ON THE CLASS NUMBER OF A CYCLIC FIELD*

BY

CLAIBORNE G. LATIMER

1. Introduction. Let \( \Omega \) be the field defined by a primitive \( m \)th root of unity, \( m \) an integer \( > 2 \), and let \( F \) be a subfield of \( \Omega \). In a recent article,\(^*\) Gut showed that if \( F \) is real, the class number may be written \( h = \delta/R \), where \( R \) is the regulator of \( F \) and \( \delta \) is a product involving certain group characters. If \( F \) is imaginary, he showed that \( h = h_1 \cdot h_2 \), where \( h_1 \) is a closed expression and \( h_2 = \delta/R \), \( \delta \) and \( R \) being as before. If \( F = \Omega \) and \( m \) is an odd prime, Gut’s \( h_1 \) and \( h_2 \) are the same, except perhaps for sign, as Kummer’s well known first and second factors of the class number.

We shall assume hereafter that the Galois group \( \mathfrak{A} \) of \( F \) is cyclic. In this case, as noted by Gut, the \( \delta \) in his expression for \( h \), or \( h_2 \), may be written as a determinant. Employing this determinantal form, we shall show that \( \delta/R \), and hence \( h \) or \( h_2 \), is equal to \( N(\tau)/N(\mathfrak{A}) \), where \( N(\mathfrak{A}) \) is the norm of a non-singular ideal \( \mathfrak{A} \), in a set \( \mathfrak{O} \) of elements in a certain commutative algebra, and \( N(\tau) \) is the norm of a principal ideal \( \langle \tau \rangle \) in \( \mathfrak{O} \), \( \tau \) being an element in \( \mathfrak{O} \).\(^+\)

In certain cases our results may be expressed in terms of an ideal in a cyclotomic field. (See Theorem 2.) For the case where \( F \) is a cubic field, the discriminant of which is the square of a prime, Theorem 2 is equivalent to Eisenstein’s result that the number of classes of certain “associated (cubic) forms” is \( h = \mu^2 - \mu \nu + \nu^2 \), where \( \mu, \nu \) are rational integers.\(^\S\)

2. The ratio of two determinants. Let \( F \) be of degree \( E \) and let \( s \) be a generating substitution of \( \mathfrak{A} \). If \( \theta \) is a number of \( F \), not rational, it will be understood that \( \theta^{(i)} = s^i(\theta) \) (\( i = 1, 2, \ldots, E \)), \( \theta^{(E)} = \theta^{(0)} = \theta \). Let \( e = E \) or \( e = E/2 \) according as \( F \) is real or imaginary. Then \( \theta^{(i+e)} \) is the conjugate imaginary of \( \theta^{(i)} \) (\( i = 0, 1, 2, \ldots, e-1 \)).

Let \( \eta_1, \eta_2, \ldots, \eta_n \) be a fundamental set of units of \( F \). By Dirichlet’s well known theorem, \( n = e - 1 \). Since every \( \eta_i \) belongs to \( F \),

* Presented to the Society, December 28, 1931; received by the editors August 27, 1932.
\(^+\) It will be understood that we use the same definitions of terms referring to ideals in \( \mathfrak{O} \) as are given by MacDuffee in his article A n introduction to the theory of ideals, etc., these Transactions, vol. 31 (1929), p. 71. In case \( \mathfrak{O} \) is a set of integral algebraic numbers, these definitions are equivalent to the usual definitions.
\(^\S\) Journal für Mathematik, vol. 29 (1845), p. 49.
where \( u_i \) is a root of unity and the \( \alpha \)'s are rational integers. Let the \( n \)th order
matrix \( A = (\alpha_{ij}) \) and let \( I \) be the identity matrix.

**Lemma 1.** \( A \) is a root of

\[
f(x) = x^n + x^{n-1} + \cdots + x + 1 = 0,
\]

and it is not a root of an equation of lower degree with rational coefficients.

By (1), if \( 0 \leq k < E \),

\[
\eta_i^{(k)} = u_i^{(k)} \eta_{i1}^{(k)} \eta_{i2}^{(k)} \cdots \eta_{in}^{(k)} \quad (i = 1, 2, \cdots, n),
\]

where \( u_i^{(k)} \) is a root of unity and the matrix \( (\alpha_{ij}) = A^k \). Since \( \eta, \eta_i', \ldots, \eta_i^{(n-1)} = \pm 1 \), it follows that \( A \) is a root of

\[
f_1(x) = x^{n-1} + x^{n-2} + \cdots + x + 1 = 0.
\]

If \( F \) is real, it follows that \( A \) is a root of (2). Suppose \( F \) is imaginary. Then

\[
f_1(A) = f(A)(A^* + I) = 0.
\]

To prove that \( A \) is a root of (2), it suffices to show that \( A^* + I \) is non-singular.

