PROOF THAT CERTAIN IDEALS IN A CYCLOTOMIC REALM ARE PRINCIPAL IDEALS*

BY

HOWARD H. MITCHELL

1. Introduction

A theorem which serves to establish a connection between cyclotomy and the representation of numbers by quadratic forms is as follows:

Let λ represent a prime of the form $4n + 3$, and q a prime that is congruent to 1, mod λ. Further, let Σa, Σb represent the sums of those integers that are respectively quadratic residues and non-residues of λ and that lie between 0 and λ. Then it is always possible to find integers x, y such that

$$x^2 + \lambda y^2 = 4q^{(\Sigma b - \Sigma a)/\lambda}.$$

This theorem, which seems to have been discovered independently by Jacobi and Cauchy,† was extended by the latter to cases where λ is a composite integer of certain types.

An essentially equivalent theorem is that if $\mathfrak{q}$ be a prime ideal factor of q in the quadratic realm $k(\sqrt{-\lambda})$, then

$$\mathfrak{q}^{(\Sigma b - \Sigma a)/\lambda}$$

is a principal ideal.‡

This result was later extended by Eisenstein§ and Stickelberger‖ to cases where $q \not\equiv 1$, mod λ. When λ is prime, the theorem holds provided q is a quadratic residue of λ.

These results follow also from Dirichlet's determination of the number of classes of quadratic forms of determinant $-\lambda$.¶

* Presented to the Society, December 28, 1916.

† Jacobi, *Werke*, vol. 6, pp. 233, 240, 254, 275; Cauchy, *Oeuvres*, 1 Serie, vol. 5, pp. 52, 64, 85, 95; H. J. S. Smith, *Report on the Theory of Numbers, Collected Mathematical Works*, vol. 1, pp. 273–283; Bachmann, *Die Lehre von der Kreistheilung* (1872), p. 290.

‡ Hilbert, *Die Theorie der algebraischen Zahlkörper*, Jahresbericht der Deutschen Mathematiker-Vereinigung, vol. 4 (1894–95), p. 386; *Encyclopädie der Mathematischen Wissenschaften*, Bd. I, p. 703; *Encyclopédie des Sciences Mathématiques*, Tome I, volume 3, p. 448.

§ Journal für Mathematik, vol. 37 (1848), pp. 97–126.

‖ Mathematische Annalen, vol. 37 (1890), p. 360.

¶ Dirichlet-Dedekind, *Zahlentheorie*, 4th edition, § 104. For a determination of the closely related class number for ideals see Hilbert, l. c., p. 320.

The author obtains a theorem in this paper which may be regarded as a further extension of these results (for the case of λ prime) to realms of higher degree. Let λ denote any prime such that $\lambda - 1$ is not a power of 2, and let $2e$ denote a divisor of $\lambda - 1$ such that $(\lambda - 1)/(2e)$ is an odd integer other than unity. Let q be a prime such that

$$q^{(\lambda-1)/2e} \equiv 1, \qquad \mod \lambda.$$

Then in the realm of degree $2e$ determined by the $2e$ periods formed from λth roots of unity it is known that q is the product of $2e$ conjugate prime ideals, which form e conjugate imaginary pairs. Further, let h denote the "first factor" of the class number of the realm.* Then if one ideal be selected from each of the e conjugate imaginary pairs, and the product of these be raised to the power h, it will be shown that the result is a principal ideal.

Expressed in another way, this theorem would state that in whatever way q^h be expressed as the product of two conjugate imaginary factors that are relatively prime, the two factors are principal ideals. It then follows from a property of units that q^h may be expressed in exactly 2^{e-1} ways as the product of two actual conjugate imaginary factors that are relatively prime, provided two factors that differ merely in sign be regarded as the same.

Another result is that if two conjugate imaginary prime ideal factors of q be each raised to the power h, the ideals thus obtained belong to the same ideal class.

2. The modified Kummer function $\psi(\alpha)$

We consider the cyclotomic function of Jacobi and Cauchy as generalized by Kummer,†

$$\psi_{-a,-b}(\alpha) = \sum_{\tau} \alpha^{-b \operatorname{ind} \tau + (a+b) \operatorname{ind} (\tau+1)},$$

where α is a primitive λth root of unity, a, b integers such that $ab(a+b) \not\equiv 0$, mod λ, and the summation is to be taken over all the marks τ (except 0 and -1) of a Galois field of order q^t, where ind τ means the index with respect to a primitive root in the Galois field, and t is the smallest exponent such that $q^t \equiv 1$, mod λ.

This function has the properties:

$$\psi(\alpha^q) = \psi(\alpha),$$

$$\psi(\alpha)\psi(\alpha^{-1}) = q^t.$$

* Kummer, Journal für Mathematik, vol. 40 (1850), p. 112. Fuchs has given an extension to cases where λ is composite, ibid., vol. 65 (1866), pp. 102, 106.

