of adjustment. When K is a quadratic field, we will describe $X(O)$ and the values of genus characters χ on ideals more precisely in the next section.

3. Explicit genus characters for quadratic orders

In the rest of the paper except for section 6, we assume that K is a quadratic extension of $\mathbb{Q}$ and denote the norm $N_{K/\mathbb{Q}}$ and the trace $Tr_{K/\mathbb{Q}}$ from K to $\mathbb{Q}$ by N and Tr, respectively. The notation N is also used for the norm $N(\mathfrak{a})$ of an ideal $\mathfrak{a}$ defined to be $[O_f : \mathfrak{a}]$, but we believe no confusion is likely to happen. Assume that the maximal order of K is written as $O_{max} = \mathbb{Z} + \mathbb{Z}\omega$. Then orders O_f of K correspond bijectively to positive integers f called conductors by

$$O_f = \mathbb{Z} + \mathbb{Z}f\omega.$$

We denote by D_K the fundamental discriminant of K and we say that $D = f^2 D_K$ is the discriminant of O_f. We say that an ideal $\mathfrak{a}$ of O_f is proper if

$$\{\alpha \in K : \mathfrak{a}\alpha \subset \mathfrak{a}\} = O_f.$$

It is obvious that $\mathfrak{a}$ is proper if and only if $\mathfrak{a}_p$ is proper in $O_{f,p} = O_f \otimes_{\mathbb{Z}} \mathbb{Z}_p$ for all primes p, where the word proper is defined similarly for $O_{f,p}$. Any principal ideal is obviously proper. So any locally principal ideal $\mathfrak{a}$ of O_f is proper. Conversely we have

Lemma 3.1. *Any proper fractional ideal of O_f is locally principal.*

Proof. Though this has been proved in [10], we give a shorter proof here. We may assume that $\mathfrak{a}$ is integral. For a proper integral ideal $\mathfrak{a}$, we have integers $a > 0$, $\ell > 0$, $d \in \mathbb{Z}$ such that

$$\mathfrak{a} = \ell(\mathbb{Z}a + \mathbb{Z}(d + f\omega))$$

with $N(d + f\omega) = ac$ for some integer c ([1]). It is enough to show that $\mathfrak{a}_p = \mathbb{Z}_p a + \mathbb{Z}_p(d + f\omega)$ is principal for any prime p. If $p \nmid f$, then $O_{f,p} = O_{max,p}$ so the result is classical (even when p splits). So

we assume $p|f$. If $a \in \mathbb{Z}_p^\times$, then $\mathfrak{a}_p = O_{f,p}^\times$ so nothing to do. Next we assume $p|a$. Since

$$N(d + f\omega) = d^2 + fdTr(\omega) + f^2N(\omega) = ac.$$

and we assumed $p|a$, $p|f$, we have $p|d$. If $p|c$, then

$$(d + f\omega)(d + f\omega^\sigma)/p = a(c/p) \in \mathfrak{a} \text{ for } \sigma \in Gal(K/\mathbb{Q}) \text{ with } \sigma \neq id.$$

But since $f\omega = fTr(\omega) - f\omega^\sigma$, we have

$$(d + f\omega)/p = -(d + f\omega^\sigma)/p + 2(d/p) + (f/p)Tr(\omega)$$

with d/p, $(f/p)Tr(\omega) \in \mathbb{Z}$, so we have $(d+f\omega)(d+f\omega)/p \in \mathfrak{a}$. On the other hand we have

$$a(d + f\omega)/p = (a/p)(d + f\omega) \in \mathfrak{a}.$$

So $\mathfrak{a}(d + f\omega)/p \subset \mathfrak{a}$. But $(d/p) + (f/p)\omega \notin O_{f,p}$ so this contradicts the assumption that $\mathfrak{a}_p$ is proper. So we have $p \nmid c$. This means $a \in (d + f\omega)O_{f,p}$, so $\mathfrak{a}_p = O_{f,p}(d + f\omega)$. □

The proper ideals are important classically since they correspond nicely to the binary quadratic forms (See [1] and section 7).

The principal genus $H(O_f)$ corresponds to square classes of locally principal ideals. This can be seen as follows. In Proposition 2.4, we may assume that $a \in b^{1-\sigma}K^\times U_+(O_f)$, so a is in the same class as $b^{1-\sigma}$ in the narrow sense. We regard $\mathbb{Q}_A^\times$ as a subset of $K_A^\times$ naturally (i.e. for $v = \infty$ or rational prime, if $K_v = \mathbb{Q}_v \oplus \mathbb{Q}_v$, then we embed $\mathbb{Q}_v$ diagonally and if K_v is a field, we embed $\mathbb{Q}_v$ as a subfield.) Since

$$bb^\sigma \in \mathbb{Q}_A^\times = \mathbb{Q}^\times \mathbb{R}_+^\times \prod_p \mathbb{Z}_p^\times \subset K^\times U_+(O_f),$$

we have $b^{1-\sigma}K^\times U_+(O_f) = b^2K^\times U_+(O_f)$, so a belongs to the square classes in the narrow sense. Hence a genus is a coset of the subgroup of $Cl^+(O_f)$ consisting of square classes in the narrow sense, and genus characters are nothing but a character of $Cl^+(O_f)$ of order at most two. We will describe these characters explicitly in this section. First we describe components of $N_{K/\mathbb{Q}}(H(O_f))$ at primes. For the sake of completeness and for reader's convenience, we review easy known results concerning O_{max} for a while. By the local class field theory, if p is unramified in K, then we have $N(O_{max,p}^\times) = \mathbb{Z}_p^\times$. The following lemma is well known and easy to see.

Lemma 3.2. *(i) When p splits in K, we have $K_p = \mathbb{Q}_p \oplus \mathbb{Q}_p$ and*

$$N(K_p^\times) = \{p^n : n \in \mathbb{Z}\} \times \mathbb{Z}_p^\times.$$

(ii) When p is unramified and remains prime in K, we have

$$N(K_p^\times) = \{p^{2n}; n \in \mathbb{Z}\} \times \mathbb{Z}_p^\times.$$

(iii) If p is odd and ramified in $K = \mathbb{Q}(\sqrt{pm})$ where m is an integer such that $p \nmid m$, then

$$N(K_p^\times) = \{(-pm)^n : n \in \mathbb{Z}_p\} \times (\mathbb{Z}_p^\times)^2.$$

Here $(\mathbb{Z}_p^\times)^2$ is defined to be the set of square elements of $\mathbb{Z}_p^\times$.
(iv) If $p = 2$ is ramified in $K = \mathbb{Q}(\sqrt{m})$ for an integer m with $2 \nmid m$ (so $m \equiv 3 \bmod 4$), we have

$$N(K_2^\times) = \begin{cases} (-2)^n \times (1 + 4\mathbb{Z}_2) & \text{if } m \equiv 3 \bmod 8, \\ 2^n \times (1 + 4\mathbb{Z}_2) & \text{if } m \equiv 7 \bmod 8. \end{cases}$$

(v) If $p = 2$ is ramified in $K = \mathbb{Q}(\sqrt{2m})$ for an integer m with $2 \nmid m$, we have

$$N(K_2^\times) = \begin{cases} \{2^n : n \in \mathbb{Z}\} \times \{1 + 8\mathbb{Z}_2, -1 + 8\mathbb{Z}_2\} & \text{if } m \equiv 1 \bmod 8, \\ \{(-2)^n : n \in \mathbb{Z}\} \times \{1 + 8\mathbb{Z}_2, 3 + 8\mathbb{Z}_2\} & \text{if } m \equiv 3 \bmod 8, \\ \{6^n : n \in \mathbb{Z}\} \times \{1 + 8\mathbb{Z}_2, -1 + 8\mathbb{Z}_2\} & \text{if } m \equiv 5 \bmod 8, \\ \{2^n : n \in \mathbb{Z}\} \times \{1 + 8\mathbb{Z}_2, 3 + 8\mathbb{Z}_2\} & \text{if } m \equiv 7 \bmod 8. \end{cases}$$

So the non-trivial character χ_p of $\mathbb{Z}_p^\times / N(O_{max,p}^\times)$ is given as follows. For (i) and (ii), we have $\chi_p = 1$. For (iii), we have $\chi_p(a) = \left(\frac{a}{p}\right)$ (the quadratic residue symbol). For (iv), $\chi_2(a)$ is $\chi_{-4}(a) = \left(\frac{-4}{a}\right)$. For (v), if $m \equiv 1 \bmod 4$, then $\chi_2(a)$ is $\chi_8(a) = \left(\frac{2}{a}\right)$. For $m \equiv 3 \bmod 4$, we have $\chi_2(a)$ is $\chi_{-8}(a) = \left(\frac{-8}{a}\right)$. For each quadratic field $K/\mathbb{Q}$, the character χ of $\prod_p \mathbb{Z}_p^\times$ is defined by $\prod_p \chi_p$ by taking χ_p on $\mathbb{Z}_p^\times$ as above, and we can prolong this naturally to a character of $\mathbb{Q}_A^\times$ by using the direct product decomposition (1) of $\mathbb{Q}_A^\times$. This is nothing but the character χ_K corresponding to the quadratic extension K over $\mathbb{Q}$.

This character is also given in another way as explained below. If a fundamental discriminant δ of some quadratic field can be divided only by one prime, then we say δ is a prime discriminant. For example, for an odd prime p, if we write $p^* = (-1)^{(p-1)/2}p$, then this is the unique prime discriminant divisible by p. For $p = 2$, the prime discriminants divisible by 2 are -4, 8, -8. For each prime discriminant δ, we define a Dirichlet character $\chi_\delta(a) = \left(\frac{\delta}{a}\right)$ as usual: We put $\chi_\delta(-1) = -1$ if $\delta < 0$ and $= 1$ if $\delta > 0$. For a prime q such that $q \nmid \delta$, we put $\chi_\delta(q) = 1$ if q splits in $\mathbb{Q}(\sqrt{\delta})$, $= -1$ if q remains prime, and $= 0$ if $q|\delta$. For any integer $a = \epsilon q_1^{e_1} \cdots q_m^{e_m}$ with $\epsilon = \pm 1$ and primes q_i, we put $\chi_\delta(a) = \chi_\delta(\epsilon) \prod_{i=1}^m \chi_\delta(q_i)^{e_i}$. Any fundamental discriminant D_K of a quadratic field K is uniquely decomposed into a product of prime discriminants δ_i as $D_K = \delta_1 \cdots \delta_r$. Then for any integer a, we define

$$\chi_K(a) = \prod_{i=1}^r \chi_{\delta_i}(a) := \left(\frac{D_K}{a}\right).$$

In particular, we see that $\chi_K(-1) = 1$ if K is real and -1 if K is imaginary. We may regard χ_K as a character $\prod_p \chi_{K,p}$ of $\prod_p \mathbb{Z}_p^\times$ where