Let \( A^* + I = (\beta_{ij}) \). We have

\[
\eta_{i1}^{(s)} = v_i \eta_{i1} \eta_{i2} \cdots \eta_{in} \quad (i = 1, 2, \cdots, n),
\]

where \( v_i \) is a root of unity. Suppose \( (\beta_{ij}) \) is singular. Then the system of equations

\[
\sum_{j=1}^{n} \beta_{ij} x_j = 0 \quad (i = 1, 2, \cdots, n)
\]

has a solution in rational integers, not all zero, and

\[
\phi = \prod_{i=1}^{n} (\eta_i \eta_i^{(s)})^{z_i}
\]

and every \( \phi^{(s)} \) is a root of unity. Let \( \lg \theta \) be the real logarithm of \( |\theta| \). Then

\[
\lg \theta^{(s)} = \lg \theta \quad \text{and, since } |\phi^{(s)}| = 1,
\]

\[
\sum_{j=1}^{n} x_j \lg \eta_j^{(s)} = 0 \quad (i = 0, 1, 2, \cdots, n - 1).
\]

From this it follows that the regulator, \( R = \pm \prod \eta_i \lg \eta_i' \cdots \lg \eta_i^{(n-1)} \) \((i = 1, 2, \cdots, n)\), of \( F \) is zero.* But this is known to be false. Hence \( A^* + I \)

is non-singular and \( A \) is a root of (2).

* We take the same definition of \( R \) as that used by Gut, loc. cit., p. 200.
It may be shown by the same method employed by Pollaczek on a similar problem\(^*\), that \(A\) is not a root of an equation of degree < \(n\) with rational coefficients. The lemma follows.

Let \(x_1, x_2, \ldots, x_n\) be independent variables and let

\[
(3) \quad x_i^{(k)} = \alpha_{1i} x_1 + \alpha_{2i} x_2 + \cdots + \alpha_{ni} x_n \quad (i = 1, 2, \ldots, n).
\]

For a fixed \(k\), the matrix of the forms \(x_i^{(k)}\) is the transpose of \(A^k\). By Lemma 1, \(A^n = I\). Thus we have a cyclic group of linear homogeneous substitutions \(S, S^2, \ldots, S^n = 1\), on the \(x\)'s. For every pair of integers \(i, k\),

\[
(4) \quad S^k(x_1^{(i)}, x_2^{(i)}, \ldots, x_n^{(i)}) = (x_1^{(i+k)}, x_2^{(i+k)}, \ldots, x_n^{(i+k)}),
\]

it being understood that if \(j \equiv j_1 \pmod{e}\), \(0 \leq j_1 < e\), then \(x_i^{(j)} = x_i^{(j_1)}\), \(x_i^{(0)} = x_i\) \((i = 1, 2, \ldots, n)\).

If \(\theta\) is a unit of \(F\), by (1) and (3)

\[
\theta = u_1 \eta_1 \eta_2 \eta_3 \cdots \eta_n, \\
\theta' = u_2 \eta_1' \eta_2' \eta_3' \cdots \eta_n',
\]

\[
(5) \quad \theta^{(n)} = u_n \eta_1^{(n)} \eta_2^{(n)} \eta_3^{(n)} \cdots \eta_n^{(n)},
\]

where the \(u\)'s are roots of unity and the \(x\)'s are rational integers. It will be observed that if we apply a substitution \(S^i\) to \(\theta\), the resulting unit is the same, except perhaps for a factor which is a root of unity, as that obtained by applying the substitution \(S^i\) to the \(x\)'s when \(\theta\) is written as in the first equation above.

