ON SEPARATION OF QUADRATIC FORMS
ON THE IMAGINARY QUADRATIC FIELD
IN ITS HILBERT CLASS FIELD

LI-CHIEN SHEN
(Communicated by Ken Ono)

Abstract. Let $K^{(1)}$ be the Hilbert class field of the imaginary quadratic field $K = \mathbb{Q}(\sqrt{d})$, $d < 0$. We derive the product representations of a class of Dirichlet L-series associated with the character group constructed from the Artin map between the ideal class group of $K$ and the Galois group $Gal(K^{(1)}/K)$. The application of the Mellin transform to the product representations of these Dirichlet series yields a family of generating functions for representations of positive integers by the subgroups of the quadratic forms.

1. Introduction

Let $K$ be a number field and $E$ a finite Galois extension of $K$. We introduce the following notation:

- $Gal(E/K) =$ the Galois group of $E$ over $K$,
- $\hat{G} =$ the character group of the group $G$,
- $O_K =$ the ring of integers of $K$,
- $I_K =$ the set of all fractional ideals of $K$,
- $P_K =$ the set of all principal fractional ideals of $K$,
- $C(O_K) = I_K/P_K =$ the ideal class group,
- $Z =$ the set of all rational integers.

The Hilbert class field $K^{(1)}$ of the field $K$ is the maximal unramified Abelian extension of $K$. The key idea of our work is based on the following statement concerning the ideal class group of $K$ and the Galois group $Gal(K^{(1)}/K)$:

**Theorem A** ([2], p. 109 or [3], p. 104). Let $K^{(1)}$ be the Hilbert class field of $K$. The Artin map

$$\left(\frac{K^{(1)}}{K}\right): I_K \to Gal(K^{(1)}/K)$$

is surjective and its kernel is precisely the subgroup of principal fractional ideals. Thus the Artin map induces an isomorphism between $C(O_K)$ and $Gal(K^{(1)}/K)$:

$$\Phi : C(O_K) \to Gal(K^{(1)}/K).$$

Received by the editors March 29, 2007, and, in revised form, July 18, 2007.

2000 Mathematics Subject Classification. Primary 11E25.

Key words and phrases. Artin map, Galois group, Hilbert class field, quadratic form.

©2008 American Mathematical Society
Reverts to public domain 28 years from publication.
Let $G = \text{Gal}(K^{(1)}/K)$. Let $\psi \in G^\wedge$ and $a \in I_K$. We define, with a slight abuse of notation,

$$\psi(a) = \psi\left(\frac{K^{(1)}|K}{a}\right).$$

Then $\psi$ is a character of $I_K$ and $\psi(a) = 1$ for all $a \in P_K$. The Dirichlet $L$ series of $\psi$ is defined as

$$L(s, \psi, K^{(1)}|K) = \sum_a \frac{\psi(a)}{N^s(a)},$$

where $a$ ranges over all non-zero ideals in $O_K$ and $N(a)$ is the norm of $a$. We will always assume the ideals to be non-zero. The series converges uniformly in the region $\text{Re} s \geq 1 + \delta$, $\delta > 0$ ([3], p. 117), and this requirement for $s$ is always assumed throughout the paper.

We recall that every $a \in I_K$ can be written uniquely as a product

$$a = \prod p_i^{r_i},$$

where $p_i$ are distinct prime ideals of $O_K$ and $r_i \in \mathbb{Z}$. Together with the fact that $\psi$ is multiplicative, $\psi(ab) = \psi(a)\psi(b)$, we can express the Dirichlet $L$ series as

$$L(s, \psi, K^{(1)}|K) = \prod_{p, \text{prime}} \left(1 - \frac{\psi(p)}{N^s(p)}\right)^{-1}. \tag{1.2}$$

In Section 2 we will consider this series in greater detail for the case where $K$ is the quadratic field. In Section 3, we further confine $K$ to the imaginary quadratic field and study the problem of representation of positive integers by the quadratic forms of $K$. We assume the reader is familiar with the basic theory of quadratic fields. A readable source for the subject of the quadratic fields can be found in [1], and an excellent account on the class field theory tailored particularly for the imaginary quadratic fields can be found in [2].