for each prime p, $\chi_{K,p}$ is the character of $\mathbb{Z}_p^\times$ already given just after Lemma 3.2. The proof is as follows. For an odd prime p and an odd prime $q \neq p$, by the quadratic reciprocity we have

$$\left(\frac{p^*}{q}\right) = \left(\frac{q}{p}\right).$$

This is true even for $q = 2$. Indeed for $p \equiv 1 \bmod 8$ and $p \equiv 5 \bmod p$, we have $\left(\frac{p}{2}\right) = 1$ and -1, respectively. For $p \equiv 3 \bmod 8$ and $7 \bmod 8$, we have $\left(\frac{-p}{2}\right) = -1$ and 1, respectively. We see that in all these cases, this is equal to $\left(\frac{2}{p}\right)$. When $p = 2$, $\chi_{K,2}$ is the same as χ_2 defined before. We can also see easily that $\prod_p \chi_{K,p}(-1) = 1$ for real K and $= -1$ for imaginary K. Of course the fact mentioned above are all classically well known. We may prolong χ_K to the character of $\mathbb{Q}_A^\times$ trivial on $\mathbb{Q}^\times \times \mathbb{R}_+^\times$. Then we have $Ker(\chi_K) = \mathbb{Q}^\times N(K_A^\times)$. In this adelic setting, calculation of the value of χ_K at an element of $\mathbb{Q}_A^\times$ not in $\prod_p \mathbb{Z}_p^\times$ is easy. For example, for a prime p with $p \nmid D_K$, put

$$[p] := (1, \ldots, 1, p, 1, \ldots, 1) \in \mathbb{Q}_A^\times,$$

where p-component is p and all the other components are 1. Then we have

$$\chi_K([p]) = \chi_K((p^{-1}, \ldots, p^{-1}, 1, p^{-1}, \ldots, p^{-1})) = \prod_{q \neq p} \chi_{K,q}(p^{-1}) = \left(\frac{D_K}{p}\right).$$

Next we consider $N(O_{f,p}^\times)$ for $p|f$. We write $D = f^2 D_K$. We denote by $\mathrm{ord}_p(f)$ the p-adic order of f.

Lemma 3.3. *Assume that $p|f$.*
(1) If p is odd, then

$$N(O_{f,p}^\times) = (\mathbb{Z}_p^\times)^2.$$

(2) If $p = 2$, then we have

$$N(O_{f,2}^\times) = \begin{cases} (i) & \mathbb{Z}_2^\times & \text{if } ord_2(f) = 1 \text{ and } D_K \text{ is odd}, \\ (ii) & 1 + 4\mathbb{Z}_2 & \text{if } ord_2(f) = 1 \text{ and } D_K \equiv 12 \bmod 16, \\ (iii) & 1 + 4\mathbb{Z}_2 & \text{if } ord_2(f) = 2 \text{ and } D_K \equiv 1 \bmod 4, \\ (iv) & 1 + 8\mathbb{Z}_2 & \text{if } D \equiv 0 \bmod 32. \end{cases}$$

The above cases exhaust all the cases, since the case (iv) is whether $ord_2(f) = 1$ and $D_K \equiv 0 \bmod 8$, $ord_2(f) = 2$ and $D_K \equiv 0 \bmod 4$, or $3 \leq ord_2(f)$.

Proof. If $p \neq 2$, then

$$N(x + yf\omega) = x^2 + xyfTr(\omega) + f^2 N(\omega) \equiv x^2 \bmod p.$$

If we put $y = 0$, we see $(\mathbb{Z}_p^\times)^2 \subset N(O_{p,f}^\times)$, so we have (1) by Hensel's lemma. Now assume $p = 2$. First of all, we note that $1 + 8\mathbb{Z}_2 = (\mathbb{Z}_2^\times)^2 \subset N(O_{f,2}^\times)$. Since $\mathbb{Z}_2^\times/(1 + 8\mathbb{Z}_2) \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, we must see how many cosets of $1 + 8\mathbb{Z}_2$ appears. In case (i), we have $O_{f,2} =$

$\mathbb{Z}_2 + \mathbb{Z}_2\sqrt{D_K}$, so $N(x + y\sqrt{D_K}) = x^2 - y^2 D_K$. So $N(O_{f,2}^\times)$ contains $-D_K$, $2^2 - D_K = 4 - D_K$. Since $D_K \equiv 1 \bmod 8$ or $5 \bmod 8$, these generate $\{1, -1, 3, -3\} \subset N(O_{f,2}^\times)$, so we have $N(O_{f,2}^\times) = \mathbb{Z}_2^\times$. In case (ii), we have $O_{f,2} = \mathbb{Z}_2 + \mathbb{Z}_2 2\sqrt{m}$ and $N(x+2y\sqrt{m}) = x^2 - 4my^2$. If this belongs to $\mathbb{Z}_2^\times$, then x should be odd. So the norm is $\equiv 1 - 4y^2 m$. This gives $1 \bmod 8$ for even y and $5 \bmod 8$ for odd y since $m \equiv 3 \bmod 4$, so (ii) is proved. In the case (iii), we have $O_{f,2} = \mathbb{Z}_2 + 2\sqrt{D_K}$ and $x^2 - 4D_K y^2 \equiv 1$ or $5 \bmod 8$. For (iv), elements of $O_{f,2}$ is written as $\mathbb{Z}_2 + \mathbb{Z}_2\sqrt{D}/2$ so $N(x + y\sqrt{D}/2) = x^2 - y^2(D/4) \equiv 1 \bmod 8$, so we prove (iv). □

In Lemma 3.3, the corresponding non-trivial character of $\mathbb{Z}_p^\times / N(O_{f,p}^\times)$ is $\left(\dfrac{p^*}{a}\right)$ for (1), trivial for (2)(i), χ_{-4} for (2)(ii) and (iii), and χ_{-4}, χ_8, χ_{-8} for (2)(iv). For a fixed discriminant $D = f^2 D_K$, a character defined as a product of several local characters of $\mathbb{Z}_p^\times / N(O_{f,p}^\times)$ appearing in Lemma 3.2 and 3.3 is equal to a character χ_δ corresponding to some fundamental discriminant δ of a divisor of $D = f^2 D_K$ such that $D/\delta \equiv 0$ or $1 \bmod 4$.

Any divisor δ of $D = f^2 D_K$ which is a fundamental discriminant of some quadratic field or 1 such that $D/\delta \equiv 0$ or $1 \bmod 4$ is called a fundamental divisor of D (Stammteiler in Weber [18]). For example, 1 and D_K are always fundamental divisors. For a fundamental divisor δ_1 of D, there exists another fundamental divisor δ_2 of D such that $\delta_1\delta_2 = f_1^2 D_K$ for some $f_1 | f$. Or equivalently we may say $D = \delta_1\delta_2 f_0^2$ for f_0 with $f_0 f_1 = f$. We say that such δ_1 and δ_2 are reciprocal. Here δ_2 is determined uniquely by δ_1. We have $\chi_{\delta_1}\chi_{\delta_2} = \chi_K$ (regarding χ_δ as the trivial character when $\delta = 1$, and taking the product so that the result becomes a primitive character, i.e. regarding the square of the same prime discriminant part as a trivial character.)

Proposition 3.4 (Weber [18])**.** *The set of reciprocal pairs of fundamental discriminants of $D = f^2 D_K$ corresponds bijectively to the set of genus characters. In particular, if we denote by ν the number of odd divisors of D, then the genus number g of O_f in the narrow sense is given as follows.*

$$g = \begin{cases} 2^{\nu-1} & \text{if } D \equiv 1 \bmod 4 \text{ or } D \equiv 4 \bmod 16, \\ 2^{\nu} & \text{if } D \equiv 8, 12, 16, 24, 28 \bmod 32, \\ 2^{\nu+1} & \text{if } D \equiv 0 \bmod 32. \end{cases}$$

Proof. Since we have

$$K_A^\times / H(O_f) \cong \mathbb{Q}^\times N(K_A^\times) / \mathbb{Q}^\times N(U_+(O_f)),$$

and $\chi_K(a) = 1$ for $a \in \mathbb{Q}^\times N(K_A^\times)$, the first part of the above proposition is obvious. The assertion on the genus number is obtained by a careful check of Lemma 3.2 and 3.3. □

A class $C \in Cl^+(O_f)$ in the narrow sense is said to be an ambig class if $C^\sigma = C$. Equivalently, this is a class C satisfying $C^2 = 1$. For such a class, we can show C contains a proper ideal $\mathfrak{a}$ such that $\mathfrak{a} = \mathfrak{a}^\sigma$. This is called an ambig ideal. Traditionally, the genus number is obtained by counting ambig ideals up to equivalence. For such proofs, see for example (the Japanese version of) [1]. (By the way, note that even if C is of order two in the wide sense, C might not contain an ambig ideal.)

Since genus characters are characters of $Cl^+(O_f)$, it is preferable to write it as a function on proper O_f ideals. We explain this below. A proper integral ideal $\mathfrak{a}$ of O_f is said to be prime to f if we have

$$\mathfrak{a} + fO_f = O_f.$$

If $\mathfrak{a}$ is prime to f, then $\mathfrak{a}$ is a proper ideal. This is equivalent to the condition that $N(\mathfrak{a})$ is prime to f. We denote by $I(O_f, f)$ the set of proper O_f ideals prime to f. It is well known that we have a bijective multiplicative mapping from $I(O_f, f)$ to $I(O_{max}, f)$ by

$$\mathfrak{a} \to \mathfrak{a}O_{max},$$

preserving norm and products (See [1]). So any ideal in $I(O_f, f)$ is uniquely decomposed into a product of prime ideals. If $\mathfrak{a}$ is a proper ideal of O_f not prime to f, then there exists $\alpha \in K_+^\times$ such that $\mathfrak{a}\alpha$ is prime to f (easily proved by the weak approximation theorem that claims K is dense in $\prod_{v \in S} K_v^\times$ for any finite set S of places of K, or see [1] for a global proof), so to give values of genus characters at ideals, it is enough to consider values at prime ideals $\mathfrak{p}$ in $I(O_f, f)$. (By the way, considering by ideles, it is clear that any proper ideal of O_f not necessarily prime to f is also decomposed uniquely to the product of ideals of O_f whose norms are powers of p. But maximal O_f ideals are not proper in general and there is no proper ideal of norm p for $p|f$. In particular, there is no prime ideal decomposition for ideals of O_f in general.)

We give a formula below how to calculate $\chi(\mathfrak{p})$ for prime ideals $\mathfrak{p} \in I(O_f, f)$ for a genus character χ. When $f = 1$, this is the same as those written in Siegel [17] II Chapter 5.