If \(0 \leq t < e\) and if \(i + k \equiv t \pmod{e}\), by (4) and (5),

\[
\theta^{(t)} = u \eta_1^{(t)} \eta_2^{(t)} \eta_3^{(t)} \cdots \eta_n^{(t)},
\]

where \(u\) is a root of unity and \(z_j = x_j^{(t)}\) \((j = 1, 2, \ldots, n)\). Let the determinant of the \(x\)'s in the first \(n\) equations of (5) be \(\Psi(x_1, x_2, \ldots, x_n)\) and let

\[
(6) \quad \delta(\theta) = \begin{vmatrix}
\lg \theta & \lg \theta' & \cdots & \lg \theta^{(n-1)} \\
\lg \theta' & \lg \theta'' & \cdots & \lg \theta^{(n)} \\
. & . & . & . \\
\lg \theta^{(n-1)} & \lg \theta^{(n)} & \cdots & \lg \theta^{(n-2)}
\end{vmatrix}.
\]
Employing (6) and the same rule for the multiplication of determinants as for matrices, we find \( \Psi(x_1, x_2, \cdots, x_n) \cdot R = \pm \delta(\theta) \). Hence

\[
\Psi(x_1, x_2, \cdots, x_n) = \pm \frac{\delta(\theta)}{R}.
\]

3. The set \( \mathcal{O} \). The algebraic roots of (2) are distinct and hence the same is true of the factors of \( f(x) \) which are irreducible in the rational field.

Let \( C \) be any matrix such that (2) is the equation of minimum degree with rational coefficients, the leading coefficient being unity, which has \( C \) as a root. Let \( \mathcal{O} \) be the set of all polynomials in \( C \) with rational integral coefficients. It has been shown that there is a one-to-one correspondence between the classes of ideals in \( \mathcal{O} \) and certain classes of matrices.† Since (2) is the minimum equation of \( A \), by the proof of this result, there is a non-singular ideal \( \mathfrak{R} \) in \( \mathcal{O} \), with a basis \( \omega_1, \omega_2, \cdots, \omega_n \) such that

\[
C\omega_i = \alpha_{i1}\omega_1 + \alpha_{i2}\omega_2 + \cdots + \alpha_{in}\omega_n \quad (i = 1, 2, \cdots, n).
\]

Let \( \tau \) be an element in \( \mathfrak{R} \). By the last equations and (3),

\[
\tau = x_1\omega_1 + x_2\omega_2 + \cdots + x_n\omega_n,
\]

\[
C\tau = x'_1\omega_1 + x'_2\omega_2 + \cdots + x'_n\omega_n,
\]

\[
\cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots
\]

\[
C^{n-1}\tau = x'^{n-1}_1\omega_1 + x'^{n-1}_2\omega_2 + \cdots + x'^{n-1}_n\omega_n,
\]

where the \( x' \)'s are rational integers. The determinant of the coefficients of the \( \omega \)'s is \( \Psi(x_1, x_2, \cdots, x_n) \).

\( I, C, C^2, \cdots, C^{n-1} \) form a basis of \( \mathcal{O} \). Hence

\[
\omega_i = g_{i1}I + g_{i2}C + \cdots + g_{in}C^{n-1} \quad (i = 1, 2, \cdots, n),
\]

where the \( g \)'s are rational integers such that the absolute value of the determinant \( |g_{ij}| \) is the norm of \( \mathfrak{R} \). If we employ the last equations to eliminate the \( \omega \)'s in the above expressions for \( C^{i-1}\tau (i = 1, 2, \cdots, n) \), in the resulting equations the determinant of the coefficients of the powers of \( C \) is \( \Psi(x_1, x_2, \cdots, x_n) \cdot N(\mathfrak{R}) \). But the \( C^{i-1}\tau \) form a basis of the principal ideal \( \{ \tau \} \). Hence \( \Psi(x_1, x_2, \cdots, x_n) \cdot N(\mathfrak{R}) = \pm N(\tau) \). Since \( \mathfrak{R} \) is non-singular, \( N(\mathfrak{R}) \neq 0 \).

Therefore by (7) we have

* By employing Lemma 1, it may be shown that \( \Psi \) is an invariant of the above-mentioned substitution group. See Frick, Lehrbuch der Algebra, vol. 2, p. 14.

Lemma 2. If $\theta = \eta_1 \eta_2 \cdots \eta_n$ is a unit of $F$, where $u$ is a root of unity, then

$$\pm \frac{\delta(\theta)}{R} = \pm \Psi(x_1, x_2, \cdots, x_n) = \frac{N(\tau)}{N(\mathfrak{R})},$$

where $\mathfrak{R}$ is a non-singular ideal in $\mathfrak{O}$, with a basis $\omega_1, \omega_2, \cdots, \omega_n$ such that

$$c_0 = \alpha_1 \omega_1 + \alpha_2 \omega_2 + \cdots + \alpha_n \omega_n \quad (i = 1, 2, \cdots, n)$$

and $N(\tau)$ is the norm of the principal ideal $\{\tau\}$, $\tau = x_1 \omega_1 + x_2 \omega_2 + \cdots + x_n \omega_n$.

