L.J. Goldstein
Nagoya Math. J.
Vol. 45 (1971), 119–127

ON PRIME DISCRIMINANTS

LARRY JOEL GOLDSTEIN[1]

1. Introduction.

Let $L = \boldsymbol{Q}(\sqrt{d}\,)$ be a quadratic field of discriminant d. We say that d is a *prime discriminant* if d is divisible by exactly one rational prime. It is classically known that the prime discriminants are given by

$$-4,\ \pm 8,\ (-1)^{\frac{p-1}{2}} p \quad (p \text{ an odd prime}).$$

Further, it is known that every discriminant d of a quadratic field can be written uniquely in the form

$$d = d_1 \cdots d_t,$$

where $d_1, \cdots, d_t$ are distinct prime discriminants. (See, for example, [2, p. 75].) In this paper, we will prove a generalization of these facts.

Let K be an algebraic number field of narrow[2] class number 1 and let L be a quadratic extension of K. Let $\mathcal{O}_K$ (resp. $\mathcal{O}_L$) denote the ring of integers of K (resp. L). Since K has class number 1, L has a relative integral basis $\{\alpha_1, \alpha_2\}$ over K. The relative discriminant

$$\Delta_{L/K}(\alpha_1, \alpha_2)$$

is a non-zero integer of K. Furthermore, if $\{\alpha_1', \alpha_2'\}$ is another relative integral basis of L over K, then

$$\Delta_{L/K}(\alpha_1', \alpha_2') = \varepsilon^2 \Delta_{L/K}(\alpha_1, \alpha_2), \tag{1}$$

where $\varepsilon \in U_K$, $U_K =$ the group of units of $\mathcal{O}_K$. Let

Received April 28, 1971.

1) Research was supported by National Science Research Grant GP–20538.

2) Let I_K denote the group of all K-ideals, $P_K^0 =$ the group of all principal K-ideals (α), with α totally positive. The narrow class number of K is the order of I_K/P_K^0. Class field theory implies that the narrow class number 1 is if and only if K has no non-trivial abelian extension which is unramified at all finite K-primes. If the narrow class number of K is 1, then the ordinary class number of K is 1.

$$\mathcal{S}(K) = \{\Delta_{L/K}(\alpha_1, \alpha_2)\}$$

where L varies over all quadratic extensions of K and $\{\alpha_1, \alpha_2\}$ varies over all relative integral bases of L over K. An element of $\mathcal{S}(K)$ is called a *K-discriminant*. A K-discriminant which is divisible by exactly one K-prime is called a *prime K-discriminant*. We say that two K-discriminants d, d' are *equivalent* if $d = \varepsilon^2 d'$ for some $\varepsilon \in U_K$. The first main result of this paper is

THEOREM A. *Let K be totally real of narrow class number* 1, *and let $d \in \mathcal{S}(K)$. Then d can be written in the form*

$$d = \pi_1 \cdots \pi_t,$$

where π_i $(1 \leq i \leq t)$ are distinct prime K-discriminants.

Let $d = \pi_1 \cdots \pi_t = \pi_1' \cdots \pi_s'$ be two decompositions of the K-discriminant d into the product of distinct prime K-discriminants. We will say that the two decompositions are *equivalent* if $s = t$ and, after suitably renumbering $\pi_1, \cdots, \pi_t$, we have π_i equivalent to π_i' for $1 \leq i \leq t$. Our second main result is

THEOREM B. *Let K be totally real of narrow class number* 1, *and let $d \in \mathcal{S}(K)$ and let L be a quadratic extension of K having d as the discriminant of some relative integral basis of L over K. Let d be divisible by t distinct K-primes, and let L^* = the maximal abelian extension of K which is unramified over L at all finite primes. Then:*

(1) $\deg(L^*/L) \geq 2^{t-1}$.

(2) *All decompositions of d into a product of prime discriminants are equivalent to one another* $\Longleftrightarrow$ $\deg(L^*/L) = 2^{t-1}$.

The author wishes to thank Professor Tomio Kubota for several valuable suggestions.