† For the case where $q \equiv 1$, mod λ, see for example H. Weber, *Lehrbuch der Algebra* (1898), vol. 1, § 177, 178; vol. 2, § 203; for the general q, Kummer, Journal für Mathematik, vol. 44 (1851), pp. 106–121; Stickelberger, l. c., p. 335; the author, these Transactions, vol. 17 (1916), pp. 165–177.

We shall suppose that λ is prime and that t is odd. In view of the first of these properties the function belongs to the subrealm of the realm $k(\alpha)$ that is determined by the $(\lambda - 1)/t$ periods. In this realm q is the product of $(\lambda - 1)/t$ prime ideal factors, which are also prime in the realm $k(\alpha)$.

Aside from an error that has been corrected by the author,* Kummer determined the prime ideal factors of this function. Let $\mathfrak{q}_0 = \mathfrak{q}_0(\alpha)$ denote any one of the prime ideal factors of q, and let

$$\mathfrak{q}_i = \mathfrak{q}_0(\alpha^{\gamma^i}),$$

where γ denotes a primitive root of λ, and the index i is to be reduced, mod $(\lambda - 1)/t$. Then if we write

$$[\psi(\alpha)] = \prod_i \mathfrak{q}_i^{m_i},$$

and if the primitive root in the Galois field of order q^t be properly selected, the exponents m_i are determined by the equations,

$$m_i = S_{-i+\operatorname{ind} a} + S_{-i+\operatorname{ind} b} - S_{-i+\operatorname{ind}(a+b)},\dagger$$

where λS_j denotes the sum of all the positive integers between 0 and λ whose indices with respect to the primitive root γ are congruent to j, mod $(\lambda - 1)/t$.

We now denote by $2e$ any divisor of $\lambda - 1$ such that $(\lambda - 1)/2e$ is an odd integer other than unity, and assume that

$$q^{(\lambda-1)/2e} \equiv 1, \qquad \operatorname{mod} \lambda.$$

In case $t = (\lambda - 1)/2e$, the function $\psi(\alpha)$ belongs to the realm determined by the $2e$ periods and the ideals $\mathfrak{q}_i$ are the prime ideal factors of q in that realm. Hence

$$\prod_i \mathfrak{q}_i^{m_i} \qquad (i = 0, 1, \cdots, 2e - 1)$$

is a principal ideal.

We shall show that a similar statement holds in case t is a divisor of $(\lambda - 1)/2e$, say $t = (\lambda - 1)/2e'$, where e' is a multiple of e. In this case we consider the product of $\psi(\alpha)$ by those of its conjugates obtained by replacing α by

$$\alpha^{\gamma^{2e}}, \ \alpha^{\gamma^{4e}}, \ \cdots, \ \alpha^{\gamma^{2e'-2e}}.$$

This product is contained in the realm determined by the $2e$ periods. The exponents of the e'/e ideals,

$$\mathfrak{q}_i, \ \mathfrak{q}_{i+2e}, \ \cdots, \ \mathfrak{q}_{i+2e'-2e},$$

* L. c., p. 171.

† This expression may be obtained either from that given by the author (l. c., p. 173) by replacing i by γ^{-i}, or else from that given by Kummer (l. c., p. 120) in case the function is rep'aced by the proper one of its conjugates.

which are conjugate under these substitutions are each equal to

$$m_i + m_{i+2e} + \cdots + m_{i+2e'-2e}.$$

This sum may itself be represented in the form represented by m_i above provided λS_j is now considered to represent the sum of the integers between 0 and λ, whose indices are congruent to j, mod $2e$. Moreover the product of these e'/e conjugate ideals is a prime ideal in the realm determined by the $2e$ periods. If we represent it by $\mathfrak{q}_i$, where the index is now to be reduced, mod $2e$, and where $\mathfrak{q}_i = \mathfrak{q}_0(\alpha^{\gamma^i})$, we conclude that

$$\prod_i \mathfrak{q}_i^{m_i} \qquad (i = 0, 1, 2, \cdots, 2e-1)$$

is a principal ideal.

We now suppose that a, b are so chosen that

$$\text{ind } a \equiv 0, \qquad \text{ind } (a+b) \equiv \text{ind } b, \qquad \text{mod } 2e.$$

Since we are assuming that $(\lambda - 1)/2e$ is greater than 1, we may select them in such a way that the second condition is satisfied. Then by multiplying each of them by a properly selected residue, mod λ, the second condition will continue to hold, and the first condition can be satisfied. With these conditions imposed on a, b the exponents of the ideals assume the special values, $m_i = S_{-i}$.