4. Proof of principal theorem. Let $\mathfrak{B}$ be the group which has as its elements the $\phi(m)$ integers in a reduced set of residues, modulo $m$. The numbers of $F$ are those numbers of $\mathfrak{O}$ which are unaltered under every substitution $(p, p^a)$, where $p$ is a primitive $m$th root of unity and $a$ is an integer in a subgroup $\mathfrak{U}$ of $\mathfrak{B}$. Let the co-sets (Neben gruppen) of $\mathfrak{B}$ with respect to $\mathfrak{U}$ be $\mathfrak{U}_0 = \mathfrak{U}, \mathfrak{U}_1, \mathfrak{U}_2, \cdots, \mathfrak{U}_{m-1}$. Then $\mathfrak{U}_i = \gamma_i \mathfrak{U}$ where the $\gamma_i$ are properly chosen integers. The factor group $\mathfrak{B}/\mathfrak{U}$ is simply isomorphic with $\mathfrak{B}^*$ which by hypothesis is cyclic. Hence we may assume that $s = (p, \rho^a)$, where $\gamma$ is an integer such that $\gamma^m \equiv a \pmod{m}$, $a$ an element in $\mathfrak{U}$. If $m$ is odd, we may assume that $\gamma$ is odd, while if $m$ is even, $\gamma$ is necessarily odd since the same is true of $a$.

If $F$ is real, by Gut’s results, $h = \Delta/R$ where

$$\Delta = \prod_{\chi} \sum_{k=1}^{m/2} - \frac{\chi(k) \log \sin \frac{\pi k}{m}}{m}.$$  

In the product, $\chi$ ranges over all the elements, except the identity element, of a group of characters which is simply isomorphic with $\mathfrak{B}$. Since $\mathfrak{B}$ is cyclic, we have

$$\Delta = \prod_{\chi} \sum_{k=1}^{m/2} - \frac{\chi(k) \log \sin \frac{\pi k}{m}}{m},$$

where $\chi$ is a fixed character. It may be shown that if $a$ and $b$ are prime to $m$, $\chi(a) = \chi(b)$ if and only if $a$ and $b$ are congruent, modulo $m$, to elements in the same co-set $\mathfrak{U}_i$. After proper choice of notation, we may assume that if $a$ belongs to $\mathfrak{U}_i$, $\chi(a) = \zeta^i$, where $\zeta$ is a primitive $m$th root of unity. Employing $\chi(m-k) = \chi(k)$, $\chi(k) = 0$ if $(m, k) > 1$, and $\sum_{k=1}^{m-1} \chi(k) = 0$ ($0 < t < e$), it may be shown that

$$2 \sum_{k=1}^{m/2} \chi(k) \log \sin \frac{\pi k}{m} = \sum_{k=1}^{m-1} \chi(k) \log (1 - \rho^k) = \sum_{i=0}^{e-1} \log \lambda_i,$$

† Gut, loc. cit., pp. 200, 223.
where \( \lambda_0 = \Pi (1 - \rho^v) \), \( a \) ranging over all the elements of \( U \), and \( \lambda_i = \lambda_0^{(i)} \) \( (i=1, 2, \ldots, n) \). Employing a well known property of cyclic determinants, it may be shown from (9) and (10) that

\[
\Delta = 2^{-n} \prod_{i=1}^{n} \sum_{i=0}^{n} \xi^{i} \log \lambda_i = \pm \delta(\theta),
\]

where \( \theta = (\lambda_1/\lambda_0)^{1/2} \). Hence \( h = \pm \delta(\theta)/R \). We shall show that \( \theta \) is a unit of \( F \). Since \( F \) is real, \( U \) contains \(-1\). Therefore \( \theta \) is a product of units in the form

\[
(1 - \rho^v)(1 - \rho^{-v})^{1/2}
\]

Since \( \gamma \) is odd, the unit on the left belongs to \( \Omega \), and hence the same is true of \( \theta \). Since \( \theta \) is unaltered under every substitution \((\rho, \rho^v)\), \( a \) in \( U \), it belongs to \( F \).