Theorem 3.5. *Let δ_1, δ_2 be a reciprocal pair of fundamental divisors and χ be a genus character associated with the pair. Then for a prime ideal $\mathfrak{p} \in I(O_f, f)$, we have the following formula.*
(1) If $\mathfrak{p}$ is unramified in K, then we have

$$\chi(\mathfrak{p}) = \chi_{\delta_1}(N(\mathfrak{p})) = \chi_{\delta_2}(N(\mathfrak{p})).$$

(2) If $\mathfrak{p}$ is ramified, then $N(\mathfrak{p})$ is prime to one of δ_i (say δ_1). Then we have

$$\chi(\mathfrak{p}) = \chi_{\delta_1}(N(\mathfrak{p})).$$

Proof. For $p \nmid f$, the prime ideal $\mathfrak{p}$ over p corresponds with an idele

$$a = (1, \ldots, 1, a_p, 1, \ldots, 1) \in K_A^\times$$

where $a_p \in K_p^\times$ is the p-th component such that $\mathfrak{p}_p = a_p O_{f,p} = a_p O_{max,p}$. The value of a genus character χ on a is determined by the value of $N(a) \in \mathbb{Q}_A^\times$ for the corresponding characters $(\chi_{\delta_1}, \chi_{\delta_2})$. When p remains prime in K, then we have $N(\mathfrak{p}) = p^2$ and $a_p = p\epsilon$ with $\epsilon \in O_{max,p}^\times$. So we have

$$N(a) = (1, \dots, 1, p^2 N(\epsilon), 1, \dots, 1) \in \mathbb{Q}_A^\times.$$

We must change this to an element of $\prod_q \mathbb{Z}_q^\times$ by multiplying an element of $\mathbb{Q}^\times$ to evaluate by the character of $\prod_q \mathbb{Z}_q^\times$. So we consider

$$p^{-2} N(a) = (p^{-2}, \dots, p^{-2}, N(\epsilon), p^{-2}, \dots, p^{-2}).$$

Since any local character is of order two at $q \neq p$ and trivial at p (since $\mathbb{Z}_p^\times = N(O_{p,f}^\times)$), we have $\chi(\mathfrak{p}) = 1$. We may write this as

$$\chi_{\delta_i}(N(\mathfrak{p})) = \chi_{\delta_i}(p^2) = 1.$$

If $\mathfrak{p}$ over p is unramified and split in K, then we have $O_{f,p} = O_{max,p} = \mathbb{Z}_p \oplus \mathbb{Z}_p$ and $a_p = (p, 1)$ or $(1, p)$. So $N(a_p) = p$. Multiplying p^{-1} to a, we have

$$p^{-1} N(a) = (p^{-1}, \dots, p^{-1}, 1, p^{-1} \dots, p^{-1}).$$

So $\chi(\mathfrak{a}) = \prod_{q \neq p} \chi_{\delta_1, q}(p^{-1}) = \chi_{\delta_1}(p^{-1})$. Since $\chi_K(p) = 1$, this is of course equal to $\chi_{\delta_2}(p^{-1})$. Since χ_{δ_i} is of order two, this is equal to $\chi_{\delta_i}(p)$. So we have $\chi(\mathfrak{p}) = \chi_{\delta_1}(N(\mathfrak{p})) = \chi_{\delta_2}(N(\mathfrak{p}))$. If $(p) = \mathfrak{p}\mathfrak{p}^\sigma$, then we also have $\chi(\mathfrak{p}^\sigma) = \chi(\mathfrak{p})$.

Finally, assume that $\mathfrak{p}$ is ramified. Then we have

$$N(a) = (1, \dots, 1, pu, 1, \dots, 1)$$

for some $u \in \mathbb{Z}_p^\times$. We have

$$p^{-1} N(a) = (p^{-1}, \dots, p^{-1}, u, p^{-1}, \dots, p^{-1}).$$

Since we assumed $p \nmid f$, one of δ_i does not contain p as a factor. Take such i (say $i = 1$). Then we have $\chi_{\delta_1, p} = 1$ so $\chi_{\delta_{1,p}}(u) = 1$ and

$$\chi(\mathfrak{p}) = \chi_{\delta_1}(p^{-1}) = \chi_{\delta_1}(p).$$

So the proof is completed. □

Remark 3.6. *(1) When p is ramified in the above proof, if we take χ_{δ_2} with $p|\delta_2$ instead, then we should have $\chi(\mathfrak{a}) = \chi_{\delta_2,p}(u) \prod_{q \neq p} \chi_{\delta_2,q}(p)$. This is the same as $\chi_{\delta_1}(p)$ since χ_K is the character that is trivial on $\mathbb{Q}^\times N(K_A^\times)$. This can be also proved directly by using Lemma 3.2.*
(2) Even when $\mathfrak{a}$ is not prime to f, we can also give some formula for $\chi(\mathfrak{a})$ by the same sort of consideration, but in this case, we cannot describe it only by $N(\mathfrak{a})$ since a value of some unit part like u for the ramified case remains. We do not go into details since it seems we cannot avoid a bit complicated case studies.

4. The L-functions of genus characters

For an order O_f of a quadratic field $K/\mathbb{Q}$, we fix a genus character χ. We define an L-function of proper ideals of O_f with character χ as

$$L(s, O_f, \chi) = \sum_{proper\ \mathfrak{a}\subset O_f} \frac{\chi(\mathfrak{a})}{N(\mathfrak{a})^s},$$

where the sum is taken over all integral proper ideals of O_f including those not prime to f. Since any proper ideal $\mathfrak{a}$ of O_f is identified with a representative $a = (a_v)$ of $K_A^\times / K^\times U_{\infty,+} \prod_p O_{f,p}^\times$ we have the unique decomposition of $\mathfrak{a}$ to the product $\mathfrak{a} = \prod_p (\mathfrak{a}_p \cap K)$ where $\mathfrak{a}_p = a_p O_{f,p}$, $a_p = (a_v)_{v|p}$. Here $N(\mathfrak{a}_p) = N(\mathfrak{a}_p \cap K)$ is a power of p. So it is clear that $L(s, O_f, \chi)$ is a product of the Euler p-factors.

The Euler p factors such that p is prime to f is simple. We see this part first. Put

$$L_f(s, O_f, \chi) = \sum_{\mathfrak{a}\in I(O_f, f)} \frac{\chi(\mathfrak{a})}{N(\mathfrak{a})^s},$$

and we will write a formula for this. Assume that χ corresponds with a reciprocal pair of fundamental divisors (δ_1, δ_2). To simplify notation, we denote the Dirichlet character χ_{δ_1}, χ_{δ_2} corresponding to δ_1 and δ_2 by ϕ and ψ. We will see the Euler p-factor for a prime p with $p \nmid f$. If p splits in K, then we have $pO_{f,p} = \mathfrak{p}_1\mathfrak{p}_2$ for some prime ideals $\mathfrak{p}_1$, $\mathfrak{p}_2$. Then by Theorem 3.5, we have $\chi(\mathfrak{p}_1) = \chi(\mathfrak{p}_2) = \phi(p) = \psi(p)$. So the Euler p factor should be

$$\frac{1}{(1-\phi(p)p^{-s})(1-\psi(p)p^{-s})}.$$

If p remain prime, then $\chi(\mathfrak{p}) = \chi(pO_{f,p}) = 1$, so the Euler factor is

$$\frac{1}{1-N(\mathfrak{p})^{-s}} = \frac{1}{1-p^{-2s}}.$$

But since $\chi_K(p) = -1$, we have $\phi(p)\psi(p) = -1$, so the Euler factor can be also written as

$$\frac{1}{(1-\phi(p)p^{-s})(1-\psi(p)p^{-s})}.$$

If p is ramified in K, then $\chi_K(p) = 0$. By definition of the character χ and the assumption $p \nmid f$, we have $\phi(p) = 0$ and $\psi(p) \neq 0$, or $\phi(p) \neq 0$ and $\psi(p) = 0$. So again the Euler p factor is

$$\frac{1}{(1-\phi(p)p^{-s})(1-\psi(p)p^{-s})}.$$

So if we write $L_f(s, \phi)$ and $L_f(s, \psi)$ the usual Dirichlet L-functions omitting the Euler p factors such that $p|f$, we have

$$L_f(s, O_f, \chi) = L_f(s, \phi)L_f(s, \psi).$$

This is well known for $f = 1$ (See Siegel [17] for example). The remaining problem is to determine the Euler p factors for $p|f$. To determine these part, we need more precise description of proper ideals of $O_{f,p}$ for $p|f$. So we fix a prime p with $p|f$. For any integer $b \geq 0$, we write

$$R_b = \mathbb{Z}_p + \mathbb{Z}_p p^b \omega$$

where $1, \omega$ is a basis over $\mathbb{Z}$ of O_{max}. This is equal to $O_{f,p}$ for any f with $ord_p(f) = b$. For a proper integral ideal $\mathfrak{a} = \alpha R_e$ of R_e, if $N(\alpha) = p^d u$ $(u \in \mathbb{Z}_p^\times)$, then we have $N(\mathfrak{a}) = N(\mathfrak{a} \cap K) = p^d$.

Lemma 4.1. *(1) If $\mathfrak{a}$ is a proper integral ideal of R_e such that $ord_p N(\mathfrak{a}) \leq 2e$, then $ord_p N(\mathfrak{a})$ is even.*
(2) Proper integral ideals $\mathfrak{a}$ of R_e such that $N(\mathfrak{a}) = p^{2c}$ with $c \leq e$ are given by $p^c \epsilon R_e$ for some $\epsilon \in R_{e-c}^\times$. The number of such ideals of R_e is equal to $[R_{e-c}^\times : R_e^\times]$.
(3) Proper integral ideals $\mathfrak{a}$ of R_e such that $N(\mathfrak{a}) = p^{2e+c}$ with $c \geq 0$ are given by $\mathfrak{a} = p^e \mathfrak{a}_0 R_e$ for integral ideals $\mathfrak{a}_0$ of $R_0 = O_{max,p}$ with $N(\mathfrak{a}_0) = p^c$. The number of such ideals of R_e is equal to $[R_0^\times : R_e^\times]$ times the number of ideals $\mathfrak{a}_0$ of R_0 with $N(\mathfrak{a}_0) = p^c$.