2. THE DIRICHLET SERIES OF THE QUADRATIC FIELDS

Let $K = \mathbb{Q}(\sqrt{d})$ be a quadratic field of discriminant $D$, where $d$ is square-free. Then $D \equiv 0, 1 \mod 4$. Moreover, $d = D$ if $D \equiv 1 \mod 4$ and $d = D/4$ if $D \equiv 0 \mod 4$.

Let $(D/n)$ be the Kronecker symbol ([I], p. 35). We recall the well-known result about the rules of decomposition of the rational primes into the prime ideals in the quadratic field $K$ ([I], p. 104 or [2], p. 145).

Let $p, q$ and $r$ be rational primes and for $a_1, a_2, \ldots, a_k \in K$, let $(a_1, a_2, \ldots, a_k)$ denote the fractional ideal of $K$ generated by $a_i, i = 1, 2, \ldots, k$.

1. If $(D/p) = 1$, then the prime $p$ splits into a product of two prime ideals in $O_K$: $(p) = p_1p_2$ and $N(p_1) = N(p_2) = p$, where $p_1 = (p, a + \sqrt{d})$, $p_2 = (p, a - \sqrt{d})$ and $a^2 \equiv d \mod p$.

2. If $(D/q) = -1$, then $\mathfrak{q} = (q)$ remains prime in $O_K$ and $N(\mathfrak{q}) = q^2$.

3. $\mathfrak{r} | D$ if and only if $(D/r) = 0$ and $(r) = (r, \sqrt{d})^2 = r^2$. Thus the prime $r$ ramifies and splits into a product of two identical prime ideals $\mathfrak{r}$ in $O_K$ with $N(\mathfrak{r}) = r$. 
We define
\( \chi \psi(p) = \psi(p_1) \) if \( (D/p) = 1 \),
\( \chi \psi(q) = \psi(q) \) if \( (D/q) = -1 \),
and
\( \chi \psi(r) = \psi(r) \) if \( (D/r) = 0 \).
For \( n = \prod p_i^{n_i} \), \( \chi \psi(n) = \prod \chi \psi(p_i) \).
We decompose the product (1.2) into

\[
L(s, \psi, K^{(1)}|K) = \prod_1 \prod_2 \prod_3.
\]

Here \( \prod_1 \) is the product over all ideals \( q = (q) \) in \( O_K \) where \( (D/q) = -1 \). \( \prod_2 \) is the product over all ideals \( p \) derived from the ideal \( (p) \) in \( O_K \) for which \( (D/p) = 1 \); we recall that these ideals decompose into two prime ideals in \( O_K \): \( (p) = p_1 p_2 \) and \( N(p_1) = N(p_2) = p \). \( \prod_3 \) is the product over all ideals \( r \) derived from \( (r) \) in \( O_K \) for which \( (D/r) = 0 \); these ideals decompose into two identical prime ideals in \( O_K \): \( (r) = r^2 \) and \( N(r) = r \).

**Lemma 1.** Let \( p, q \) and \( r \) be the rational primes described above. Then
\[
\chi \psi(p) = \overline{\psi}(p_2) \text{ if } (D/p) = 1,
\]
\[
\chi \psi(q) = 1 \text{ if } (D/q) = -1;
\]
and for \( (D/r) = 0 \)
\[
\chi \psi(r) = 1
\]
if \( r = (r, \sqrt{d}) \) is a principal ideal, otherwise there exists a \( \psi \in G^\wedge \) such that \( \chi \psi(r) = -1 \).

**Proof.** Since the Artin map takes the principal ideals to the identity element of \( G \),
we derive from the multiplicativity of \( \psi \) and the definition of \( \chi \psi \)
\[
1 = \psi((p)) = \psi(p_1 p_2) = \psi(p_1) \psi(p_2) = \chi \psi(p) \psi(p_2),
\]
\[
1 = \psi((q)) = \chi \psi(q)
\]
and
\[
1 = \psi((r)) = \psi^2(r) = \chi^2 \psi(r).
\]

Clearly the first two conclusions follow from the above relation and \( \chi \psi(r) = 1 \) if \( r \) is principal. If \( r \) is not principal, then for some \( \psi \in G^\wedge \), \( \psi(r) = -1 \), and hence the conclusion.

