ON THE CLASS NUMBER OF A CYCLIC FIELD*

BY

CLAIBORNE G. LATIMER

1. **Introduction.** Let Ω be the field defined by a primitive mth root of unity, m an integer >2, and let F be a subfield of Ω. 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 δ 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 $h_2=\delta/R$, δ 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 δ in his expression for h, or h_2, may be written as a determinant. Employing this determinantal form, we shall show that δ/R, and hence h or h_2, is equal to $N(\tau)/N(\mathfrak{K})$, where $N(\mathfrak{K})$ is the norm of a non-singular ideal $\mathfrak{K}$, in a set $\mathfrak{G}$ of elements in a certain commutative algebra, and $N(\tau)$ is the norm of a principal ideal $\{\tau\}$ in $\mathfrak{G}$, τ being an element in $\mathfrak{K}$.‡

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 μ, ν are rational integers.§

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

Let $\eta_1,\ \eta_2,\ \cdots,\ \eta_n$ be a fundamental set of units of F. By Dirichlet's well known theorem, $n=e-1$. Since every η_i' belongs to F,

---

* Presented to the Society, December 28, 1931; received by the editors August 27, 1932.

† *Die Zetafunktion, die Klassenzahl und die Kronecker'sche Grenzformel eines beliebigen Kreiskörpers,* Commentarii Mathematici Helvetici, vol. 1 (1929), p. 160.

‡ It will be understood that we use the same definitions of terms referring to ideals in $\mathfrak{G}$ as are given by MacDuffee in his article *An introduction to the theory of ideals*, etc., these Transactions, vol. 31 (1929), p. 71. In case $\mathfrak{G}$ is a set of integral algebraic numbers, these definitions are equivalent to the usual definitions.

§ Journal für Mathematik, vol. 29 (1845), p. 49.

$$\eta_i' = u_i \eta_1^{\alpha_{i1}} \eta_2^{\alpha_{i2}} \cdots \eta_n^{\alpha_{in}} \qquad (i = 1, 2, \cdots, n), \tag{1}$$

where u_i is a root of unity and the α's are rational integers. Let the nth order matrix $A \equiv (\alpha_{ij})$ and let I be the identity matrix.

LEMMA 1. *A is a root of*

$$f(x) \equiv x^n + x^{n-1} + \cdots + x + I = 0, \tag{2}$$

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

By (1), if $0 \leqq k < E$,

$$\eta_i^{(k)} = u_i^{(k)} \eta_1^{\alpha_{i1}^{(k)}} \eta_2^{\alpha_{i2}^{(k)}} \cdots \eta_n^{\alpha_{in}^{(k)}} \qquad (i = 1, 2, \cdots, n),$$

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

$$f_1(x) \equiv x^{E-1} + x^{E-2} + \cdots + x + I = 0.$$

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

$$f_1(A) = f(A)(A^e + I) = 0.$$

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

Let $A^e + I \equiv (\beta_{ij})$. We have

$$\eta_i \eta_i^{(e)} = v_i \eta_1^{\beta_{i1}} \eta_2^{\beta_{in}} \cdots \eta_n^{\beta_{i2}} \qquad (i = 1, 2, \cdots, n),$$

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

$$\sum_{j=1}^{n} \beta_{ji} x_j = 0 \qquad (i = 1, 2, \cdots, n)$$

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

$$\phi \equiv \prod_{i=1}^{n} (\eta_i \eta_i^{(e)})^{x_i}$$

and every $\phi^{(i)}$ is a root of unity. Let $\lg \theta$ be the real logarithm of $|\theta|$. Then $\lg \theta^{(e)} = \lg \theta$ and, since $|\phi^{(i)}| = 1$,

$$\sum_{j=1}^{n} x_j \lg \eta_j^{(i)} = 0 \qquad (i = 0, 1, 2, \cdots, n-1).$$

From this it follows that the regulator, $R = \pm |\lg \eta_i \ \lg \eta_i' \cdots \lg \eta_i^{(n-1)}|$ $(i = 1, 2, \cdots, n)$, of F is zero.* But this is known to be false. Hence $A^e + I$ 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 $x_1, x_2, \cdots, x_n$ be independent variables and let

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

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

$$S^k(x_1^{(i)}, x_2^{(i)}, \cdots, x_n^{(i)}) = (x_1^{(i+k)}, x_2^{(i+k)}, \cdots, x_n^{(i+k)}), \tag{4}$$

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

If θ is a unit of F, by (1) and (3)

$$\begin{aligned} \theta &= u_1 \eta_1^{x_1} \eta_2^{x_2} \cdots \eta_n^{x_n}, \\ \theta' &= u_2 \eta_1^{x_1'} \eta_2^{x_2'} \cdots \eta_n^{x_n'}, \\ &\ \ \vdots \\ \theta^{(n)} &= u_n \eta_1^{x_1^{(n)}} \eta_2^{x_2^{(n)}} \cdots \eta_n^{x_n^{(n)}}, \end{aligned} \tag{5}$$

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 θ, 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 θ is written as in the first equation above.