2. Generalization of Furuta's Genus Formula.

In this paragraph, let K be any number field and let L/K be an abelian extension. Let L^* denote the maximal abelian extension of K which contains L and is such that L^*/L is unramified at all finite L-primes. We will refer to L^* as the *weak genus field* of L/K, and $\deg(L^*/L)$ as the *weak genus number* of L/K. Furuta [1] has introduced a similar notion which assumes that L^*/L is unramified also at infinite L-primes. In this case, we will refer to the *strong genus field* of L/K and the *strong genus number* of L/K.

Let h_K denote the ordinary class number of K, S_∞ = the set of infinite K-primes, $S_{\infty,1}$ = the set of real K-primes, $S_{\infty,2}$ = the set of complex K-primes, r_i = the number of elements in $S_{\infty,i}$ $(i = 1, 2)$. We will prove

THOEREM 2.1. *The weak genus number of L/K is given by*

$$\deg(L^*/L) = \frac{h_K 2^{r_1} \prod_{\mathfrak{p} \notin S_\infty} e_\mathfrak{p}}{\deg(L/K) \cdot [U_K : U_{L/K}]},$$

where $\mathfrak{p}$ runs over primes of K, $e_\mathfrak{p}$ = the ramification index of $\mathfrak{p}$ in L/K, U_K = the group of units of the ring of K-integers, $U_{L/K}$ = the group of units of the ring of K-integers, which are local norms at all finite primes and are totally positive.

Our proof will follow the derivation of Furuta's formula [1] for the strong genus number.

LEMMA 2.2. [1, p. 282]. *Let J_L denote the group of ideles of L and let $\hat{H}$ be an admissible subgroup of J_L, $\hat{L}$ = the class field over L corresponding to $\hat{H}$. Let $\hat{L}_0$ be the maximal abelian extension of K which is contained in $\hat{L}$. Then $K^\times \cdot (N_{L/K}\hat{H})$ is the admissible subgroup of J_K corresponding to $\hat{L}_0$, where $N_{L/K}$ denotes the idele norm from L to K.*

LEMMA 2.3. *Let H^* denote the admissible subgroup of J_K corresponding to L^*, where J_K = the idele group of K. Then*

$$H^* = K^\times \cdot \prod_{\mathfrak{p} \in S_{\infty,1}} \boldsymbol{R}_+ \times \prod_{\mathfrak{p} \in S_{\infty,2}} \boldsymbol{C}^\times \prod_{\mathfrak{p} \notin S_\infty} NU_\mathfrak{P},$$

where $\boldsymbol{R}_+ = \{x \in \boldsymbol{R} \mid x > 0\}$, $\boldsymbol{C}^\times = \boldsymbol{C} - \{0\}$, $\mathfrak{P}$ = a prime divisor of $\mathfrak{p}$ in L, $U_\mathfrak{P}$ = the local unit group at $\mathfrak{P}$ and N = the local norm from $L_\mathfrak{P}$ to $K_\mathfrak{p}$.

Proof. Let $\hat{L}$ = the maximal abelian extension of L which is unramified at all finite L-primes. Then the admissible subgroup of J_L corresponding to L is given by

$$L^\times \cdot \prod_{\mathfrak{P}\ \text{real}} \boldsymbol{R}_+ \prod_{\mathfrak{P}\ \text{complex}} \boldsymbol{C}^\times \times \prod_{\mathfrak{P}\ \text{finite}} U_\mathfrak{P}.$$

But L^* = the maximal abelian extension of K contained in L. Thus, the Lemma follows from Lemma 2.2.

Let us now prove Theorem 2.1. Let U denote the group of unit ideles of K. Then

$$\begin{aligned}
\deg(L^*/L) &= \frac{\deg(L^*/K)}{\deg(L/K)} \\
&= \frac{(J_K : H^*)}{\deg(L/K)} \\
&= \frac{(J_K : K^\times U)(K^\times U : H^*)}{\deg(L/K)} \\
&= \frac{h_K(K^\times U : H^*)}{\deg(L/K)} \quad (\text{since } J_K/K^\times U \approx \text{the ideal class group of } K) \\
&= \frac{h_K(H^*U : H^*)}{\deg(L/K)} \quad (\text{since } H^* \supseteq K^\times) \\
&= \frac{h_K(U : H^* \cap U)}{\deg(L/K)} = \frac{h_K}{\deg(L/K)} \frac{(U : C)}{(H^* \cap U : C)},
\end{aligned}$$

where $C = \prod_{\mathfrak{p} \in S_{\infty,1}} \boldsymbol{R}_+ \times \prod_{\mathfrak{p} \in S_{\infty,2}} \boldsymbol{C}^\times \times \prod_{\mathfrak{p} \notin S_\infty} NU_{\mathfrak{P}} \subseteq H^* \cap U$ (Lemma 2.3). But

$$(U : C) = 2^{r_1} \cdot \prod_{\mathfrak{p} \notin S_\infty} e_{\mathfrak{p}}.$$