When there is no danger of confusion, we will simply write \( \chi \) for \( \chi \psi \).

**Lemma 2.**
\[
L(s, \psi, K^{(1)}|K) = \sum_{n=1}^{\infty} \frac{\chi(n)}{n^s} \sum_{k=1}^{\infty} \frac{(D/k)\chi(k)}{k^s}.
\]
Proof. Using the properties of $\chi$, we can write (2.1) as

$$L(s, \psi, K^{(1)}|K) = \prod_{1} \left(1 - \frac{1}{q^{2s}}\right)^{-1} \prod_{2} \left(1 - \frac{\chi(p)}{p^{s}}\right)^{-1} \prod_{3} \left(1 - \frac{\chi(r)}{r^{s}}\right)^{-1}$$

$$= \prod_{1} \left(1 - \frac{\chi(q)}{q^{s}}\right)^{-1} \left(1 - \frac{(D/q)\chi(q)}{q^{s}}\right)^{-1}$$

$$\times \prod_{2} \left(1 - \frac{\chi(p)}{p^{s}}\right)^{-1} \left(1 - \frac{(D/p)\chi(p)}{p^{s}}\right)^{-1}$$

$$\times \prod_{3} \left(1 - \frac{\chi(r)}{r^{s}}\right)^{-1} \left(1 - \frac{(D/r)\chi(r)}{r^{s}}\right)^{-1}$$

$$= \sum_{n=1}^{\infty} \frac{\chi(n)}{n^{s}} \sum_{k=1}^{\infty} \frac{(D/k)\chi(k)}{k^{s}}.$$}

Multiplying the above series together, we have

**Theorem 1.**

$$\sum_{a} \frac{\psi(a)}{N^{s}(a)} = \sum_{n=1}^{\infty} \left(\sum_{k|n} (D/k)\overline{\chi(k)}\chi(n/k)\right) \frac{1}{n^{s}}.$$ (2.2)

Recall that the Mellin transform of a function $f$ is defined as

$$(Mf)(s) = \frac{1}{\Gamma(s)} \int_{0}^{\infty} f(t)t^{s-1}dt.$$ 

Then for $f(t) = e^{-\alpha t}$ and $\Re \alpha > 0$,

$$(Mf)(s) = \alpha^{-s}.$$ 

Thus

$$M^{-1}(\alpha^{-s}) = e^{-\alpha t} = q^{\alpha},$$

where $q = e^{-t}$.

Applying the inverse Mellin transform to (2.2) by choosing $\alpha = N(a)$ and $n$, we obtain

**Corollary 1.**

$$\sum_{a} \psi(a)q^{N(a)} = \sum_{n=1}^{\infty} q^{\alpha} \left(\sum_{k|n} (D/k)\overline{\chi(k)}\chi(n/k)\right).$$

3. The quadratic forms of the imaginary quadratic fields

Throughout the remaining part of the work, the number field $K$ will be an imaginary quadratic field $Q(\sqrt{D})$ of discriminant $D < 0$.

Define $w = 4$ if $D = -4$, $w = 6$ if $D = -3$ and $w = 2$ for $D \neq -3, -4$. So $w$ counts the number of units in the ring $O_{K}$ of the quadratic field $Q(\sqrt{D})$.

We say $\alpha_{1}, \alpha_{2} \in O_{K}$ are associates if there exists a unit $u \in O_{K}$ such that $\alpha_{2} = u\alpha_{1}$. Hence each $\alpha$, including itself, has $w$ associates.
Let $C(O_K) = \{A_i, i = 1, 2, ..., h\}$ be the ideal class group of $K$. The class number $h$ is defined as the order of the ideal class group. We assign $A_1$ to be the principal ideal class.