3. Proof of the theorem

The functions conjugate to that considered above under the substitutions in which α is replaced by

$$\alpha^{\gamma}, \ \alpha^{\gamma^2}, \ \cdots, \ \alpha^{\gamma^{e-1}}$$

have the following expressions in terms of the prime ideal factors

$$\prod_i \mathfrak{q}_i^{m_{i-1}}, \ \prod_i \mathfrak{q}_i^{m_{i-2}}, \ \cdots, \ \prod_i \mathfrak{q}_i^{m_{i-e+1}}.$$

If now we raise the original function to the power p_0, and its conjugates to the powers $p_1, p_2, \cdots, p_{e-1}$ respectively, and then form the product, the exponent of $\mathfrak{q}_i$ in the product will be equal to

$$p_0 m_i + p_1 m_{i-1} + \cdots + p_{e-1} m_{i-e+1}.$$

If we equate these exponents for $i = 0, 1, \cdots, e-1$, we obtain $e-1$ equations which we write as follows:

$$p_0(m_i - m_0) + p_1(m_{i-1} - m_{-1}) + \cdots + p_{e-1}(m_{i-e+1} - m_{-e+1}) = 0 \qquad (i = 1, 2, \cdots, e-1)$$

In view of our assumption that $(\lambda - 1)/2e$ is odd, ind $(-1) \equiv e$, mod $2e$, and hence if a number r appears in the sum λS_j, $\lambda - r$ will appear in the

sum λS_{j+e}. Consequently

$$m_i + m_{i+e} = (\lambda - 1)/2e.$$

We set

$$m_i - m_{i+e} = d_i,$$

where d_i is an odd integer, and write the above equations in the form

$$p_0(d_i - d_0) + p_1(d_{i-1} - d_{-1}) + \cdots + p_{e-1}(d_{i-e+1} - d_{-e+1}) = 0.$$

If the exponents of the ideals $\mathfrak{q}_i$ be equated for $i = e, e+1, \cdots, 2e-1$, the same set of equations are obtained. Hence if rational integers $p_0, p_1, \cdots, p_{e-1}$ can be found to satisfy these equations, the product formed as described will assume the form

$$(\mathfrak{q}_0 \mathfrak{q}_1 \cdots \mathfrak{q}_{e-1})^k (\mathfrak{q}_e \mathfrak{q}_{e+1} \cdots \mathfrak{q}_{2e-1})^{k-h},$$

where k and h are integers, and hence

$$(\mathfrak{q}_0 \mathfrak{q}_1 \cdots \mathfrak{q}_{e-1})^h$$

will be a principal ideal.

These equations will all be satisfied if we take for the integers p_j the values,

$$p_j = D_j/2^{e-1},$$

where D_j denotes the minor of the element d_{-j} in the first row of the determinant

$$D = \begin{vmatrix} d_0 & d_{-1} & \cdots & d_{-e+1} \\ d_1 - d_0 & d_0 - d_{-1} & \cdots & d_{-e+2} - d_{-e+1} \\ d_2 - d_0 & d_1 - d_{-1} & \cdots & d_{-e+3} - d_{-e+1} \\ \vdots & \vdots & & \vdots \\ d_{e-1} - d_0 & d_{e-2} - d_{-1} & \cdots & d_0 - d_{-e+1} \end{vmatrix}.$$

The exponent h is equal to

$$p_0 d_0 + p_1 d_{-1} + \cdots + p_{e-1} d_{-e+1},$$

and if the p's have the values given above, this is equal to

$$h = D/2^{e-1}.$$

In view of the relations, $d_{-i} = -d_{e-i}$, the determinant D, if the first row be added to each of the others, belongs to the class known as "skew circulants,"* and may thus be expressed in the form

$$D = \prod_i (d_0 + d_{-1}\beta^i + d_{-2}\beta^{2i} + \cdots + d_{-e+1}\beta^{(e-1)i}),$$

where β is a primitive root of the equation $x^e = -1$, and the product is to be taken over the values $i = 1, 3, \cdots, 2e-1$.

* See, for example, Muir, *Theory of Determinants* (1882), pp. 187–191.

Since

$$d_{-j} = m_{-j} - m_{-j-e} = S_j - S_{j+e} = S_j + S_{j+e}\,\beta^{ei},$$

provided i is odd, we may write

$$h = \frac{1}{2^{e-1}} \prod_i (S_0 + S_1\,\beta^i + S_2\,\beta^{2i} + \cdots + S_{2e-1}\,\beta^{(2e-1)i}).$$

This expression is equal to the "first factor" of the class number of the realm determined by the $2e$ periods.*

This result may be made more general by observing that if instead of equating the exponents of the ideals $\mathfrak{q}_0, \mathfrak{q}_1, \cdots, \mathfrak{q}_{e-1}$, we had replaced part or all of them by their conjugate imaginary ideals, and followed the same procedure, the same value of h would have been obtained except possibly for sign. The only difference in the determinant D, when simplified by the addition of the first row to each of the others, would have been that the signs of all the elements in some of the rows would have been changed.