Proof. Since proper ideals are locally principal, we write $\mathfrak{a} = (x + yp^e\omega)R_e$. Then $N(\mathfrak{a}) = p^c$ is equivalent to $\mathrm{ord}_p N(x + yp^e\omega) = c$. We put $a = \mathrm{ord}_p(x)$. If we assume that $2e \leq c$, then $e \leq a$. Indeed if $a < e$, then

$$N(x + yp^e\omega) = x^2 + xp^e yTr(\omega) + p^{2e}N(\omega) \equiv 0 \bmod p^c,$$

and

$$\mathrm{ord}_p(x^2) = 2a < a + e \leq \mathrm{ord}_p(xp^e yTr(\omega))$$

so $\mathrm{ord}_p(N(x + p^e y\omega)) = 2a < 2e \leq c$, which is a contradiction. So we have $e \leq a$ and

$$\mathfrak{a} = p^e \alpha_0 R_e \qquad \text{for some } \alpha_0 = x_0 + y_0\omega \in R_0.$$

If we put $\mathfrak{a}_0 = \alpha_0 R_0$, then this is of course an ideal of R_0. Here the generators of $\mathfrak{a}_0$ are written as $\alpha_0\epsilon$ with $\epsilon \in R_0^\times$, but generators of $\alpha_0\epsilon R_e$ are $\alpha_0\epsilon\epsilon_0$ with $\epsilon_0 \in R_e^\times$. So, for each R_0 ideal $\mathfrak{a}_0$, the number of ideals $\mathfrak{b}_0$ of R_e such that $\mathfrak{b}_0 R_0 = \mathfrak{a}_0$ is $[R_0^\times : R_e^\times]$, Hence we prove (3). (Note here that $\mathfrak{a}_0 R_e$ is not an integral ideal of R_e in general, but $p^e\mathfrak{a}_0 R_e$ is.) Next we assume that $c < 2e$. We show that we have $c/2 \leq a$. Indeed, if $a < c/2$, then $\mathrm{ord}_p(x^2) < c$, $c \leq [c/2] + e \leq \mathrm{ord}_p(xp^e yTr(\omega))$, and $c < \mathrm{ord}_p(p^{2e}y^2N(\omega))$, so we have $\mathrm{ord}_p(N(x + yp^e\omega)) = \mathrm{ord}_p(x^2) < c$ which is a contradiction. So we have $c/2 \leq a$. If c is odd, then $(c+1)/2 \leq a$, e, and we see that $\mathfrak{a} = p^{(c+1)/2}(x_0 + p^{e-(c+1)/2}y\omega)$, so $c+1 \leq \mathrm{ord}_p N(\mathfrak{a})$, which is a contradiction. So there exists no ideal such that $\mathrm{ord}_p N(\mathfrak{a})$ is odd and $< 2e$. So we have (1). If c is even, we rewrite c by $2c$. Then we have

$$\mathfrak{a} = p^c(x_0 + y_0 p^{e-c}\omega)R_e.$$

Since $N(\mathfrak{a}) = p^{2c}$, we have $x_0 + y_0 p^{e-c} \in R_{e-c}^{\times}$. So the number of ideals is exactly equal to $[R_{e-c}^{\times} : R_e^{\times}]$. □

In order to count the number of ideals, we give necessary indices.

Lemma 4.2. *For $1 \leq e - c$ we have*

$$[R_{e-c}^{\times} : R_e^{\times}] = p^c.$$

For $e = c$ and $R_{e-c} = R_0$, we have

$$[R_0^{\times} : R_e^{\times}] = p^{e-1}(p - \chi_K(p)).$$

Proof. First we assume that p splits in K. Then we have $K_p = \mathbb{Q}_p \oplus \mathbb{Q}_p$ and $R_0 = O_{max,p} = \mathbb{Z}_p \oplus \mathbb{Z}_p$. Since $\omega \in K$ is embedded in $\mathbb{Z}_p \oplus \mathbb{Z}_p$ by $\omega \to (\omega, \omega^{\sigma})$ where σ is the non trivial automorphism of $K/\mathbb{Q}$, it is easy to see that

$$R_e = O_{f,p} = \{(a, b) \in \mathbb{Z}_p \oplus \mathbb{Z}_p; a \equiv b \bmod p^e\}.$$

So if $e - c > 0$, we have

$$R_{e-c}^{\times}/R_e^{\times} \cong (1 + p^{e-c}\mathbb{Z}_p)/(1 + p^e\mathbb{Z}_p) \cong \mathbb{Z}_p/p^c\mathbb{Z}_p$$

and the order is p^c. If $e = c$, then

$$R_0^{\times}/R_e^{\times} = \mathbb{Z}_p^{\times}/(1 + p^e\mathbb{Z}_p)$$

and the order is $p^{e-1}(p-1) = p^{e-1}(p - \chi_K(p))$. Next we assume that p remains prime in K. We write $P = pO_{max,p}$. When $c = e$, the order of $R_0^{\times}/(1 + P^e) \cong R_0^{\times}/(1 + P) \times (1 + P)/(1 + P^e)$ is $(p^2 - 1)p^{2(e-1)}$. If $c < e$, then

$$R_{e-c}^{\times}/(1 + P^e) \cong R_{e-c}^{\times}/(1 + P^{e-c}) \times (1 + P^{e-c})/(1 + P^e).$$

and the order is $(p-1)p^{e+c-1}$. So we have

$$[R_{e-c}^{\times} : R_e^{\times}] = \begin{cases} p^c & \text{if } c < e, \\ p^{e-1}(p+1) & \text{if } c = e. \end{cases}$$

So noting that $\chi_K(p) = -1$, we have the assertion. Finally we assume that p ramifies in K and denote by P the prime ideal of $O_{max,p}$. Then we have $P^2 = pO_{max,p}$. Assume that $c < e$. Then we have

$$[R_{e-c}^{\times} : 1 + P^{2e}] = [R_{e-c}^{\times} : 1 + P^{2(e-c)}][1 + P^{2(e-c)} : 1 + P^{2e}].$$

The order of this index is $(p-1)p^{e+c-1}$. So we have

$$[R_{e-c}^{\times} : R_e^{\times}] = p^c.$$

If $c = e$, then

$$[R_0^{\times}; R_e^{\times}] = [R_0^{\times} : 1+P^{2e}]/[R_e : 1+P^{2e}] = (p-1)p^{2e-1}/(p-1)p^{e-1} = p^e.$$

Since $\chi_K(p) = 0$, we have the result. □

Finally we calculate the L-function of the genus character including the Euler p factors with $p|f$. We fix a genus character χ of O_f corresponding to a pair (δ_1, δ_2) of reciprocal fundamental divisors. By definition, we have $\delta_1\delta_2 = f_1^2 D_K$ of some divisor f_1 of f. If we put $f_0 = f/f_1$, then we can also say that $D = \delta_1\delta_2 f_0^2$. For any $p|f$, we write $m_p = \mathrm{ord}_p(f_0) = \mathrm{ord}_p(f/f_1)$. For any fundamental discriminant δ of a quadratic field $F/\mathbb{Q}$ and the Dirichlet character $\chi_\delta(a) = \left(\frac{\delta}{a}\right)$, we define the Dirichlet L-function $L(s, \chi_\delta)$ as usual by

$$L(s, \chi_\delta) = \prod_p (1 - \chi_\delta(p)p^{-s})^{-1}.$$

Here we regard $\chi_\delta(p) = 0$ if $p|\delta$. For the sake of simplicity, we write $\phi = \chi_{\delta_1}$ and $\psi = \chi_{\delta_2}$ as before.

The following theorem was given in [12]. We give here a far simpler alternative proof.

Theorem 4.3. *Notation being as above, we have*

$$(2) \quad L(s, O_f, \chi) = L(s, \phi)L(s, \psi)\times$$
$$\prod_{p|f_0} \frac{(1 - \phi(p)p^{-s})(1 - \psi(p)p^{-s}) - p^{m_p(1-2s)-1}(p^{1-s} - \phi(p))(p^{1-s} - \psi(p))}{1 - p^{1-2s}},$$

where the product is taken over primes dividing the positive integer f_0 such that $D = \delta_1\delta_2 f_0^2$. Here if $m_p = ord_p(f_0) = 0$, then the p-factor of the product is regarded as 1.

Before proving this, we prove

Lemma 4.4. *(1) Assume that $m_p < e$. Then we have $\phi(p) = \psi(p) = 0$. (2) If $\phi(p) = \psi(p) = 0$ and $p \nmid D_K$, then $m_p < e$.*

Proof. (1) Since we assumed $\mathrm{ord}_p(f_1) = e - \mathrm{ord}_p(f_0) = e - m_p > 0$, at least one of δ_1 and δ_2 is divisible by p. Assume that $\mathrm{ord}_p\,\delta_1 > 0$ and $\mathrm{ord}_p(\delta_2) = 0$. Then we have

$$\mathrm{ord}_p(\delta_1) = 2(e - m_p) + \mathrm{ord}_p(D_K).$$

Since $e - m_p > 0$, we have $\mathrm{ord}_p(\delta_1) \geq 2$, and since δ_1 is a fundamental discriminant, we should have $p = 2$. So $\mathrm{ord}_2(\delta_1) = 2$ or 3, and $\mathrm{ord}_2(D_K) = 0$ or 1 for each case. The latter cannot happen, so we have $\mathrm{ord}_2(D_K) = 0$, $\mathrm{ord}_2(f_1) = 1$, and $\mathrm{ord}_2(\delta_1) = 2$. Here -4 is a prime discriminant dividing δ_1, so if we write $\delta_1 = (-4)\delta_0$, then δ_0 is an odd fundamental discriminant. So we have

$$\delta_0\delta_2 = -(f_1/2)^2 D_K.$$

Here since $f_1/2$ is odd, RHS is $\equiv 3 \bmod 4$. This contradicts that δ_0 and δ_2 are odd fundamental discriminants. This means that any $p|f$ divides both δ_1 and δ_2 if $0 < e - m_p$. So (1) is proved.
(2) By definition we have $\chi_K = \phi\psi$. Here the product is taken so

that the result is primitive. So if $\phi_p = \psi_p$ with $p \nmid D_K$, we are taking $\phi_p\psi_p = 1$. So it might happen that $\phi_p(p) = \psi(p) = 0$ and $\chi_K(p) \neq 0$ in general. Now in our setting, if $\phi(p) = \psi(p) = 0$, that is, if $1 \leq \mathrm{ord}_p(\delta_i)$ for both $i = 1, 2$, then since

$$2 \leq \mathrm{ord}_p(\delta_1) + \mathrm{ord}_p(\delta_2) = 2\,\mathrm{ord}_p(f_1) + \mathrm{ord}_p(D_K),$$

and $\mathrm{ord}_p(D_K) = 0$ by our assumption, we have $1 \leq \mathrm{ord}_p(f_1) = e - m_p$, so $1 \leq e - m_p$. □

Proof of Theorem 4.3. Any genus character χ of O_f regarded as a character of $K_A^\times$ is trivial on $R_e^\times$ for $e = \mathrm{ord}_p(f)$. By the construction, a genus character χ of O_f associated with a pair (δ_1, δ_2) such that $\delta_1\delta_2 = f_1^2 D_K$ can be regarded as a genus character of O_{f/p^c} for $c \leq e$ if and only if $\mathrm{ord}_p(f_1) \leq e - c$. In other words, if we denote by I_c the group of fractional ideals of R_e defined by

$$I_c = \{\epsilon R_e : \epsilon \in R_{e-c}^\times\},$$

then χ is trivial on I_c if and only if $c \leq e - \mathrm{ord}_p(f_1) = m_p$. So if $m_p < e$, we have

$$\sum_{\mathfrak{a} \in I_c/R_e^\times} \chi(\mathfrak{a}) N(p^c\mathfrak{a})^{-s} = 0 \qquad \text{for all } c = m_p + 1, \ldots, e \tag{3}$$

since χ is not trivial on I_c in these cases and $N(p^c\mathfrak{a}) = p^{2c}$ for any ideal $\mathfrak{a} \in I_c$.