Let $A \in C(O_K)$ and let $A^{-1}$ be its inverse. Let $a, b$ be ideals in $A$ and $A^{-1}$, respectively. We recall that

1. $a \in A$ if and only if there exists $b \in A^{-1}$ such that $(a) = ab$.
2. Let $a = [\alpha, \beta]$, where $\alpha, \beta$ is an ordered base for $a$. We can associate a primitive quadratic form $Q(x, y)$ with $a$ in the following manner ([11], p. 200):

$$Q(x, y) = \frac{N(\alpha x + \beta y)}{N(a)}.$$  

For a fixed ideal class $A$, the quadratic forms generated by $a \in A$ form an equivalent class of quadratic forms. For $i = 1, 2, ..., h$, let $Q_i(x, y)$ be a representative of the quadratic forms associated with the ideal class $A_i$. For the principal ideal $A_1$, we choose $Q_1(x, y)$ as follows:

$$Q_1(x, y) = x^2 + xy + \frac{1-D}{4}y^2 \text{ if } D \equiv 1 \mod 4$$

and

$$Q_1(x, y) = x^2 + (-D/4)y^2 \text{ if } D \equiv 0 \mod 4.$$  

We call $Q_1(x, y)$ the principal form.

(3) Since $\psi(a) = \psi(b)$ if $a, b \in A$, we define $\psi(Q) = \psi(A) = \psi(a), a \in A$.

**Lemma 3.** Let $Q(x, y)$ be a quadratic form associated with the ideal class $A$. Then

$$\sum_{b \in A^{-1}} \frac{1}{N^*(b)} = \frac{1}{w} \sum_{(m, n) \neq (0, 0)} \frac{1}{Q^*(m, n)}.$$  

**Proof.** Fix an ideal $a = [\alpha, \beta] \in A$. Then, for every $b \in A^{-1}$,

$$N(b) = \frac{N(a)N(b)}{N(a)} = \frac{N(\eta)}{N(a)} = Q(m, n),$$

where $\eta = ma + nb$ for some integers $m, n$. The conclusion follows easily from (3.1). The presence of $\frac{1}{w}$ is due to the $w$-to-one correspondence between the associates of $\eta$ and the ideal $(\eta)$ generated by $\eta$.

**Theorem 2.**

$$\sum_{i=1}^{h} \psi(Q_i) \sum_{(m, n) \neq (0, 0)} q^{Q_i(m, n)} = w \sum_{n=1}^{\infty} q^n \sum_{k|n} (D/k) \chi_{\psi(k)} \chi_{\psi(n/k)}.$$  

**Proof.** From Lemma 3,

$$\sum_{a} \frac{\psi(a)}{N^*(a)} = \frac{1}{w} \sum_{b \in A^{-1}} \frac{1}{N^*(b)} = \frac{1}{w} \sum_{i=1}^{h} \psi(A_i) \frac{1}{Q^*_i(m, n)}.$$  

In the last equality, we use the fact that $\psi(A_i^{-1}) = \psi(A_i) = \psi(Q_i)$. From (2.2) and (3.2),

$$\sum_{i=1}^{h} \psi(Q_i) \sum_{(m, n) \neq (0, 0)} \frac{1}{Q^*_i(m, n)} = w \sum_{n=1}^{\infty} q^n \sum_{k|n} (D/k) \chi_{\psi(k)} \chi_{\psi(n/k)}.$$  

Applying the inverse Mellin transform to (3.3), we obtain the conclusion.
Corollary 2.

\[ \sum_{m,n=-\infty}^{\infty} q^{Q(m,n)} = 1 + \frac{w}{h} \sum_{n=1}^{\infty} q^n \sum_{\psi} \psi(Q_j) \sum_{k|n}(D/k) \chi_\psi(k) \chi_\psi(n/k). \]

In particular,

\[ \sum_{m,n=-\infty}^{\infty} q^{Q_1(m,n)} = 1 + \frac{w}{h} \sum_{n=1}^{\infty} q^n \sum_{\psi} \sum_{k|n}(D/k) \chi_\psi(k) \chi_\psi(n/k). \]

Proof: This follows easily by summing the identity in Theorem 2 over all the characters \( \psi \) and observe that \( \frac{1}{h} \sum_{\psi} \psi(Q_j) \psi(Q_j) = \delta_{ij} \), the Kronecker delta function.