If $0 \leqq t < e$ and if $i + k \equiv t \pmod e$, by (4) and (5),

$$\theta^{(t)} = u \eta_1^{(i)\, z_1} \eta_2^{(i)\, z_2} \cdots \eta_n^{(i)\, z_n},$$

where u is a root of unity and $z_j = x_j^{(k)}$ $(j = 1, 2, \cdots, n)$. Let the determinant of the x's in the first n equations of (5) be $\Psi(x_1, x_2, \cdots, x_n)$ and let

$$\delta(\theta) \equiv \begin{vmatrix} \lg \theta & \lg \theta' & \cdots \lg \theta^{(n-1)} \\ \lg \theta' & \lg \theta'' & \cdots \lg \theta^{(n)} \\ \cdot & \cdot & \cdots \cdot \\ \lg \theta^{(n-1)} & \lg \theta^{(n)} & \cdots \lg \theta^{(n-3)} \end{vmatrix}. \tag{6}$$

---

* Mathematische Zeitschrift, vol. 21 (1924), pp. 8, 9; Bulletin of the National Research Council, No. 62, *Algebraic Numbers*, II, pp. 94–96.

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*

$$\Psi(x_1, x_2, \cdots, x_n) = \pm \frac{\delta(\theta)}{R}\cdot \tag{7}$$

3. **The set $\mathfrak{G}$.** 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 $\mathfrak{G}$ 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 $\mathfrak{G}$ 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 $\mathfrak{G}$, 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 τ be an element in $\mathfrak{R}$. By the last equations and (3),

$$\begin{aligned} \tau &= x_1\omega_1 + x_2\omega_2 + \cdots + x_n\omega_n, \\ C\tau &= x_1'\omega_1 + x_2'\omega_2 + \cdots + x_n'\omega_n \\ &\cdots\cdots\cdots\cdots\cdots\cdots \\ C^{n-1}\tau &= x_1^{(n-1)}\omega_1 + x_2^{(n-1)}\omega_2 + \cdots + x_n^{(n-1)}\omega_n, \end{aligned}$$

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

$I, C, C^2, \cdots, C^{n-1}$ form a basis of $\mathfrak{G}$. 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 ω'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 Ψ is an invariant of the above-mentioned substitution group. See Fricke, *Lehrbuch der Algebra*, vol. 2, p. 14.

† Latimer and MacDuffee, *A correspondence between classes of ideals and classes of matrices*, Annals of Mathematics, vol. 34 (1933).

LEMMA 2. *If $\theta = u\eta_1^{x_1}\eta_2^{x_2} \cdots \eta_n^{x_n}$ is a unit of F, where u is a root of unity, then*

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

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

$$C\omega_i = \alpha_{i1}\omega_1 + \alpha_{i2}\omega_2 + \cdots + \alpha_{in}\omega_n \qquad (i = 1, 2, \cdots, n)$$

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 $\mathfrak{R}$ 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 Ω which are unaltered under every substitution (ρ, ρ^a), where ρ is a primitive mth root of unity and a is an integer in a subgroup $\mathfrak{U}$ of $\mathfrak{R}$. Let the co-sets (Nebengruppen) of $\mathfrak{R}$ with respect to $\mathfrak{U}$ be $\mathfrak{U}_0 = \mathfrak{U}, \mathfrak{U}_1, \mathfrak{U}_2, \cdots, \mathfrak{U}_{E-1}$. Then $\mathfrak{U}_i = \gamma_i\mathfrak{U}$ where the γ_i are properly chosen integers. The factor group $\mathfrak{R}/\mathfrak{U}$ is simply isomorphic with $\mathfrak{A}$,* which by hypothesis is cyclic. Hence we may assume that $s = (\rho, \rho^\gamma)$, where γ is an integer such that $\gamma^E \equiv a \pmod{m}$, a an element in $\mathfrak{U}$. If m is odd, we may assume that γ is odd, while if m is even, γ is necessarily odd since the same is true of a.

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

(8)
$$\Delta = \prod_{\chi} \sum_{k=1}^{m/2} - \chi(k) \log \sin \frac{\pi k}{m} \cdot$$

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

(9)
$$\Delta = \prod_{t=1}^{n} \sum_{k=1}^{m/2} - \chi^t(k) \log \sin \frac{\pi k}{m},$$

where χ 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 ζ is a primitive eth root of unity. Employing $\chi(m-k) = \chi(k)$, $\chi(k) = 0$ if $(m, k) > 1$, and $\sum_{k=1}^{m-1} \chi^t(k) = 0$ $(0 < t < e)$, it may be shown that

(10)
$$2\sum_{k=1}^{m/2} \chi^t(k) \log \sin \frac{\pi k}{m} = \sum_{k=1}^{m-1} \chi^t(k) \lg (1 - \rho^k) = \sum_{i=0}^{n} \zeta^{ti} \lg \lambda_i,$$

* Weber, *Lehrbuch der Algebra*, 2d edition, vol. 2, p. 75.