By definition we have $0 \leq m_p \leq e$. First we assume that $m_p \neq e$. Then by Lemma 4.1 (2) and (3), we have no contribution for $L(s, O_f, \chi)$ from ideals $\mathfrak{a}$ with $N(\mathfrak{a}) = p^c$ with $m_p < c/2$. Indeed, if $c \leq 2e$ and c is odd, there is no such ideal by Lemma 4.1 (1). If $c \leq 2e$ and $c = 2c_0$ is even, then the ideals run over $p^{c_0} I_{c_0}$ and since $m_p < c_0 \leq e$, the contribution vanishes by (3). If $c = 2e + c_0$ with $0 \leq c_0$ and $m_p < e$, then the ideals run over $p^e\mathfrak{a}_0 I_e$ for several ideals $\mathfrak{a}_0$ of R_0 with $N(\mathfrak{a}_0) = p^c$, and again the contribution is 0 by (3) since $m_p < e$ means $\mathrm{ord}_p(f_1) > 0$ and χ is non-trivial on $I_e/R_e^\times$. In particular, if $m_p = 0$, then by Lemma 4.4, we have $\phi(p) = \psi(p) = 0$ unless $e = 0$, and the p Euler factor of Theorem 4.3 (2) becomes 1. Next, consider ideals $\mathfrak{a}$ such that $N(\mathfrak{a}) = p^{2c}$ with $c \leq m_p < e$. Then $\mathfrak{a}$ runs over $p^c I_c$, and χ is trivial on these ideals. So by Lemma 4.1 (2), the contribution of such ideals to the L-function is given by $[R_{e-c}^\times : R_e^\times]p^{-2cs}$, and by Lemma 4.2, the total contribution from $c \leq m_p$ is given by

$$1 + p^{1-2s} + p^{2(1-2s)} + \cdots + p^{m_p(1-2s)} = \frac{1 - p^{(1+m_p)(1-2s)}}{1 - p^{1-2s}}. \tag{4}$$

By Lemma 4.4, we have $\phi(p) = \psi(p) = 0$ in this case. So the p Euler factor of Theorem 4.3 (2) coincides with the above (4). Next we assume that $m_p = e$. This means that χ is regarded as a genus character of O_{f/p^e}. Then the character χ is trivial on ideals $\mathfrak{a}$ of norm up to p^{2e}

and this part is given by (4). If $\mathfrak{a} = p^e\mathfrak{a}_0 R_e$ with ideals $\mathfrak{a}_0$ of R_0 then the value of the character $\chi(\mathfrak{a}) = \chi(\mathfrak{a}_0 R_e)$ is the same value for the corresponding character χ on $Cl^+(O_{f/p^e})$. By using Lemma 4.2, we see that the contribution of this part is given by

$$\frac{p^{e-1}(p-\chi_K(p))p^{-2es}}{(1-\phi(p)p^{-s})(1-\psi(p)p^{-s})}. \tag{5}$$

So summing up (4) and (5), and noting $\chi_K(p) = \phi(p)\psi(p)$ for any prime p by Lemma 4.4 (2), we obtain (2) of Theorem 4.3. □

5. The genus number in the wide sense.

If we replace the definition $U_+(O)$ by $U(O) = U_\infty \prod_p O_p^\times$ in section 2, where $U_\infty = (\mathbb{R}^\times)^{r_1} \times (\mathbb{C}^\times)^{r_2}$, then the genus in the wide sense is defined by taking $a \in K_A^\times$ such that $N(a) \in \mathbb{Q}^\times N(U(O))$ in the same way. (Since we are assuming K is cyclic over $\mathbb{Q}$, actually we have $r_1 = 0$ or $r_2 = 0$.) The genus theory in the wide sense for maximal orders is given in general setting in Furuta [7], for example. Maybe the concrete genus numbers in the wide sense for orders of a quadratic field are well known but we give the formula as an appendix as a continuation of the previous sections. Of course this is nothing but the number of cosets in the ideal class group in the wide sense over the group of square classes. We will give an application of this formula in the next section.

We first prove results for maximal orders for the sake of simplicity, and then state the result for general quadratic orders.

Proposition 5.1. *Let K be a quadratic field. Let t be the number of prime divisors of the fundamental discriminant D_K of K.*
(1) If K is imaginary, or if $-1 \in N(K^\times)$, then the genus number in the wide sense is the same as the genus number in the narrow sense and given by 2^{t-1}.
(2) If K is real and $-1 \notin N(K^\times)$, then the genus number in the wide sense is 2^{t-2}.
(3) For a real quadratic field K, we have $-1 \in N(K^\times)$ if and only if all the odd prime divisors of D_K are $1 \bmod 4$.

The condition (3) above is equivalent to the condition that the genus field of K in the narrow sense (the abelian extension of K corresponding to the principal genus classes in the narrow sense) is real, that is, unramified at infinite places. (The genus field of K in the wide sense is always real for real K by the class field theory.) Note also that by (3), we always have $t \geq 2$ in (2).

Proof. The results (1) and (2) are essentially due to [7], but we reprove it here. The claim is clear when K is imaginary, so we assume K is real. The difference from the narrow sense comes from $N(U_\infty) = \mathbb{R}^\times$ since

this is not contained in $\mathbb{R}_+^\times$. So correcting this part by multiplying by $-1 \in \mathbb{Q}$, the genus number in the wide sense is given by the index

$$\frac{1}{2}\Big[\prod_p \mathbb{Z}_p^\times : \prod_p N(O_{max,p}^\times) \bigcup (-1)\prod_p N(O_{max,p}^\times)\Big].$$

This number is the same as the genus number in the narrow sense if and only if $-1 \in N(O_{max,p}^\times)$ for all p, and half of it if $-1 \notin N(O_{max,p}^\times)$ for some p. For a real field, the condition that $-1 \in N(O_{max,p}^\times)$ for all primes p is equivalent to the condition $-1 \in N(K)$. Indeed, if -1 is a norm at all local places, then the global element $-1 \in \mathbb{Q}^\times$ is a norm of an element of $K^\times$ by the Hasse norm theorem. Conversely, if $N(c) = -1$ for $c \in K^\times$, then $c \in O_{max,p}$ if K_p is a field and $-1 \in N(O_{max,p}^\times)$. If $K_p = \mathbb{Q}_p \oplus \mathbb{Q}_p$, then $-1 \in \mathbb{Z}_p^\times = N(\mathbb{Z}_p^\times \times \mathbb{Z}_p^\times)$ always. So (1) and (2) are proved. Now more concrete condition is as follows. If p does not ramify, then $-1 \in \mathbb{Z}_p^\times = N(O_{max,p}^\times)$ always. If p ramifies, then by Lemma 3.2, for odd p, we have $-1 \in N(O_{max,p}^\times)$ if and only if $p \equiv 1 \bmod 4$. For $p = 2$, by Lemma 3.2 (iv) and (v), we have $-1 \in N(O_{max,2}^\times)$ if and only if $8|D_K$ and $D_K/8 \equiv 1 \bmod 4$. But since we assumed $D_K > 0$, the condition that all odd $p|D_K$ satisfy $p \equiv 1 \bmod 4$ means that $D_K/8 \equiv 1 \bmod 4$. □

Note that $-1 \in N(K^\times)$ is much weaker than the existence of a unit $\epsilon \in O_{max}^\times$ with $N(\epsilon) = -1$. For example, for $K = \mathbb{Q}(\sqrt{221}) = \mathbb{Q}(\sqrt{13 \cdot 17})$, we have $N\left(\dfrac{5+\sqrt{221}}{14}\right) = -1$ but the fundamental unit $(15+\sqrt{221})/2$ of K has norm $+1$. In this case, if we put

$$\mathfrak{c} = \mathbb{Z}7 + \mathbb{Z}\frac{5+\sqrt{221}}{2},$$

then

$$\mathfrak{c}^2 = \left(\frac{5+\sqrt{221}}{2}\right) O_K.$$

Here we have $N(\frac{5+\sqrt{221}}{2}) = -49$, so square classes in the wide sense are equal to square classes in the narrow sense. The genus numbers in the narrow sense and in the wide sense are both equal to 2. The genus field for K is $\mathbb{Q}(\sqrt{13}, \sqrt{17})$. For general quadratic K, if $N(c) = -1$ for $c \in K^\times$, then by using the prime ideal decomposition of cO_K, we can easily see that $cO_K = \mathfrak{c}^{1-\sigma}$ for an ideal $\mathfrak{c}$ that is a product of prime ideals splitting in K. This means that $\mathfrak{c}^2 = cN(\mathfrak{c})O_K$ and that the square classes in the narrow sense and in the wide sense are the same.

Finally, for a quadratic order O_f of general conductor f, we have the following results.

Proposition 5.2. *Put $D = f^2 D_K$. The genus number for O_f in the narrow sense is equal to the genus number in the wide sense if and only*

if the following two conditions are satisfied.
(1) $p \equiv 1 \bmod 4$ *for all odd* $p|D$.
(2) $D \not\equiv 0 \bmod 16$.
Otherwise, the genus number in the narrow sense is 2 *times the one in the wide sense.*

The proof is almost the same as the proof of Proposition 5.1 by using Lemma 3.2 and 3.3, so we omit it here.

6. Maximal orders of matrix algebras over algebraic number fields

Let F be an algebraic number field and $O_{max} = O_F$ be the ring of all integers of F. A submodule L of F^n is said to be an O_F lattice if it is finitely generated O_F module and contains a basis of F^n. A subring Λ of $M_n(F)$ is said to be an O_F order of $M_n(F)$ if it is an O_F lattice in $M_n(F)$ and contains the unit matrix. We denote by $F_+^\times$ the subgroup of elements of $F^\times$ which are positive under all real embeddings of F. We define a subgroup $GL_n^+(F)$ of $GL_n(F)$ as

$$GL_n^+(F) = \{g \in GL_n(F) : \det(g) \in F_+^\times\}.$$

The number of $GL_n(F)$ conjugacy classes of maximal O_F orders of $M_n(F)$ is called a type number of $M_n(F)$ (sometimes called in the wide sense in this paper). The similar number up to $GL_n^+(F)$ conjugacy classes will be called a type number in the narrow sense in this paper. The purpose of this section is to characterize these numbers in terms of ideal classes. This has been known for type numbers in the wide sense in [8] for $n = 2$ and in [2] for general n. We include this theory in the paper because when $n = 2$ and F is quadratic, these two kinds of type numbers are given by the genus number in the wide sense and in the narrow sense, respectively. The papers [8] and [2] use a global method but here we prove everything adelically. Most results below except for Propositions 6.3 and 6.4 are also found in [16].