By equating the coefficients on both sides of the identity (3.4), we deduce

Corollary 3. Let \( N(n) \) denote the number of ways the positive integer \( n \) can be represented by the principal quadratic form \( Q_1(x,y) \). Then

\[ N(n) = \frac{w}{h} \sum_{n=1}^{\infty} \sum_{\psi} \sum_{k|n}(D/k) \chi_\psi(k) \chi_\psi(n/k). \]

The Artin map, in conjunction with the Galois theory, allows us to describe precisely the connection between the subgroups of \( C(O_K) \) and subfields of \( K^{(1)} \). We now derive an immediate consequence from it.

Let \( H \) be a subgroup of \( C(O_K) \). We say \( Q_1(x,y) \in H \) if \( A_i \in H \). From the Artin map (1.2), \( \Phi(H) \) is a subgroup of \( G \). Let \( M \) be the subfield of \( K^{(1)} \) fixed by the subgroup \( \Phi(H) \). Then \( G/\Phi(H) \cong Gal(M/K) \) and we have

Theorem 3.

\[ \sum_{m,n=-\infty}^{\infty} \sum_{Q \in H} q^{Q(m,n)} = |H| \left( 1 + \frac{w}{h} \sum_{n=1}^{\infty} q^n \sum_{\psi \in (G/\Phi(H))^\wedge} \sum_{k|n}(D/k) \chi_\psi(k) \chi_\psi(n/k) \right), \]

where \( |H| \) is the order of the subgroup \( H \) and \( (G/\Phi(H))^\wedge \), the character group of \( G/\Phi(H) \).

We mention a few interesting special cases of Theorem 3.

(1) \( H = \{ A_1 \} \). Then the formula (3.5) yields (3.4).

(2) Let \( H = C(O_K) \). Then \( \psi \equiv 1 \), hence \( \chi_\psi \equiv 1 \) and we derive (4, Theorem 4):

\[ \sum_{m,n=-\infty}^{\infty} \sum_{Q \in \psi} q^{Q(m,n)} = h + w \sum_{n=1}^{\infty} q^n \sum_{k|n}(D/k) = h + w \sum_{n=1}^{\infty} (D/n) \frac{q^n}{1 - q^n}. \]

(3) Let \( H = C(O_K)^2 \) be the subgroup of the principal genus. The corresponding field \( M \) is called the genus field of \( K \). It is well-known (2, pp. 120-127) that

\[ M = K(\sqrt{p_1}, \sqrt{p_2},..., \sqrt{p_r}), \]

where \( p_1, p_2, ..., p_r \) are the odd prime divisors of \( D \) and \( p_i^* = (-1)^{(p_i-1)/2} p_i \). Moreover,

\[ Gal(M/K) \cong (Z/2Z)^m, \]

where \( m = r \) or \( r - 1 \) according to \( D \equiv 0 \mod 4 \) or \( 1 \mod 4 \). Hence if \( \psi \in (G/C(O_K)^2)^\wedge \), the group of genus characters, it takes the value of either 1 or \(-1\).
Thus \( \chi_\psi = \chi_\psi \) for every \( \psi \). Hence, \( \chi_\psi (n/k) \chi_\psi (k) = \chi_\psi (n/k) \chi_\psi (k) = \chi_\psi (n) \), and Theorem 3 assumes a simpler form.

**Corollary 4.**

\[
\sum_{m,n=-\infty}^{\infty} q^{Q(m,n)} = |C(O_K)^2| \left( 1 + \sum_{n=1}^{\infty} q^n \sum_{\psi \in (G/\Phi(C(O_K)^2))^\wedge} \chi_\psi (n) \sum_{k|n} (D/k) \right).
\]

We note that when the principal genus consists of only one element, namely, the principal form, the above formula yields the generating function for representation of integers by the principal quadratic form involving all the genus characters.

**References**

2. D. Cox, Primes of the Form \( x^2 + ny^2 \), John Wiley and Sons, New York, 1989. MR1028322 (90m:11016)

Department of Mathematics, University of Florida, Gainesville, Florida 32611-2082

E-mail address: shen@math.ufl.edu

License or copyright restrictions may apply to redistribution; see http://www.ams.org/journal-terms-of-use