† Gut, loc. cit., pp. 200, 223.

where $\lambda_0 = \Pi(1-\rho^a)$, a ranging over all the elements of $\mathfrak{U}$, and $\lambda_i = \lambda_0^{(i)}$ $(i=1, 2, \cdots, n)$. Employing a well known property of cyclic determinants, it may be shown from (9) and (10) that

$$\Delta = 2^{-n} \prod_{t=1}^{n} \sum_{i=0}^{n} \zeta^{ti} \lg \lambda_i = \pm \delta(\theta),$$

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

$$\left[\frac{(1-\rho^{\gamma a})(1-\rho^{-\gamma a})}{(1-\rho^{a})(1-\rho^{-a})}\right]^{1/2} = \pm \rho^{(1-\gamma)a/2}\left(\frac{1-\rho^{\gamma a}}{1-\rho^{a}}\right).$$

Since γ is odd, the unit on the left belongs to Ω, and hence the same is true of θ. Since θ is unaltered under every substitution (ρ, ρ^a), a in $\mathfrak{U}$, 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 Δ is exactly the same as the right side of (8), except that in this case χ ranges over those characters, except the principal character, such that $\chi(-1)=1$.† The whole group of characters is simply isomorphic with $\mathfrak{A}$ and hence every character is a power of one of them. For a generating character χ, we have $\chi(-1) = -1$. Hence $h_2 = \Delta/R$, where

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

Since $s^e(\theta)$ is the conjugate imaginary of θ, the co-set $\mathfrak{U}_e$ contains -1 and we may take as the elements of $\mathfrak{U}_{i+e}$ the negatives of the elements in the corresponding $\mathfrak{U}_i$. If a and b are prime to m and a is in $\mathfrak{U}_i$, then $\chi^2(a) = \chi^2(b)$ if and only if b is congruent to an element in $\mathfrak{U}_i$ or in $\mathfrak{U}_{i+e}$. The notation for the co-sets may be so chosen that if a belongs to $\mathfrak{U}_i$ then $\chi^2(a) = \zeta^i$, where ζ is a primitive eth root of unity. If we define the λ_i as before, let $\theta \equiv (\lambda_1 \cdot \lambda_{e+1} / \lambda_0 \cdot \lambda_e)$ and employ the fact that λ_{i+e} is the conjugate imaginary of λ_i, we find as before that $\Delta = \pm\delta(\theta)$, $h_2 = \pm\delta(\theta)/R$ and θ 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*

* For a special case of this, see Fueter, *Die Klassenzahl zyklischer Körper*, etc., Journal für Mathematik, vol. 147 (1917), p. 183.

† Gut, loc. cit., pp. 201, 223.

$n=e-1$. *Let* $\mathfrak{G}$ *be the set of all polynomials with rational integral coefficients in the nth order matrix* $A=(\alpha_{ij})$, *where the* α*'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*

$$H = N(\tau)/N(\mathfrak{K}),$$

where $N(\mathfrak{K})$ *is the norm of a non-singular ideal* $\mathfrak{K}$ *in* $\mathfrak{G}$ *and* $N(\tau)$ *is the norm of a principal ideal* $\{\tau\}$ *in* $\mathfrak{G}$, τ *being an element in* $\mathfrak{K}$. *If* F *is the field defined by a primitive mth 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 θ, $\delta(\theta)$, R, when properly specialized, are identical, except perhaps for sign, with Kummer's $e(\alpha)$, D, Δ respectively.*

It will be observed that by the proof of the above theorem, $\pm H$ is represented by the form $\Psi(x_1, x_2, \cdots, x_n)$, which, as previously noted, is an invariant 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 ζ be a primitive eth root of unity. ζ is a root of (2), and $1, \zeta, \zeta^2, \cdots, \zeta^{n-1}$ form a basis of the integral numbers in the field K defined by ζ. Hence by Lemma 1, $\mathfrak{G}$ is equivalent to the set of all integral algebraic numbers in K. Then, by well known theorems in algebraic numbers, there is an ideal $\mathfrak{L}$ such that $\{\tau\}=\mathfrak{K}\mathfrak{L}$ and $N(\tau)=N(\mathfrak{K})\cdot N(\mathfrak{L})$. We have then

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

$$H = N(\mathfrak{L}),$$

where $\mathfrak{L}$ *is an ideal in the field defined by a primitive eth root of unity.*

If F is the field defined by a primitive mth 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 Council, loc. cit., p. 34.

UNIVERSITY OF KENTUCKY,
LEXINGTON, KY.