Further, it is easy to see that $H^* \cap U = (K^\times \cap U) \cdot C$. Therefore,

$$\begin{aligned}
(H^* \cap U : C) &= ((K^\times \cap U) \cdot C : C) \\
&= (K^\times \cap U : K^\times \cap U \cap C) \\
&= (U_K : U_{L/K}).
\end{aligned}$$

COROLLARY 2.4. *Let L/K be a quadratic extension with relative discriminant $d_{L/K}$. Further, assume that K is totally real and that $d_{L/K}$ is divisible by t distinct K primes. Then*

$$\deg(L^*/L) \geq h_K \cdot 2^{t-1}.$$

Proof. Let $U_K^2 = \{u^2 \mid u \in U_K\}$. Then $U_{L/K} \supseteq U_K^2$. Moreover, since K is totally real, Dirichlet's unit theorem implies that

$$U_K \approx \{\pm 1\} \times \boldsymbol{Z}^{r_1 - 1}.$$

Therefore,

$$\begin{aligned}
[U_K : U_{L/K}] &\leq [U_K : U_K^2] \\
&\leq 2^{r_1}
\end{aligned}$$

Thus, by Theorem 2.1,

$$\deg(L^*/L) \geq h_K \cdot 2^{t-1}.$$

3. Some Lemmas.

Throughout the remainder of this paper, let K be a totally real number field of narrow class number 1. Let $d \in \mathcal{S}(K)$ and let us fix a quadratic extension L of K and a relative integral basis $\{\alpha_1, \alpha_2\}$ of L over K such that $d = \Delta_{L/K}(\alpha_1, \alpha_2)$. Further, let L^* denote the genus field of L/K, H^*=the admissible subgroup of J_K which corresponds to L^*.

LEMMA 3.1. Gal (L^*/K) *is an abelian group of exponent* 2 *and therefore*

$$\mathrm{Gal}\,(L^*/K) \approx \boldsymbol{Z}/(2) \oplus \cdots \oplus \boldsymbol{Z}/(2),$$

where $\boldsymbol{Z}/(2)$ *denotes the additive group of integers modulo* 2.

Proof. By class field theory,

$$\begin{aligned} \mathrm{Gal}\,(L^*/K) &\approx J_K/H^* \\ &\approx J_K/K^\times \cdot C, \end{aligned} \tag{2}$$

where $C = \prod_{\mathfrak{p} \in S_{\infty,1}} \boldsymbol{R}_+ \times \prod_{\mathfrak{p} \in S_{\infty,2}} \boldsymbol{C}^\times \times \prod_{\mathfrak{p} \in S_\infty} NU_{\mathfrak{P}}$, and where we have applied Lemma 2.3. Let U denote the subgroup of all unit ideles of J_K. Then $J_K/K^\times \cdot U$ is isomorphic to the ideal class group of K. But since K has class number 1, $J_K = K^\times \cdot U$. Therefore, in order to prove the Lemma, it suffices to show that if $\alpha \in U$, then $\alpha^2 \in K^\times \cdot C$. But this is obvious.

LEMMA 3.2. $L = K(\sqrt{d})$.