We start from description of O_F lattices $L \subset F^n$. For any $g = (g_v) \in GL_n(F_A)$, we define $O_F^n g$ by

$$O_F^n g = \bigcap_{v<\infty} (O_{F,v}^n g_v \cap F^n).$$

For any O_F lattice L and a finite place v of F, we put $L_v = L \otimes_{O_F} O_{F,v}$. Then we have $L_v = O_v^n$ for almost all v and it is clear that we have $L_v = O_v^n g_v$ for some $g_v \in GL_n(F_v)$ for all v. So any O_F lattice is written as $O_F^n g$ for some $g \in G_A$.

For an O_F lattice L, we write

$$\Lambda_L = \{g \in M_n(F); Lg \subset L\}$$

and call it the right order of L. Any maximal order Λ of $M_n(F)$ is the right order of some L. This is clear since $L\Lambda$ is again an O_F lattice

for any O_F lattice L and we have $\Lambda \subset \Lambda_{L\Lambda}$. So any maximal order of $M_n(F)$ is written as

$$g^{-1}M_n(O_F)g := \bigcap_{v<\infty}(g_v^{-1}M_n(O_{F,v})g_v \cap M_n(F))$$

for some $g = (g_v) \in GL_n(F_A)$.

To write down global orbits of lattices and conjugacy classes of maximal orders, we prepare adelic subgroups.

We denote by $GL_n^+(\mathbb{R})$ the subgroup of elements of $GL_n(\mathbb{R})$ with positive determinants. We denote by r_1 and r_2 the number of real places and complex places of F. Put $U_\infty = GL_n(\mathbb{R})^{r_1} \times GL_n(\mathbb{C})^{r_2}$ and $U_{\infty,+} = GL_n^+(\mathbb{R})^{r_1} \times GL_n(\mathbb{C})^{r_2}$. We put $U_0 = \prod_{v<\infty} GL_n(O_{F,v})$ and $U = U_\infty U_0$ and $U_+ = U_{\infty,+}U_0$. For ideal classes $C_i \in Cl(O_F)$ and $C_j^+ \in Cl^+(O_F)$, we fix representative ideles a_i and b_j in $F_A^\times$, respectively. So we have

$$F_A^\times = \bigsqcup_i a_i F^\times (\mathbb{R}^\times)^{r_1}(\mathbb{C}^\times)^{r_2} \prod_{v<\infty} O_{F,v}^\times \quad (disjoint)$$
$$F_A^\times = \bigsqcup_j b_j F^\times (\mathbb{R}_+^\times)^{r_1}(\mathbb{C}^\times)^{r_2} \prod_{v<\infty} O_{F,v}^\times \quad (disjoint).$$

We define ideals $\mathfrak{a}_i$ and $\mathfrak{b}_i$ corresponding these by

$$\mathfrak{a}_i = \bigcap_{v<\infty}(a_{i,v}O_{F,v} \cap F), \quad \mathfrak{b}_j = \bigcap_{v<\infty}(b_{j,v}O_{F,v} \cap F).$$

Here we may assume that infinite components a_i and b_i are all 1. We define diagonal matrices $g_i = diag(1, \dots, 1, a_i)$ and $h_j = diag(1, \dots, 1, b_j)$ in $GL_n(F_A)$. It is well known that we have the following double coset decomposition. The proof is based on the strong approximation theorem on SL_n, and we omit the proof.

Lemma 6.1 ([14])**.** *We have*

$$GL_n(F_A) = \bigsqcup_i U g_i GL_n(F) \quad (disjoint),$$
$$GL_n(F_A) = \bigsqcup_j U_+ h_j GL_n(F) \quad (disjoint).$$

If we denote by $GL_n^+(F_A)$ the subgroup of elements of $GL_n(F_A)$ whose infinite components are in $U_{\infty,+}$. Then, since $F^\times$ contains an element with arbitrary sign at real places, we also have

$$GL_n^+(F_A) = \bigsqcup_j U_+ h_j GL_n^+(F) \quad (disjoint).$$

It is easy to see that any $g \in GL_n(F_A)$ belongs to the double coset of g_i if and only if $\det(g)$ belongs to the ideal class of $\mathfrak{a}_i$ and any $g \in GL_n^+(F_A)$ belongs to h_j if and only if $\det(g)$ belongs to the ideal class of $\mathfrak{b}_j$.

In terms of global lattices, Lemma 6.1 is written as follows.

Lemma 6.2. *We fix an O_F lattice L.*
(1) There exists the unique ideal class $C_i \in Cl(O_F)$ such that the $GL_n(F)$ orbit of L contains $(O_F, \dots, O_F, \mathfrak{a}_i)$ for $\mathfrak{a}_i \in C_i$.
(2) There exists the unique ideal class $C_j^+ \in Cl^+(O_F)$ such that the $GL_n^+(F)$ orbit of L contains $(O_f, \dots, O_F, \mathfrak{b}_j)$ for $\mathfrak{b}_j \in C_j^+$.

So any maximal order of $M_n(F)$ is $GL_n^+(F)$ conjugate to

$$\Lambda(\mathfrak{a}) = \begin{pmatrix} O_F & \cdots & O_F & \mathfrak{a} \\ \vdots & \cdots & \vdots & \vdots \\ O_F & \cdots & O_F & \mathfrak{a} \\ \mathfrak{a}^{-1} & \cdots & \mathfrak{a}^{-1} & O_F \end{pmatrix}$$

for some ideal $\mathfrak{a}$ of O_F. (This is well known up to $GL_n(F)$ conjugacy. See [16] for example.) We note that when $n = 1$, we have $\Lambda(\mathfrak{a}) = O_F$ by definition.

Next problem is to describe dependence of $\Lambda(\mathfrak{a})$ on $\mathfrak{a}$. The relation $g^{-1}M_n(O)g = M_n(O)$ for $g = (g_v) \in GL_n(F_A)$ means that $M_n(O_{F,v})g_v$ $(v < \infty)$ is a two sided ideal of $M_n(O_{F,v})$. It is well known that any two sided ideal is written as $c_v M_n(O_{F,v})$ for some $c_v \in F_v^\times$ (See [16]). Now take k_1, $k_2 \in GL_n^+(F_A)$ and assume that $g_0^{-1}k_1^{-1}M_n(O)k_1g_0 = k_2^{-1}M_n(O)k_2$ for some $g_0 \in GL_n^+(F)$. Assume that k_1 and k_2 belong to the double cosets of h_i and h_j in Lemma 6.1, respectively. Then by the above consideration, there exists $c \in F_A^\times$ whose infinite components are 1 such that

$$U_+ h_i GL_n^+(F) = U_+ c h_j GL_n^+(F).$$

This means that $\det(ch_j) = c^n b_j$ belongs to the narrow class of b_i. The argument for conjugacy classes with respect to $GL_n(F)$ is similar. So we have

Proposition 6.3. *(1) $\Lambda(\mathfrak{a}_i)$ and $\Lambda(\mathfrak{a}_j)$ are $GL_n(F)$ conjugate if and only if $\mathfrak{a}_i$ and $\mathfrak{a}_j\mathfrak{c}^n$ belong to the same ideal class in the wide sense for some fractional ideal $\mathfrak{c}$ of O_F.*
(2) $\Lambda(\mathfrak{b}_i)$ and $\Lambda(\mathfrak{b}_j)$ are $GL_n^+(F)$ conjugate if and only if $\mathfrak{b}_i$ and $\mathfrak{b}_j\mathfrak{c}^n$ belong to the same ideal class in the narrow sense for some fractional ideal $\mathfrak{c}$ of O_F.

Of course the type numbers for both cases are the orders of ideal class groups $Cl(O_F)$ and $Cl^+(O_F)$ divided by n-th power classes, respectively. In particular, when $n = 1$, then the type numbers are one. When $n = 2$ and F is quadratic over $\mathbb{Q}$, these are genus numbers.

Proposition 6.4. *When K is a quadratic field over $\mathbb{Q}$, the number of maximal orders of $M_2(K)$ up to $GL_2(K)$ conjugation is equal to the genus number in the wide sense, and up to $GL_2^+(K)$ conjugation is equal to the genus number in the narrow sense.*

Example: When $K = \mathbb{Q}(\sqrt{3})$ then the genus number in the wide sense is 1, while the one in the narrow sense is 2. Representatives of maximal orders up to $GL_2^+(K)$ conjugacy classes are given by

$$M_2(O_K) \quad \text{and} \quad \begin{pmatrix} O_K & \sqrt{3}O_K \\ (\sqrt{3})^{-1}O_K & O_K \end{pmatrix}.$$

These are conjugate by $\begin{pmatrix} 1 & 0 \\ 0 & \sqrt{3} \end{pmatrix}$ but not conjugate by any element of $GL_2^+(K)$.

7. Appendix on quadratic forms

In this section, for readers' convenience, we explain relations between classes and genera of binary quadratic forms and those of proper ideal classes of a quadratic order.

Let K be a quadratic extension of $\mathbb{Q}$ and D_K be the fundamental discriminant of K. We fix a positive integer f and put $D = f^2 D_K$. We denote by O_f the quadratic order of K of conductor f as before. For a fixed D, we consider the set of quadratic forms

$$ax^2 + bxy + cy^2$$

with $b^2 - 4ac = D$ and $\gcd(a, b, c) = 1$, where gcd means the greatest common divisor. This is bijective to the following set $S(D)$ defined as

$$S(D) = \{S = \begin{pmatrix} a & b/2 \\ b/2 & c \end{pmatrix}; a, b, c \in \mathbb{Z}, b^2 - 4ac = D, \gcd(a, b, c) = 1\}.$$

We call an element of $S(D)$ a primitive quadratic form of discriminant D. We say that S_1, $S_2 \in S(D)$ belongs to the same class in the narrow sense if $S_2 = {}^tAS_1A$ for some $A \in SL_2(\mathbb{Z})$. We say that S_1 and $S_2 \in S(D)$ are in the same class in the wide sense if $S_2 = \det(A)\,{}^tAS_1A$ for some $A \in GL_2(\mathbb{Z})$. When $D < 0$, we put

$$S^+(D) = \{S \in S(D); S > 0\},$$

where $S > 0$ means that S is positive definite. The following theorem is well known.