If \( F \) is imaginary, Gut’s expression for \( h \) may be written \( h = h_1 \cdot h_2 \), where \( h_1 \) is a closed expression and \( h_2 = \Delta/R \), where \( \Delta \) is exactly the same as the right side of (8), except that in this case \( \chi \) ranges over those characters, except the principal character, such that \( \chi(-1)=1 \).† The whole group of characters is simply isomorphic with \( \mathbb{F} \) and hence every character is a power of one of them. For a generating character \( \chi \), we have \( \chi(-1) = -1 \). Hence \( h_2 = \Delta/R \), where

\[
\Delta = \prod_{i=1}^{n} \sum_{k=1}^{m/2} - \chi^{2k}(k) \log \sin \frac{\pi k}{m}.
\]

Since \( s \theta \) is the conjugate imaginary of \( \theta \), the co-set \( U_* \) contains \(-1\) and we may take as the elements of \( U_{i+} \), the negatives of the elements in the corresponding \( U_i \). If \( a \) and \( b \) are prime to \( m \) and \( a \) is in \( U_i \), then \( \chi^2(a) = \chi^2(b) \) if and only if \( b \) is congruent to an element in \( U_i \) or in \( U_{i+} \). The notation for the co-sets may be so chosen that if \( a \) belongs to \( U_i \), then \( \chi^2(a) = \xi^i \), where \( \xi \) is a primitive \( p \)th root of unity. If we define the \( \lambda_i \) as before, let \( \theta = (\lambda_1 \cdot \lambda_{i+1} / \lambda_0 \cdot \lambda_i) \) and employ the fact that \( \lambda_{i+} \) is the conjugate imaginary of \( \lambda_i \), we find as before that \( \Delta = \pm \delta(\theta), h_2 = \pm \delta(\theta)/R \) and \( \theta \) is a real unit of \( F \). By Lemma 2, we have then the following, except the last sentence.

**Theorem 1.** Let \( F \) be a field, of degree \( E \), which is cyclic with respect to the rational field. Let \( e = E \) or \( e = E/2 \) according as \( F \) is real or imaginary, and let

---

† Gut, loc. cit., pp. 201, 223.
Let $\mathcal{O}$ be the set of all polynomials with rational integral coefficients in
the $n$th order matrix $A = (\alpha_i)$, where the $\alpha$'s are given in (1). If $F$ is real let $H$ be
the class number of $F$, and if $F$ is imaginary let $H$ be the absolute value of Gut's
second factor of the class number. Then

$$H = \frac{N(\tau)}{N(\mathcal{O})},$$

where $N(\mathcal{O})$ is the norm of a non-singular ideal $\mathcal{O}$ in $\mathcal{O}$ and $N(\tau)$ is the norm of
a principal ideal $\{\tau\}$ in $\mathcal{O}$, $\tau$ being an element in $\mathcal{O}$. If $F$ is the field defined by a
primitive $m$th root of unity, $m$ an odd prime, $\pm H$ is Kummer's second factor of
the class number.

To prove the last sentence of the theorem, it suffices to note that our $\theta$, $\delta(\theta)$, $R$, when properly specialized, are identical, except perhaps for sign,
with Kummer's $e(\alpha)$, $D$, $\Delta$ respectively.*

It will be observed that by the proof of the above theorem, $\pm H$ is repre-
sented by the form $\Psi(x_1, x_2, \ldots, x_n)$, which, as previously noted, is an in-
variant of the cyclic substitution group defined by the transpose of $A$.

5. A special case of Theorem 1. Suppose $e$ of Theorem 1 is an odd prime,
$F$ real or imaginary. Let $\xi$ be a primitive $e$th root of unity. $\xi$ is a root of (2),
and $1, \xi, \xi^2, \ldots, \xi^{e-1}$ form a basis of the integral numbers in the field $K$
deﬁned by $\xi$. Hence by Lemma 1, $\mathcal{O}$ is equivalent to the set of all integral
algebraic numbers in $K$. Then, by well known theorems in algebraic num-
biers, there is an ideal $\mathcal{I}$ such that $\{\tau\} = \mathcal{I} \mathcal{O}$ and $N(\tau) = N(\mathcal{O}) \cdot N(\mathcal{I})$. We have
then

**Theorem 2.** If $e$ in Theorem 1 is an odd prime,

$$H = N(\mathcal{O}),$$

where $\mathcal{O}$ is an ideal in the field defined by a primitive $e$th root of unity.

If $F$ is the field defined by a primitive $m$th root of unity, $m$ an odd prime,
and if $e = (m - 1)/2$ is also an odd prime, it may be shown that Kummer's
first factor of the class number is the norm of a principal ideal in $K$, $K$ as
above. Hence the class number of $F$ is the norm of an ideal in $K$.

* Journal für Mathematik, vol. 40 (1850), pp. 110, 99; Bulletin of the National Research Coun-
cil, loc. cit., p. 34.

University of Kentucky,
Lexington, Ky.