Proof. Since L/K is a quadratic extension and K has class number 1, $L = K(\sqrt{\mu})$, where $\mu \in \mathcal{O}_K$ is square-free. Let us show that

$$d = \mu \eta^2 \quad (\eta \in \mathcal{O}_K). \tag{3}$$

This will suffice to prove the Lemma. In order to prove (3), let us explicitly construct a relative integral basis of L/K whose discriminant is of the form $\mu \cdot \tau^2$ $(\tau \in \mathcal{O}_K)$. By (1), this suffices to prove (3). Let

$$2\mathcal{O}_K = \mathfrak{p}_1^{a_1} \cdots \mathfrak{p}_t^{a_t},$$

where $\mathfrak{p}_i$ $(1 \leq i \leq t)$ denotes a K-prime. Suppose that

$$\mathfrak{p}_i \nmid \mu (1 \leq i \leq s), \quad \mathfrak{p}_i | \mu \mathcal{O}_K \ (s+1 \leq i \leq t).$$

Let r_i $(1 \leq i \leq s)$ be the largest non-negative integer $\leq a_i$ such that

$$\mu \equiv u_i^2 \ (\mathrm{mod}\ \mathfrak{p}_i^{2r_i}),$$

for some K integer u_i. Then a classical result asserts that the relative discriminant $d_{L/K}$ of L over K is given by

$$d_{L/K}=\prod_{i=1}^{s}\mathfrak{p}_i^{2(a_i-r_i)}\cdot\prod_{i=s+1}^{t}\mathfrak{p}_i^{2a_i}\cdot\mu\mathcal{O}_K. \tag{4}$$

Further, if we choose $b\in\mathcal{O}_K$ so that

$$b\equiv u_i \pmod{\mathfrak{p}_i^{r_i}}\quad(1\le i\le s),$$

then $b^2\equiv\mu \pmod{\mathfrak{p}_i^{2r_i}}$ $(1\le i\le s)$. Choose π_i so that $\mathfrak{p}_i=\pi_i\mathcal{O}_K$ $(1\le i\le s)$, and set $\lambda=\prod_{i=1}^{s}\pi_i^{r_i}$. Then, by (4),

$$\alpha_1=1,\quad \alpha_2=\frac{b-\sqrt{\mu}}{\lambda}$$

is an integral basis of L over K. And the relative discriminant of this basis is $\mu\cdot(4/\lambda^2)$.

4. Proof of Theorems *A* and *B*.

Let all notations be as in Section 3. By Lemma 3.1, we have

$$L^*=K(\sqrt{\alpha_1},\cdots,\sqrt{\alpha_r})$$

for some $\alpha_1,\cdots,\alpha_r\in K^\times$, where $2^r=\deg(L^*/K)$. By Corollary 2.4, $r\ge t$. Further, by Lemma 3.2, we may choose $\alpha_1,\cdots,\alpha_r$ to be K-discriminants. For if β_i is the relative discriminant of some relative integral basis of $K(\sqrt{\alpha_1})$, then Lemma 3.2 implies that $K(\sqrt{\alpha_i})=K(\sqrt{\beta_i})$. Thus, throughout, let us assume that $\alpha_1,\cdots,\alpha_r$ are chosen to be K-dicsriminants. Note that none of $\alpha_1,\cdots,\alpha_r$ are K-units since K has narrow class number 1. If $t=1$, then d is a prime discriminant and thus we can trivially write d as a product of prime discriminants. Thus, let us assume $t>1$, and let us proceed by induction on t. Since $t>1$, we have $r>1$. Let $\mathfrak{p}_1,\cdots,\mathfrak{p}_r$ be the distinct finite K primes dividing d.

Reduction 1. We may assume that no α_i is divisible by all of $\mathfrak{p}_1,\cdots,\mathfrak{p}_t$.