Theorem 7.1. *The set of classes in the wide sense of $S(D)$ is bijective to the proper ideal class group $Cl(O_f)$ in the wide sense. The set of classes in the narrow sense of $S^+(D)$ for $D < 0$ or the set of the classes in the narrow sense of $S(D)$ for $D > 0$ is bijective to the proper ideal class group $Cl^+(O_f)$ in the narrow sense.*

We omit the proof here, since this is written for example in [1] English version Chapter 6 Theorem 6.7.

Next we consider the genus of quadratic forms. In general a genus means the set of quadratic forms that are isomorphic locally at every place and integrally at every finite place. Before giving a precise definition of a genus of quadratic forms, we give a remark on a relation

between equivalence by $GL_n(\mathbb{Z}_p)$ and by $SL_n(\mathbb{Z}_p)$ for general n-ary quadratic forms.

Lemma 7.2. *Let n be any natural number. Let S_1 and S_2 be any symmetric matrices in $M_n(\mathbb{Z}_p)$ and assume that $\det(S_1) = \det(S_2) \neq 0$. If $S_2 = {}^tBS_1B$ for an element $B \in GL_n(\mathbb{Z}_p)$, then we have $S_2 = {}^tAS_1A$ for some element $A \in SL_n(\mathbb{Z}_p)$.*

Proof. This is essentially in [3] Chapter 8 Lemma 3.2 Corollary, but we give here an alternative proof for readers' convenience. Since $\det(S_2) = \det(B)^2 \det(S_1)$, we have $\det(B) = \pm 1$. If $\det(B) = 1$, we have nothing to prove, so assume that $\det(B) = -1$. By Jordan decomposition of a quadratic form, we may assume that ${}^tCS_1C$ for some $C \in GL_n(\mathbb{Z}_p)$ is an orthogonal sum of several matrices of the following shape,

$$p^{e_1}u \quad (u \in \mathbb{Z}_p^\times), \quad p^{e_2}\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad p^{e_3}\begin{pmatrix} 2 & 1 \\ 1 & 2 \end{pmatrix}.$$

(See for example [13] Theorem 5.3.1, 5.2.5.) Here $\det(C) = \epsilon \in \mathbb{Z}_p^\times$. But if we write the diagonal matrix D of diagonal elements $(1, \dots, 1, \epsilon^{-1})$ and replace C by $C_1 = CD$, then $\det(C_1) = 1$ and ${}^tC_1SC_1$ can be taken again as an orthogonal sum containing one of

$$p^{e_1}\epsilon^{-2}u, \quad p^{e_2}\begin{pmatrix} 0 & \epsilon^{-1} \\ \epsilon^{-1} & 0 \end{pmatrix}, \quad p^{e_3}\begin{pmatrix} 2 & 2\epsilon^{-1} \\ 2\epsilon^{-1} & 2\epsilon^{-2} \end{pmatrix},$$

the others being unchanged. Since we have

$$(-1)p^{e_1}\epsilon^{-2}u(-1) = p^e\epsilon^{-2}$$

$$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} p^{e_2}\begin{pmatrix} 0 & \epsilon^{-1} \\ \epsilon^{-1} & 0 \end{pmatrix}\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} = p^{e_2}\begin{pmatrix} 0 & \epsilon^{-1} \\ \epsilon^{-1} & 0 \end{pmatrix}$$

$$\begin{pmatrix} 0 & \epsilon \\ \epsilon^{-1} & 0 \end{pmatrix} p^{e_3}\begin{pmatrix} 2 & \epsilon^{-1} \\ \epsilon^{-1} & 2\epsilon^{-2} \end{pmatrix}\begin{pmatrix} 0 & \epsilon^{-1} \\ \epsilon & 0 \end{pmatrix} = p^{e_3}\begin{pmatrix} 2 & \epsilon^{-1} \\ \epsilon^{-1} & 2\epsilon^{-2} \end{pmatrix},$$

there exists $C_2 \in GL_2(\mathbb{Z}_p)$ with $\det(C_2) = -1$ such that ${}^t(C_1C_2)S_1(C_1C_2) = {}^tC_1S_1C_1$. So if we put $C_0 = C_1C_2C_1^{-1}$, then

$$S_2 = {}^tBS_1B = {}^t(C_0B)S_1(C_0B)$$

and $\det(C_0B) = 1$. This proves the assertion. □

We put $\mathbb{Z}_\infty = \mathbb{R}$ as before. If S_1, $S_2 \in GL_n(\mathbb{Q})$ and there exists $A_v \in GL_n(\mathbb{Z}_v)$ such that $S_2 = {}^tA_vS_1A_v$ for any place v, then we have automatically $\det(S_1) = \det(S_2)$. Indeed, we have $\det(S_2)/\det(S_1) = \det(A_p)^2 \in \mathbb{Z}_p^\times$, so $\det(S_2)/\det(S_1) = \pm 1$ but by $S_2 = {}^tA_\infty S_1A_\infty$, we have $\det(S_2)/\det(S_1) > 0$, so $\det(S_2) = \det(S_1)$. We also have $\det(A_v) = \pm 1$.

Definition 7.3. *We say that S_1, $S_2 \in S(D)$ belongs to the same genus in the narrow sense if there exists $A_v \in GL_2(\mathbb{Z}_v)$ such that $S_2 = {}^tA_vS_1A_v$ for each place v of $\mathbb{Q}$. We say that S_1, $S_2 \in S(D)$ belongs to the*

same genus in the wide sense if, for a fixed $\epsilon \in \{\pm 1\}$*, there exists* $A_v \in GL_2(\mathbb{Z}_v)$ *such that* $S_2 = \det(A_v)\,{}^tA_vS_1A_v$ *with* $\det(A_v) = \epsilon$ *for every place* v *of* $\mathbb{Q}$*.*

The above definition of the genus of binary quadratic forms in the wide sense would be new. If S_1 and S_2 are in the same genus in the wide sense for $\epsilon = -1$, then S_1 and $-S_2$ are in the same genus in the narrow sense by virtue of Lemma 7.2. The genus in the narrow sense is the usual definition of a genus of quadratic forms. In this case, by Lemma 7.2, we may assume that $\det(A_v) = 1$ for all places v. The following theorem is well known for the genera in the narrow sense (See for example [3]).

Theorem 7.4. *Fix a positive integer* f *and a quadratic field* K*. The genera of binary quadratic forms in* $S(D)$ *for* $D > 0$ *or in* $S^+(D)$ *for* $D < 0$ *of discriminant* $D = f^2D_K$ *in the narrow sense correspond bijectively to the genera of* $Cl^+(O_f)$*. The genera in the wide sense in* $S(D)$ *correspond bijectively to the genera of* $Cl(O_f)$ *in the wide sense.*

Proof. When $D < 0$, every class in $S(D)$ in the wide sense has a representative in $S^+(D)$, and we also have $Cl^+(O_f) = Cl(O_f)$, so the genera in the wide sense and in the narrow sense are the same. So in this case, it is sufficient to prove the claim for the narrow sense. For any element $S \in S(D)$ with $D > 0$ or in $S \in S^+(D)$ with $D < 0$, it is well known that there exists an element $S_0 = \begin{pmatrix} a & b/2 \\ b/2 & c \end{pmatrix}$ equivalent in the narrow sense to S such that $a > 0$ ([1] p.83). For the sake of simplicity, we denote by $S_0(D)$ the subset of $S(D)$ such that $(1,1)$ component is positive, i.e.

$$S_0(D) = \left\{ \begin{pmatrix} a & b/2 \\ b/2 & c \end{pmatrix} \in S(D); a > 0 \right\}.$$

When $D < 0$, of course we have $S_0(D) = S^+(D)$. Now for S_1, $S_2 \in S_0(D)$, we write

$$S_i = \begin{pmatrix} a_i & b_i/2 \\ b_i/2 & c_i \end{pmatrix} \qquad (i = 1, 2).$$

The corresponding proper primitive ideals in Theorem 7.1 are given by

$$\mathfrak{a}_i = \mathbb{Z}a_i + \mathbb{Z}\frac{b_i + \sqrt{D}}{2}.$$

Fix $\epsilon \in \{\pm 1\}$. First we assume that $S_2 = \det(A_v)\,{}^tA_vS_1A_v$ for some elements $A_v \in GL_2(\mathbb{Z}_v)$ with $\det(A_v) = \epsilon$ for every place v of $\mathbb{Q}$. (If S_1, $S_2 \in S^+(D)$, then $\epsilon = 1$ automatically, but this does not matter.) In this case, we show that $\mathfrak{a}_1$ and $\mathfrak{a}_2$ belong to the same genus in the narrow sense if $\epsilon = 1$ and belong to the same genus in the wide sense

if $\epsilon = -1$. For ideals $\mathfrak{a}_i$, we take $\alpha_i \in K_A^\times$ such that ∞ component $\alpha_{i,\infty} = 1 \in K_\infty (= \mathbb{R}^2$ or $\mathbb{C})$ and p components $\alpha_{i,p}$ for primes p satisfy

$$\mathfrak{a}_i = \bigcap_p (O_{f,p}\alpha_{i,p} \cap K).$$

We will show that $\alpha_2\alpha_1^{-1}$ belongs to the principal genus in the narrow sense if $\epsilon = 1$ and in the wide sense if $\epsilon = \pm 1$. For each prime p, we define $\omega_{1,p}$, $\omega_{2,p} \in K_p$ by

$$(\omega_{1,p}, \omega_{2,p}) = (a_1, \frac{b_1 + \sqrt{D}}{2})A_p. \tag{6}$$

If we write $\mathfrak{a}_{i,p} = \mathfrak{a}_i \otimes_{\mathbb{Z}} \mathbb{Z}_p$ for $i = 1, 2$, then $(\omega_{1,p}, \omega_{2,p})$ is a basis of $\mathfrak{a}_{1,p}$ over $\mathbb{Z}_p$. For variables x, y, we put

$$\begin{pmatrix} X \\ Y \end{pmatrix} = A_p \begin{pmatrix} x \\ y \end{pmatrix}.$$

Multiplying ${}^t(x, y)$ from the right of (6) and taking the norm of both sides, we have

$$N(\omega_{1,p})x^2 + Tr(\omega_{1,p}\omega_{2,p}^\sigma)xy + N(\omega_{2,p})y^2 = a_1(a_1X^2 + b_1XY + c_1Y^2),$$

where σ denotes the non-trivial automorphism of K_p over $\mathbb{Q}_p$. Here by the relation of S_1 and S_2, the right hand side is equal to

$$\epsilon a_1(a_2x^2 + b_2xy + c_2y^2),$$

so we have

$$N(\omega_{1,p}) = a_1a_2\epsilon \tag{7}$$

$$Tr(\omega_{1,p}\omega_{2,p}^\sigma) = a_1b_2\epsilon \tag{8}$$

$$N(\omega_{2,p}) = a_1c_2\epsilon. \tag{9}$$

On the other hand, by taking the conjugate by σ of (6), we have

$$\begin{pmatrix} \omega_{1,p} & \omega_{2,p} \\ \omega_{1,p}^\sigma & \omega_{2,p}^\sigma \end{pmatrix} = \begin{pmatrix} a_1 & \frac{b_1+\sqrt{D}}{2} \\ a_1 & \frac{b_1-\sqrt{D}}{2} \end{pmatrix} A_p,$$

and taking the determinants of both sides, we have

$$\omega_{1,p}\omega_{2,p}^\sigma - \omega_{2,p}\omega_{1,p}^\sigma = \epsilon(-a_1\sqrt{D}).$$