We therefore conclude that in whatever way q^h be represented as the product of two conjugate imaginary ideal factors that are relatively prime, those factors are principal ideals.

4. Some consequences and an example

There are two consequences of this theorem that may be mentioned. If in the expression

$$(\mathfrak{q}_0\,\mathfrak{q}_1 \cdots \mathfrak{q}_{e-1})^h$$

we replace one of the prime ideals $\mathfrak{q}_i$ by its conjugate imaginary $\mathfrak{q}_{i+e}$, and then form the quotient of the two expressions, we conclude that $\mathfrak{q}_i^h/\mathfrak{q}_{i+e}^h$ may be expressed as the quotient of two principal ideals and hence that $\mathfrak{q}_i^h$ and $\mathfrak{q}_{i+e}^h$ belong to the same ideal class.

Another consequence is that q^h may be represented in exactly 2^{e-1} ways as the product of two actual conjugate imaginary factors that are relatively prime, provided we regard as the same two factors that differ merely in sign. For if

$$q^h = F(\alpha)\,F(\alpha^{-1}),$$

and if $E(\alpha)$ denotes a unit such that

$$q^h = F(\alpha)\,E(\alpha)\,F(\alpha^{-1})\,E(\alpha^{-1}),$$

then $E(\alpha)\,E(\alpha^{-1}) = 1$. By a theorem due to Kummer† it follows from this that $E(\alpha)$ is a root of unity. But the only roots of unity in the realm determined by the $2e$ periods are ± 1.

* L. c.

† Extensions have been given by Kronecker and Minkowski; see Hilbert, l. c., p. 221.

As an example consider the case where $\lambda = 31$, $2e = 6$, $q = 2$. We select the primitive root γ of 31 to be 3, and represent by η_i the sum of the five 31st roots α^j such that $\text{ind}_3 j \equiv i$, mod 6. We find that $a = 1$, $b = 1$ satisfy the conditions,

$$\text{ind } a \equiv 0, \quad \text{mod } 6; \qquad \text{ind } b \equiv \text{ind } (a + b), \quad \text{mod } 6.$$

If then we select the primitive root in the Galois field of order 2^5 to be a root of the irreducible congruence

$$x^5 + x^2 + 1 \equiv 0, \quad \text{mod } 2,$$

we find that

$$\psi_{-1,-1}(\alpha) = \sum_{\tau} \alpha^{-\text{ind } \tau + 2 \text{ ind } (\tau+1)} = 2(\eta_0 + \eta_1 + \eta_3),$$

where the summation is taken over all the marks τ of the field except 0 and 1.

If $\mathfrak{q}_0$ is the properly selected prime ideal factor of 2, the exponents of the ideals $\mathfrak{q}_i$ are $m_i = S_{-i}$, and these are found to be respectively

$$1, 3, 3, 4, 2, 2$$

for $i \equiv 0, 1, 2, 3, 4, 5$, mod 6. The exponents of the ideal factors in the two conjugate functions obtained by replacing α by α^3 and α^9 are

$$2, 1, 3, 3, 4, 2,$$
$$2, 2, 1, 3, 3, 4.$$

Hence the exponents of the ideal factors in the product

$$\psi(\alpha)\psi^2(\alpha^3)\psi^4(\alpha^9)$$

are

$$13, 13, 13, 22, 22, 22.$$

We find that this product is equal to

$$2^{13}(-6 - \eta_0 + 10\eta_1 + 4\eta_2 + 5\eta_4 + \eta_5),$$

and we thus obtain an expression for 2^9 as the product of two conjugate imaginary factors, i. e.,

$$2^9 = (-6 - \eta_0 + 10\eta_1 + 4\eta_2 + 5\eta_4 + \eta_5) \times (-6 - \eta_3 + 10\eta_4 + 4\eta_5 + 5\eta_1 + \eta_2).$$

That these factors are relatively prime may be verified by noticing that their difference may be expressed in the form

$$1 + 6\eta_1 + 4\eta_2 + 2\eta_3 - 4\eta_4 - 2\eta_5,$$

which is obviously prime to 2. We readily find that 9 is the first factor of the class number of the realm under consideration.

Three other such factorizations of 2^9 are possible, two of which may be obtained from that given above by permuting the η's. In the other the factors would be expressible in terms of $\sqrt{-31}$, a case that has been fully treated by Stickelberger,* since, if the included quadratic realm is imaginary, its class number divides the first factor of the class number of the realm determined by the $2e$ periods. The class number of $k(\sqrt{-31})$ is 3, and we have obviously

$$2^3 = \frac{1+\sqrt{-31}}{2} \cdot \frac{1-\sqrt{-31}}{2}.$$

UNIVERSITY OF PENNSYLVANIA,
PHILADELPHIA, PA.

* L. c.