For assume that $\mathfrak{p}_1\mathfrak{p}_2\cdots\mathfrak{p}_t|\alpha_1$. Then $\mathfrak{p}_1,\mathfrak{p}_2,\cdots,\mathfrak{p}_t$ all ramify in $K(\sqrt{\alpha_1})$. Since $\deg(L/K)=2$ and L^*/L is unramified at all finite L-primes, we see that $K(\sqrt{\alpha_1},\sqrt{\alpha_2})/K(\sqrt{\alpha_1})$ is unramified. Therefore, the relative discriminant of $K(\sqrt{\alpha_1},\sqrt{\alpha_2})/K$ is given by $\alpha_1^2\mathcal{O}_K$. However, since the relative discriminant of $K(\sqrt{\alpha_2})/K$ is given by $\alpha_2\mathcal{O}_K$, we see that the relative discriminant of $K(\sqrt{\alpha_1}, \sqrt{\alpha_2})/K$ is divisible by $\alpha_2^2\mathcal{O}_K$. Thus, $\alpha_2|\alpha_1$. Let $\alpha_1' = \alpha_1\alpha_2^{-1}\in\mathcal{O}_K$. Then $L^* = K(\sqrt{\alpha_1'}, \sqrt{\alpha_2}, \cdots, \sqrt{\alpha_r})$. Moreover, since α_2 is not a unit, and since every K-prime has ramification index at most 2 in L^*/K, we see that not all of $\mathfrak{p}_1, \cdots, \mathfrak{p}_r$ ramify in $K(\sqrt{\alpha_1'})/K$. Let α_1'' be relative discriminant of a relative integral basis of $K(\sqrt{\alpha_1'})/K$. Then $K(\sqrt{\alpha_1'}) = K(\sqrt{\alpha_1''})$ and not all of $\mathfrak{p}_1, \cdots, \mathfrak{p}_t$ divide α''. Thus, $L^*=K(\sqrt{\alpha_1''}, \sqrt{\alpha_2}, \cdots, \sqrt{\alpha_r})$ and α_1'' is not divisible by all of $\mathfrak{p}_1, \cdots, \mathfrak{p}_t$. Repeating this construction, we may guarantee that a similar condition holds for $\alpha_2, \cdots, \alpha_r$, thus validating the reduction.

Henceforth, let us assume that the reduction has been carried out. By the induction hypothesis, α_i can be written as a product of prime K-discriminants

$$\alpha_1 = \pi_1^{(i)}\cdots\pi_{j(i)}^{(i)} \qquad (1\leq i\leq r).$$

Then

$$K(\sqrt{\pi_1^{(1)}}, \sqrt{\pi_2^{(1)}}, \cdots, \sqrt{\pi_{j(r)}^{(r)}}) = L^{**}$$

is an abelian extension of K which is unramified over L. Therefore, since we clearly have $L^{**} \supseteq L^* = K(\sqrt{\alpha_1}, \cdots, \sqrt{\alpha_r})$, the definition of L^* implies that $L^{**} = L^*$. Therefore, we have

Reduction 2. We may assume that $\alpha_1, \cdots, \alpha_r$ are prime discriminants.

By Reduction 2, each α_i is divisible by exactly one K-prime and this K-prime must be one of $\mathfrak{p}_1, \cdots, \mathfrak{p}_t$. Let us renumber the α_i so that

$$\mathfrak{p}_i|\alpha_i \quad (1\leq i\leq t).$$

Let us show that

$$d = \varepsilon^2\cdot\alpha_1\cdot\alpha_2\cdots\alpha_t, \tag{*}$$

where $\varepsilon\in U_K$. This will immediately imply that d is a product of prime discriminants.

Since $L^*/K(\sqrt{d})$ is unramified at all finite K-primes, we see that $K(\sqrt{d})$ is the largest subfield of L^* which contains K and in which all of $\mathfrak{p}_1, \cdots, \mathfrak{p}_t$ are totally ramified. On the other hand, since $L^* = K(\sqrt{\alpha_1}, \cdots, \sqrt{\alpha_r})$, we see that $K(\sqrt{\alpha_1\cdots\alpha_t})$ is a quadratic extension of K, contained in L^*, in

L^*, which all of $\mathfrak{p}_1, \cdots, \mathfrak{p}_t$ are totally ramified. Therefore,

$$K(\sqrt{d}) = K(\sqrt{\alpha_1 \cdots \alpha_t})$$
$$\Longrightarrow d = \eta^2 \cdot \alpha_1 \cdots \alpha_t, \quad \eta \in K^\times. \tag{5}$$