Subtracting this from (8), we have

$$\omega_{2,p}\omega_{1,p}^\sigma = a_1\epsilon\frac{b_2 + \sqrt{D}}{2}. \tag{10}$$

If we put $\gamma_p = \frac{a_2}{\omega_{1,p}}$, then by (7) and (11), we have

$$\omega_{2,p}\gamma_p = \frac{b_2 + \sqrt{D}}{2}.$$

So we have

$$O_{f,p}\alpha_{2,p} = \mathfrak{a}_{2,p} = \mathfrak{a}_{1,p}\gamma_p = O_{f,p}\alpha_{1,p}\gamma_p.$$

So $\alpha_{2,p} = u_p\alpha_{1,p}\gamma_p$ for some $u_p \in O_{f,p}^\times$. We also have $N(\gamma_p) = \epsilon a_2/a_1$ by (7). If $D > 0$, then there exists $\gamma_\infty \in K_\infty$ such that $N(\gamma_\infty) = \epsilon a_2/a_1$. If $D < 0$, then we should have $\epsilon = 1$ and since we assumed that $a_i > 0$, there exists $\gamma_\infty \in K_\infty$ such that $N(\gamma_\infty) = a_2/a_1$. So in both cases, by Hasse's norm theorem, we have $\gamma \in K^\times$ such that $N(\gamma) = \epsilon a_2/a_1$. So if we put $u_\infty = \gamma^{-1} \in K_\infty$ and $u = (u_v)$, then we have

$$N(\alpha_2/\alpha_1) \in N(\gamma)N(U(O_f)) \subset \mathbb{Q}^\times N(U(O_f))$$

if $\epsilon = \pm 1$, so $\mathfrak{a}_1$ and $\mathfrak{a}_2$ belong to the same genus in the wide sense. If $\epsilon = 1$, then $N(\gamma) > 0$, so

$$N(\alpha_2/\alpha_1) \in N(\gamma)N(U_+(O_f)) \subset \mathbb{Q}^\times N(U_+(O_f)).$$

So $\mathfrak{a}_1$ and $\mathfrak{a}_2$ belong to the same genus in the narrow sense.

On the contrary, assume that $\mathfrak{a}_1$ and $\mathfrak{a}_2$ belongs to the same genus in the narrow sense. Then we have

$$N(\alpha_2/\alpha_1) \in \mathbb{Q}^\times N(U_+(O_f)).$$

Here $\mathbb{Q}^\times$ part is obviously a norm of an element of $K_A^\times$ and by Hasse's norm theorem, it is written as $N(\gamma)$ for some $\gamma \in K^\times$. So there exists $w = (w_v) \in K_A^\times$ with $N(w) = 1$ and $u \in U_+(O_f)$ such that

$$\alpha_2/\alpha_1 = \gamma w u.$$

So we have

$$\mathfrak{a}_{2,p} = \mathfrak{a}_{1,p}\gamma w_p.$$

Since we assumed $\alpha_{i,\infty} = 1$, we have $N(\gamma) > 0$, so if we put $\mathfrak{a}_3 = \mathfrak{a}_1\gamma$, then $\mathfrak{a}_3$ is equivalent to $\mathfrak{a}_1$ in the narrow sense. So if we put

$$\mathfrak{a}_2 = \mathbb{Z}a_2 + \frac{b_2 + \sqrt{D}}{2}, \quad \mathfrak{a}_3 = \mathbb{Z}a_3 + \frac{b_3 + \sqrt{D}}{2}$$

with $a_2 > 0$, $a_3 > 0$ and $D = b_i^2 - 4a_ic_i$ for $i = 2, 3$, then we have

$$(a_2, \frac{b_2 + \sqrt{D}}{2}) = (a_3, \frac{b_3 + \sqrt{D}}{2})w_pA_p \tag{11}$$

for some $A_p \in GL_2(\mathbb{Z}_p)$. So we have

$$\begin{pmatrix} a_2 & \frac{b_2+\sqrt{D}}{2} \\ a_2 & \frac{b_2-\sqrt{D}}{2} \end{pmatrix} = \begin{pmatrix} w_p & 0 \\ 0 & w_p^\sigma \end{pmatrix} \begin{pmatrix} a_3 & \frac{b_3+\sqrt{D}}{2} \\ a_3 & \frac{b_3-\sqrt{D}}{2} \end{pmatrix} A_p.$$

Since $N(w_p) = 1$, taking the determinant of both sides, we have

$$-a_2\sqrt{D} = -a_3\sqrt{D}\det(A_p).$$

Since $a_2/a_3 = \det(A_p) \in \mathbb{Z}_p^\times$ for all p and $a_2/a_3 > 0$, we have $a_2 = a_3$ and $\det(A_p) = 1$ for all p. Writing

$$\begin{pmatrix} X \\ Y \end{pmatrix} = A_p \begin{pmatrix} x \\ y \end{pmatrix},$$

and multiplying ${}^t(x, y)$ to both sides of (11) from the right and taking the norm, we have

$$a_2(a_2x^2 + b_2xy + c_2y^2) = a_3(a_3X^2 + b_3XY + c_3Y^2).$$

We write

$$S_i = \begin{pmatrix} a_i & b_i/2 \\ b_i/2 & c_i \end{pmatrix}$$

for $i = 2$, 3. Then since we proved $a_3 = a_2$, we have

$$S_2 = {}^tA_pS_3A_p.$$

We also have $A_\infty \in SL_2(\mathbb{R})$ such that

$$S_2 = {}^tA_\infty S_3 A_\infty$$

since this is valid for any positive definite, or indefinite real symmetric matrices of the same determinant. So we see that S_1 and S_2 belong to the same genus in the narrow sense. Now assume that $\mathfrak{a}_1$ and $\mathfrak{a}_2$ belong to the same genus in the wide sense. By definition, we have

$$N(\alpha_2\alpha_1^{-1}) \in \mathbb{Q}^\times N(U(O_f))$$

so we have

$$\alpha_2\alpha_1^{-1} = \gamma w u$$

for some $\gamma \in K^\times$, $w \in K_A^\times$ with $N(w) = 1$, and $u \in U(O_f)$ in the same way as before. Here we might have $N(\gamma) < 0$. But anyway, if we put

$$\mathfrak{a}_3 = \mathfrak{a}_1\gamma$$

then

$$S_3 = \det(B)\,{}^tBS_2B$$

for some $B \in GL_2(\mathbb{Z})$ by Theorem 7.1. Here S_3 and S_2 belong to the same genus in the narrow sense by the same argument as before, so S_1 and S_2 belong to the same genus in the wide sense. □

References

[1] T. Arakawa, T. Ibukiyama and M. Kaneko, Bernoulli numbers and zeta functions, New Edition (in Japanese), Kyoritsu Shuppan Ltd, 2022. English version without genus theory is: Bernoulli numbers and zeta functions, Springer Monogr. Math. Springer, Tokyo, 2014.

[2] S. Arima, *Ideals and lattices*, Chapter 2 and 3 of Number Theory of Algebra (in Japanese), Ed. by Y. Kawada, Seminary Notes 3, University of Tokyo, (1963), 16–63.

[3] J. W. S. Cassels, Rational quadratic forms. London Mathematical Society Monogr. **13**. Academic Press, Inc., London, New York, 1978.

[4] C. Chevalley, *La théorie du corps de classes*, Ann. of Math. **41**(1940), 394-418.

[5] G. Chinta and O. Offen, *Orthogonal period of a $GL_3(\mathbb{Z})$ Eisenstein series.* Representation theory, complex analysis, and integral geometry, Birkhäuser/Springer, New York, (2012), 41–59.

[6] P. G. L. Dirichlet, Vorlesungen über Zahlentheorie, Herausgegeben und mit Zusätzen versehen von R. Dedekind. Vierte umgearbeitete und vermehrte Auflage, Chelsea Publ. Co., New York, 1968.

[7] Y. Furuta, *The genus theory and genus number in algebraic number fields*, Nagoya Math. J. **29** (1967), 281–285.
[8] H. Helling, *Bestimmung der Kommensurabilitätsklasse der Hilbertschen Modulgruppe*, Math. Zeit. **92** (1966), 269–280.
[9] M. Horie, *On the genus field in algebraic number fields*. Tokyo J. Math. **6** (1983), 363–380.
[10] Y. Ihara, *Hecke Polynomials as congruence ζ functions in elliptic modular case*. Ann. of Math. (2) **85** (1967), 267–295.
[11] S. Iyanaga and T. Tamagawa, *Sur la théorie du corps de classes sur le corps des nombres rationnels*, J. Math. Soc. Japan, **1** (1951), 220–227.
[12] M. Kaneko and Y. Mizuno, *Genus character L-functions of quadratic orders and class numbers.* J. Lond. Math. Soc. (2) **102** (2020), 69–98.
[13] Y. Kitaoka, Arithmetic of quadratic forms, Cambridge tracts in Math. **106**, Cambridge Univ. Press, Cambridge, 1993.
[14] M. Kneser, *Strong approximation*, Algebraic groups and discontinuous subgroups, Proc. Symp. Pure Math. Vol IX. Amer. Math. Soc., Providence, RI, (1966), 187–196.
[15] F. Lemmermeyer, *The development of the principal genus theorem*, The shaping of arithmetic after C. F. Gauss's Disquisitiones Arithmeticae, Ed. by C. Goldstein, N. Schappacher, J. Schwermer. Springer, Berlin, (2007), 529–561.
[16] I. Reiner, Maximal orders, London Math. Soc. Monographs, New series **28**, Oxford Science Publications, 2003.
[17] C. L. Siegel, Analytische Zahlentheorie I, II, Vorlesung, gehalten im Wintersemester 1963/64 an der Universität Göttingen, Mathematisches Institut der Universität Göttingen, 1965.
[18] H. Weber, Lehrbuch der Algebra Vol. III, Chelsea Publ, Co., New York, 1961.
[19] A. Weil, Basic Number Theory, Die Grundlehren der mathematischen Wissenschaften **144**, Springer-Verlag New York, Inc., New York, 1967.

Department of Mathematics, Graduate School of Mathematics, Osaka University, Machikaneyama 1-1, Toyonaka,Osaka, 560-0043 Japan
Email address: ibukiyam@math.sci.osaka-u.ac.jp