Since $\deg(L^*/K(\sqrt{d})) = 2^{r-1}$ and since L^*/L is unramified at all finite primes, we see that the relative discriminant $d_{L^*/K}$ of L^* over K is given by

$$d_{L^*/K} = d^{2^{r-1}} \mathcal{O}_K. \tag{6}$$

Set $L_0 = K(\sqrt{\alpha_1}, \cdots, \sqrt{\alpha_t})$. Then, since each K-prime has ramification index at most 2 in L^*/K, we see that L^*/L_0 is unramified at all finite primes. But since the relative discriminant of $K(\sqrt{\alpha_i})/K$ is just $\alpha_i \mathcal{O}_K$, and since

$$(\alpha_i \mathcal{O}_K, \alpha_j \mathcal{O}_K) = 1 \quad (1 \leq i < j \leq t),$$

we see that the relative discriminant of L_0/K is given by

$$(\alpha_1 \cdots \alpha_t)^{2^{t-1}} \mathcal{O}_K.$$

Therefore, since L^*/L_0 is unramified at all finite primes,

$$d_{L^*/K} = [(\alpha_1 \cdots \alpha_t)^{2^{t-1}} \mathcal{O}_K]^{2^{r-t}}$$
$$= (\alpha_1 \cdots \alpha_t)^{2^{r-1}} \mathcal{O}_K. \tag{7}$$

Comparing (6) and (7) with (5), we see that η of (5) is a unit of $\mathcal{O}_K$, which proves the assertion (*). This completes the proof of Theorem A.

Note also that if $r > t$, then the above procedure can be applied to produce several inequivalent factorizations of d as a product of prime discriminants. Thus, if $r > t$, the expression of d as a product of prime discriminants is not unique. If $r = t$, and if $d = \alpha_1 \cdots \alpha_m$ is an expression of d as a product of prime discriminants, then $K(\sqrt{\alpha_1}, \cdots, \sqrt{\alpha_m})/K(\sqrt{d})$ is unramified at all finite primes. Therefore, $K(\sqrt{\alpha_1}, \cdots, \sqrt{\alpha_m}) \subseteq L^*$ and $m \leq r$. But since $\alpha_1, \cdots, \alpha_m$ are prime discriminants, we see that $m \geq t$, which implies that $m = r$ and

$$L^* = K(\sqrt{\alpha_1}, \cdots, \sqrt{\alpha_m}).$$

Therefore, $\alpha_1, \cdots, \alpha_m$ are uniquely determined by the extension L/K, up to multiplication by units of $\mathcal{O}_K$. Thus, all factorizations of d as a product of prime discriminants are equivalent in case $r = t$. This completes the proof of Theorem B.

5. An Example.

Let K be a real quadratic field with fundamental unit ε. Then

$$U_K = \{\pm \varepsilon^n \mid n \in \boldsymbol{Z}\}.$$

Further, we have

$$\{\varepsilon^n \mid n \in \boldsymbol{Z}\} \supseteq U_{L/K} \supseteq \{\varepsilon^{2n}\} n \in \boldsymbol{Z}\}.$$

Moreover, a unit $\eta \in U_K$ is a local norm at all K-primes $\Longleftrightarrow \eta$ is a (global) norm from, L, by Hasse's theorem and the fact that L/K is cyclic. Therefore, we conclude:

$$U_{L/K} = \{\varepsilon^n \mid n \in \boldsymbol{Z}\} \Longleftrightarrow N_{L/K}(\varepsilon) = +1 \text{ and } \varepsilon \text{ is a norm from } L.$$

In all other cases,

$$U_{L/K} = \{\varepsilon^{2n} \mid n \in \boldsymbol{Z}\}.$$

In the first case, $[U_K : U_{L/K}] = 2$, while in the second case $[U_K : U_{L/K}] = 4$. Therefore, by Theorem 2.1, we have $\deg(L^*/L) = 2^t$ in the first case and $\deg(L^*/L) = 2^{t-1}$ in the second case. Thus, we have

THEOREM 5.1. *Let K be a real quadratic field of narrow class number* 1, *d the relative discriminant of a quadratic extension L of K, ε = the fundamental unit of K. Then d can be written as a product of prime K-discriminants. If ε is not a norm from L, then all representations of d as a product of prime discriminants are equivalent. In all other cases, there exist at least two equivalent representations of d.*

BIBLIOGRAPHY

[1] Furuta, Y. "The Genus Field and Genus Number in Algebraic Number Fields," Nagoya Math. J. **29** (1967), pp. 281–285.

[2] Siegel, C.L. *Lectures on Advanced Analytic Number Theory*, Tata Institute of Fundamental Research, Bombay, 1961.

Department of Mathematics
University of Maryland
College Park, Maryland 20742